ICT-2007-216676

ECRYPT II

European Network of Excellence in Cryptology II

Network of Excellence

Information and Communication Technologies

D.MAYA.7

Final Report on Jointly Executed Research Activities on Design and Analysis of Primitives and Protocols

Due date of deliverable: N.A.
Actual submission date: N.A.

Start date of project: 1 August 2008 Duration: 4 years

Lead contractor: Katholieke Universiteit Leuven (KUL)

Revision 1.1

Project co-funded by the European Commission within the 7th Framework Programme		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission services)	

Final Report on Jointly Executed Research Activities on Design and Analysis of Primitives and Protocols

Editor
Nigel Smart (BRIS)

N.A.
Revision 1.1

The work described in this report has in part been supported by the Commission of the European Communities through the ICT program under contract ICT-2007-216676. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Contents

Abstract

This report is the final update of the report on jointly executed research activities in public key encryption of the ECRYPT2 Network of Excellence (NoE), funded within the Information & Communication Technologies (ICT) Programme of the European Commission's Seventh Framework Programme (FP7).

The report provides a summary of the work carried out in the areas of research covered by all MAYA activities. This encompasses area of primitive and protocol design, techniques for proving that the created primitives and protocols are secure, as well as foundational mathematical techniques such a understanding the underlying hard mathematical problems.

Chapter 1

Introduction

In this report we outline the research which has been undertaken in the MAYA virtual lab. This is the part of ECRYPT-2 which focuses on analysis and design of new cryptographic protocols and schemes, and the analysis of the underlying hard mathematical problems.

We have divided this report into a number of chapters, which broadly divide the work done into related areas. However, the division is not tight and some work could have been placed in multiple chapters.

We start in Chapter 2 we make special note of the work conducted on schemes which are either widely deployed in the "real world", or which are either standardized or in the process of being standardized. This chapter is devoted to the constructive analysis of schemes and protocols, as well as attacks against these schemes and protocols. This chapter is therefore of the most direct relevance to industry.

In Chapter 3, Chapter 4 and Chapter 5 we focus on three applied areas which have shown a considerable advance over the period of ECRYPT-2. The first is devoted to the rapidly growing field of security related to RFID technology. We then turn to the topic of multi-party computation which is rapidly moving from a theoretical construction to a deployed technology. Then we turn to cloud computing, where some of the ideas from multi-party computation are now being applied.

The next two chapters, Chapter 6 and Chapter 7, deal with new results on two particular areas; namely signature schemes and identity based encryption. The first chapter on signatures displays the increasing interest in privacy preserving mechanisms in various application domains, whereas the second on IBE shows how this technology is now becoming more deployed and how ECRYPT-2 is influencing its development.

In Chapter 8 we describe the work which does not easily fit into the above classification. Mainly focusing on new schemes and concepts which are yet to find mainstream application areas.

We end this report by focusing on three more mathematical areas. In Chapter 9 we examine foundational and definitional issues related to the design and analysis of cryptographic algorithms and protocols. Then we pass in Chapter 10 to the discussion of various works on cryptanalysis on general systems which have been performed. This chapter covers all the work on attacking systems which has not been previously covered in the document, it mainly focuses on the more mathematical attacks on various parameter settings. Finally we end in Chapter 11 by examining implementation aspects of a series of existing (or proposed) protocols and schemes. This chapter focuses on the more mathematical aspects of implementation work done in ECRYPT-2, as opposed to the applied work in the VAMPIRE virtual lab.

Chapter 2

Work on Standardized or Deployed Schemes

2.1 TLS/SSL

The paper [170], which was ranked in the top three papers submitted to ASIACRYPT in 2008, provides an analysis of a minor variation of the TLS handshake protocol. The authors show, in the random oracle model, that the security requirements of the pre-master secret key agreement protocol within the TLS stack can be rather weak. This in particular implies that *deterministic* encryption can be used as a key transport mechanism. However, if *probabilistic* encryption is used for key transport, then the encryption scheme should be secure in the presence of a plaintext-checking oracle.

In [53], the authors present the first real-world exploit of a ”bug attack”, as proposed by Biham Carmeli and Shamir at CRYPTO 2008 . Roughly, a bug attack consists of exploring a dorment error in a cryptographic primitive implementation. Such an error must occur rarely enough so as to go undetected by standard testing methods yet, if known to an attacker, it may be triggered to break the security of the primitive and recover a secret key. The concrete bug to be explored in [53] is a faulty implementation of a modular reduction algorithm underlying the elliptic curve cryptography stack of (a specific version of) openssl. It is shown that static variants of ECDH implemented in openssl can be subject to a bug attack and recover a server’s secret key. Proactive and corrective countermeasures against this sort of attack are also discussed in the paper.

A major issue with analysing key agreement protocols such as TLS/SSL is that the standard security models cannot normally be applied. In particular the bridge between the key agreement phase and the secure channel phase is often problematic; and standard mechanisms to ensure such composability (such as the UC framework) cannot be applied in practice. In [55] a new approach to modeling composability is presented. The new approach is modular but tailors it’s security analysis to the requirements of the schemes under consideration. The paper presents the general framework, which is presented in terms of games as opposed to simulatability based definitions; and then goes onto to apply the new framework to TLS/SSL.

2.2 SSH

Two of our papers provide security analysis of the widely-deployed Internet protocol SSH [14, 183]. In [14], the authors presented a variety of plaintext-recovering attacks against the SSH Binary Packet Protocol (BPP) and implemented a proof of concept of the attacks against OpenSSH. Their paper explained why a combination of flaws in the basic design of SSH leads implementations such as OpenSSH to be open to the attacks, why current provable security results for SSH did not cover the attacks, and how the attacks can be prevented in practice. In [183], the authors followed-up the first paper with a provable security analysis of the SSH BPP in counter mode in a security model that accurately captures the capabilities of real-world attackers, as well as security-relevant features of the SSH specifications and the OpenSSH implementation of SSH. Under reasonable assumptions on the block cipher and MAC algorithms used to construct the SSH Binary Packet Protocol, the authors of [183] were able to show that the SSH BPP meets a strong and appropriate notion of security: indistinguishability under buffered, stateful chosen-ciphertext attacks. This result helps to bridge the gap between the existing security analysis of the SSH BPP by Bellare et al. and the attacks against the SSH BPP in [14].

A major problem with the analysis of the channel security of SSH is the issue of ciphertext fragmentation. In [45] the authors present a full analysis of symmetric encryption in the presence of ciphertext fragmentation. The authors consider security properties related to ciphertext boundary hiding and robustness against Denial-of-Service attacks.

2.3 EMV

The Schnorr signature scheme is an old scheme which currently is not deployed, although it is has just been standardised by ISO. In [171] the authors provide a security proof of the Schnorr signature scheme in the generic group model. This allows them to provide explicit requirements on the hash functions used within the scheme. Unsurprisingly the requirements are weaker than those for signature schemes such as DSA, thus either smaller hash sizes need be taken, or weaker hash functions may be used (or both). In light of current concerns over the security of hash functions, the paper sheds important light on what may become an important signature scheme. This is particularly relevant as Schnorr signatures are being considered as the underlying signature scheme for the next generation of the EMV standard.

In [205] the author examines an extension of the Bleichenbacher/Manger attack to the PIN encryption scheme used within the EMV system. The paper shows that if access to a certain plaintext partial validity checking oracle can be obtained, then the scheme can be broken using a very small number of queries to this oracle.

In [130] the authors consider a scenario in which parties use a public key encryption scheme and a signature scheme with a single public key/private key pair—so the private key is used for both signing and decrypting. Such a simultaneous use of a key is in general considered poor cryptographic practice, but from an efficiency point of view looks attractive. In addition such a situation occurs in many real life scenarios; for example in the EMV payment system, or in TLS/SSL. The paper offers security notions to analyze such violations of key separation. For both the identity- and the non-identity-based setting it is shown that — although being insecure in general — for schemes of interest the resulting combined (identity-based) public key scheme can offer strong security guarantees.

In [179] the authors revisit this topic of joint security for combined public key schemes, wherein a single keypair is used for both encryption and signature primitives in a secure manner. While breaking the principle of key separation, such schemes have attractive properties and are sometimes used in practice. The authors give a general construction for a combined public key scheme having joint security that uses IBE as a component and that works in the standard model, and provide a more efficient direct construction, also in the standard model. The authors then consider the problem of how to build signcryption schemes from jointly secure combined public key schemes, and provide a construction that uses any such scheme to produce a triple of schemes – signature, encryption, and signcryption – that are jointly secure in an appropriate and strong security model.

As remarked above this topic is important, since the EMV standards allow for the same key-pair to be used for both signature and encryption, as this may reduce processing and storage costs. In [87] the authors provide a formal security treatment of current and future algorithms for signature and encryption in the EMV standards under this setting. First a theoretical attack for EMV's current RSA-based algorithms is presented, showing how access to a partial decryption oracle can be used to forge a signature on a freely chosen message. This would allow an attacker to carry out an offline transaction using a CDA card without knowing its cardholder's PIN. EMV Co is currently considering adopting elliptic-curve-based signature and encryption algorithms in future versions of the EMV standards. In the second part of the paper, the authors show that for these elliptic-curve-based algorithms the practice of sharing the same key-pair is secure.

In 1999, an existential signature forgery attack based on index calculus techniques [250] was discovered against two popular RSA signature standards, ISO-9796-1 and ISO-9796-2. Following this attack, ISO-9796-1 was withdrawn, and ISO-9796-2 was amended by increasing the message digest size requirement to at least 160 bits. This amended version, ISO-9796-2:2002, was considered safe against the previous attack. The authors of [78] propose a number of algorithmic refinements to successfully attack ISO-9796-2:2002 for all modulus sizes. The new attack is based on several tools, including more efficient algorithms for finding smooth integers in a large batch of numbers, which improve the efficiency of the previous attack by a large constant factor and renders ISO-9796-2:2002 vulnerable. A practical ISO-9796-2:2002 forgery for the RSA-2048 challenge modulus was computed in a couple of days using 19 servers on the Amazon EC2 cloud for a total cost of $\approx$ 800 USD. The same attack also applies to the ISO-9796-2-compliant signature formats defined as part of the EMV specifications, and while more computationally demanding, it is within reach of a resourceful attacker ($\approx$ 45,000 USD on Amazon EC2); since the attack requires signatures on many chosen messages, however, it is unlikely to be a practical threat to EMV payment card users. This new attack led to another amendment of the standard, ISO-9796-2:2010, being drafted and published within 18 months.

The earliest and one of the best known examples of fault analysis in cryptology is the so-called Bellcore attack described by Boneh, DeMillo and Lipton against RSA-CRT signatures [234]. If an RSA signature for an RSA modulus $n = pq$ is computed using the Chinese Remainder Theorem (as is usually the case for efficiency reasons), an adversary can let the device operate correctly during the computation modulo p and inject a fault during the computation modulo q. This results in a signature which is correct modulo p and faulty modulo q, and enables the adversary to retrieve a value which is equal to the original padded message modulo p but not modulo q. Therefore, when the signature padding used in the scheme is deterministic (e.g. FDH), or when it is probabilistic with public randomness (e.g.

PFDH), the adversary can directly factor N by taking the GCD of this faulty value with the correct padded message. The attack is thwarted, however, when the signature padding involves randomness which isn't transmitted along with the message (e.g. PSS) or when parts of the message are recovered as part of signature verification (e.g. certain schemes from the ISO-9796-2 standard). Nevertheless, for affine padding schemes (including ISO-9796-2 and EMV signatures), a CHES 2009 paper [249] showed how Coppersmith techniques can be used to recover the unknown parts of the padded message from the faulty signature when they are short enough, after which factoring N again becomes a matter of computing a GCD. This technique can in principle recover unknown parts as large as 0.207 times the modulus size with a single fault, and up to half of the modulus size when more faults are available. In practice, however, even with several faults, fractions larger than about 0.23 are computationally intractable, because larger fractions require more faults and the complexity increases exponentially with the number of faults. The authors of [79] describe another lattice-based fault attack using entirely different techniques (so-called orthogonal lattices) whose complexity remains polynomial in the number of faults. As a result, this new attack can handle much larger unknown parts in practice (the theoretical limit of one half becomes practical), including those occurring in most EMV signature formats. The authors present a particular EMV format well beyond the reach of the previous attack, for which the modulus N can be factored in a fraction of a second using ten faulty signatures using the new attack.

A number of refinement of Boneh et al.'s attack were later proposed, as well as numerous countermeasures to protect from them, but most of the corresponding research has concentrated on the perturbation of one of the two half-exponentiations in signature generation. The authors of [51], on the other hand, consider the injection of faults in the *public modulus* before CRT interpolation. This is a very different type of fault which does not seem to have been considered before, and which defeats fault countermeasures that concentrate on protecting the exponentiations. The new attack, based on the orthogonal lattice techniques of Nguyen and Stern [299], proves very effective in practice: depending on the fault model, between 5 to 45 faults suffice to recover the RSA factorization within a few seconds. In its simplest form, the attack requires that the adversary knows the faulty moduli, but more sophisticated variants work even if the moduli are unknown, under reasonable fault models. All variants were validated experimentally with laser fault-injection techniques.

2.4 RSA PKCS# v1.5 Encryption

PKCS#1 v1.5 is an ad hoc message encoding format for RSA encryption, which remains one of the most widely used RSA encryption padding to this day, despite several known security vulnerabilities, and the currently valid version of the PKCS standard advising against its use. The authors of [30] provide further analysis of its security, and in particular describe two new attacks against it in different settings. On the one hand, they show that Coppersmith techniques can be used to attack PKCS#1 v1.5 encryption in a broadcast setting with small public exponent: if the same message is encrypted for sufficiently many recipients with different random nonces for each, an adversary can recover all the nonces and the original message. For $e = 3$ and 64-bit nonces (the recommended minimum), for example, 4 ciphertexts for different recipients are theoretically enough to decrypt in polynomial time. On the other hand, they investigate the validity-checking security of PKCS#1 v1.5 encryption, namely the security against an adversary with access to an oracle deciding whether a given element of

$\mathbb{Z}_N^*$ is a valid ciphertext. Bleichenbacher's well-known attack against SSL [232] relied on the fact that a million queries to such an oracle can break the one-wayness of PKCS#1 v1.5. In this paper, the authors show that a single query is sufficient to break semantic security with overwhelming advantage.

2.5 RSA-FDH Signature Scheme

RSA-FDH and many other schemes secure in the Random-Oracle Model (ROM) require a hash function with output size larger than standard sizes. In [156] the authors show that the random-oracle instantiations proposed in the literature for such cases are weaker than a random oracle, including early proposals by Bellare and Rogaway, and the ones implicit in IEEE P1363 and PKCS standards. Next, the authors study the security impact of hash function defects for ROM signatures. The authors give evidence that in the case of RSA and Rabin/Rabin-Williams, an appropriate PSS padding is more robust than all other paddings known.

2.6 Timestamps in ISO-9798

New generic modelling technique that can be used to extend existing frameworks for theoretical security analysis in order to capture the use of timestamps are presented in [24]. The authors apply this technique to two of the most popular models adopted in literature: the Bellare-Rogaway [226] and Canetti-Krawczyk [246] models. They analyse previous results obtained using these models in light of the proposed extensions, and demonstrate their application to a new class of protocols. In the timed CK model the paper concentrates on modular design and analysis of protocols, and proposes a more efficient timed authenticator relying on timestamps. The structure of this new authenticator implies that an authentication mechanism standardised in ISO-9798 [283] is secure. Finally, the authors use their timed extension to the BR model to establish the security of an efficient ISO protocol [282] for key transport and unilateral entity authentication.

2.7 Machine Readable Travel Documents (e-Passports)

Machine Readable travel documents have been rapidly put in place since 2004. The initial standard was made by the ICAO ([280, 281]) and it has been quickly followed by the Extended Access Control (EAC: [222]). In [67] the authors discuss about the evolution of these standards and more precisely on the evolution of EAC. This paper intends to give a realistic survey on these standards and discusses about their problems, such as the inexistence of a clock in the biometric passports and the absence of a switch preventing the lecture of a closed passport. The paper also looks at the issue with retrocompatibility that could be easily solved and the issue with terminal revocation that is harder. Hence the conclusions of [67] invalidates the claims of [300].

Different security notions and settings for identification protocols have been proposed so far, considering different powerful adversaries that can play "man-in-the-middle" attacks. In [44] the authors consider one of the strongest forms of these attacks, namely resettably non-transferable identification introduced in [223]. This notion immunizes a scheme from powerful adversaries that have physical access to the proving device and can thus reset it to a previous state. Then the authors discuss some limitations of existing notions as well as different impossibility results for strong notions of non-transferability. They introduce a strong and achievable notion for resettably non-transferable identification that reflects real scenarios more adequately and show a general protocol that satisfies it. They show how to efficiently instantiate their construction and discuss the viability of their protocol for the next generation of electronic passports (e-passports).

2.8 Direct Anonymous Attestation

In [69] the authors develop a proof for a previously published pairing based Direct Anonymous Attestation (DAA) protocol. Subsequent to the publication a number of problems were found in the proof and in the scheme. However, many of these same problems also apply to all other DAA schemes.

In [32] these problems are dicussed in more detail and a full game-based security model for DAA protocols is provided. The model pay particular attention to the functional requirements of linkability (and non-linkability) and in addition the notion of what an identity is in such schemes. Many of these points having been ignored, or glossed over, in prior work. In addition the paper presents a secure DAA scheme based on pairings; however despite the proof of security the TCG (Trusted Computing Group) is in the process of standardizing the flawed scheme from [69] rather than the one from [32].

The privacy-CA solution (PCAS) designed by the Trusted Computing Group (TCG) was specified in TCG Trusted Platform Module (TPM) Specification Version 1.2 in 2003 and allows a TPM to obtain from a certification authority (CA) certificates on short term keys. The protocol is a lighter alternative to the Direct Anonymous Attestation (DAA) scheme for anonymous platform authentication. One undesirable property of the protocol is that security holds only when no TPM is corrupt as, otherwise, an attack can be easily mounted. The paper [68] proposes and investigates a stronger protocol (which we refer to as the enhanced PCAS). The intention is that the newly proposed protocol withstand attacks of corrupt TPMs. This paper introduces new security notions than those considered in the literature in the context of of the PCAS protocol and analyzed the newly proposed protocol with respect to these properties. These properties are : *unforgeability* which refines earlier models for the case where TPMs may be corrupted, *deniability* which says that a CA cannot prove to a third party that he engaged in a run of the protocol with a certain TPM, and *anonymity* is the property that third parties cannot tell the identity of TPMs based on the certificates that the TPM uses. The newly proposed protocol is shown to satisfy all of these properties.

Anonymous credential systems provide privacy-preserving authentication solutions for accessing services and resources. In these systems, copying and sharing credentials can be a serious issue. As this cannot be prevented in software alone, these problems form a major obstacle for the use of fully anonymous authentication systems in prac- tice. In this [65], the authors propose a solution for anonymous authentication that is based on a hardware security module to prevent sharing of credentials. Their protocols are based on the standard protocols Transport Layer Security (TLS) and Direct Anonymous Attestation (DAA). The authors present a detailed description and a reference implementation of their approach based on a Trusted Platform Module (TPM) as hardware security module. Moreover, they discuss drawbacks and alternatives, and provide a pure software implementation to compare with their TPM-based approach.

2.9 Random Number Generation

In [71] the authors study a quite simple deterministic randomness extractor from random Diffie-Hellman elements defined over a prime order multiplicative subgroup G of a finite field $\mathbb{Z}_p$ (the truncation), and over a group of points of an elliptic curve (the truncation of the abscissa). Informally speaking, they show that the least significant bits of a random element in $G \subset \mathbb{Z}_p^*$ or of the abscissa of a random point in $\mathcal{E}(\mathbb{F}_p)$ are indistinguishable from a uniform bit-string. Such an operation is quite efficient, and is a good randomness extractor, since they show that it can extract nearly the same number of bits as the Leftover Hash Lemma can do for most Elliptic Curve parameters and for large subgroups of finite fields. To this aim, the authors develop a new technique to bound exponential sums that allows us to double the number of extracted bits compared with previous known results proposed at ICALP'06 by Fouque *et al.* [264]. It can also be used to improve previous bounds proposed by Canetti *et al.* [244]. One of the main applications of this extractor is to mathematically prove an assumption proposed by Canetti *et al.* [247] at Crypto '07 and used in the security proof of the Elliptic Curve Pseudo Random Generator proposed by the NIST. The second most obvious application is to perform efficient key derivation given Diffie-Hellman elements.

2.10 Key Management – KMIP

Key management is the Achilles' heel of cryptography. In recent work [37], a novel *Key-Lifecycle Management System (KLMS)* has been introduced, which addresses two issues that have not been addressed comprehensively so far. First, the novel KLMS introduces a *pattern-based* method to *simplify* and to *automate* the *deployment* task for keys and certificates, i.e., the task of associating them with endpoints that use them. Currently, the best practice is often a *manual* process, which does not scale and suffers from human error. The pattern-based approach eliminates these problems and specifically takes into account the lifecycle of keys and certificates. The result is a centralized, scalable system, addressing the current demand for automation of key management. Second, KLMS provides a novel form of *strict access control* to keys and realizes the first cryptographically sound and secure access-control policy for a key-management interface. It is based on the policy model developed by Cachin and Chandran [240]. Strict access control takes into account the cryptographic semantics of certain key-management operations (such as key wrapping and key derivation) to prevent attacks through the interface, which plagued earlier key-management interfaces with less sophisticated access control. The API policy implementing strict access control is specific to cryptographic keys and therefore particularly interesting from the security perspective. The system design of KLMS addresses the needs of a variety of different applications and endpoints, and includes an interface to the Key Management Interoperability Protocol (KMIP) that has been standardized recently [301].

To provide efficient key management in various banking applications keys are often stored in Hardware Security Modules (HSMs); indeed the keys never leave the HSM and all cryptographic operations need to be performed by the said HSM. But such HSMs have very limited cryptographic functionality and in particular often do not implement more modern approaches to providing secure communication. In [47] a protocol to enable the use of an HSM to provide an authenticated encryption scheme is analysed. The protocol/mode-of-operation is deployed in a number of European banks and this paper is the first paper to provide a public security analysis and general treatment of the scheme. The advantage of the scheme analysed is that it can provide an authenticated encryption scheme with only using single call to the HSM.

Chapter 3

Work on Protocols and Schemes for RFID Tags

There has been considerable work on protocols and schemes for RFID tags. We summarize the work conducted in ECRYPT-2 on this in this chapter.

3.1 Security Models for RFID Tags

Vaudenay presented in [313] a general RFID security and privacy model that abstracts some previous works in a single, concise, and much more understandable framework. He introduced eight distinct notions of privacy, corresponding to adversaries of different strength, and proved some possibility and impossibility results for such privacy notions. However, some interesting problems as:

1. Achieving *stronger privacy using low-cost tags* (i.e., tags that usually can not perform public-key cryptography),

2. Achieving *stronger privacy in presence of side-channel attacks* (e.g., DoS attacks, detection of the outputs of identification protocols),

3. Achieving *stronger privacy under standard complexity-theoretic assumptions*,

are still left open.

In [82, 83], the authors address the above problems and give two contributions. First of all they show that Vaudenay's privacy notions are *impossible to achieve* in presence of DoS attacks. Therefore, they extend the model to better reflect the real-world scenario, where these attacks are easy to mount (e.g., by physically destroying/making inactive tags). More precisely, they refine Vaudenay's privacy model to deal with DoS and DoS-like attacks, and introduce an additional privacy notion, referred to as *semi-destructive* privacy, which takes into account hardware features of some real-world tags. Then, they show an *efficient RFID protocol* that, by only using symmetric-key cryptography, satisfies the notion of semi-destructive privacy, *under standard complexity-theoretic assumptions*.

In [198] the authors extend and improve the current state-of-the art for privacy-protecting RFID by introducing a security and privacy model for anonymizer-enabled RFID systems. Their model builds on top of Vaudenay's model and supports anonymizers, which are separate devices specifically designated to ensure the privacy of tags. They present a privacy-preserving

RFID protocol that achieves narrow-strong privacy without requiring tags to perform public-key operations, thus providing a satisfying notion of privacy for low-cost tags in response to an open question raised by Vaudenay.

The strongest achievable notion of privacy in Vaudenay's model (*narrow-strong privacy*) requires public-key cryptography, which in general exceeds the computational capabilities of current cost-efficient RFIDs. Other privacy notions achievable without public-key cryptography heavily restrict the power of the adversary and thus are not suitable to realistically model the real world. In [199], the authors extend and improve the current state-of-the art for privacy-protecting RFID by introducing a security and privacy model for *anonymizer*-enabled RFID systems. The model builds on top of Vaudenay's model and supports anonymizers, which are separate devices specifically designated to ensure the privacy of tags. The auhors present a privacy-preserving RFID protocol that uses anonymizers and achieves narrow-strong privacy without requiring tags to perform expensive public-key operations (i.e., modular exponentiations), thus providing a satisfying notion of privacy for cost-efficient tags.a

In [201] the authors present an efficient privacy-preserving RFID protocol that addresses Vaudenay's open question on the feasibility of destructive privacy, i.e., privacy of tags that are destroyed during corruption. The protocol is based on the use of Physically Unclonable Functions (PUFs), which provide cost-efficient means to fingerprint chips based on their physical properties and can be used to realize tamper-evident storage for cryptographic secrets.

In [19] the authors revisit the model proposed by Vaudenay and investigate some subtle issues such as tag corruption aspects. They show that in formal definition tag corruption discloses the temporary memory of tags and leads to the impossibility of achieving both mutual authentication and any reasonable notion of RFID privacy in their model. Moreover, they show that the strongest privacy notion (narrow-strong privacy) cannot be achieved simultaneously with reader authentication even if the adversary is not capable of corrupting a tag during the protocol execution. Although the results are shown on the privacy definition of Vaudenay, they give insight to the difficulties of setting up a mature security and privacy model for RFID systems that aims at fulfilling the sophisticated requirements of real-life applications.

In [20] the authors revisit the model proposed by Paise and Vaudenay [303] that defines mutual authentication (between RFID tags and readers) and several privacy notions that capture adversaries with different tag corruption behavior and capabilities. More in details, in [20] the authors investigate some subtle issues such as tag corruption aspects. They show that in the formal definitions of [303] tag corruption discloses the temporary memory of tags and leads to the impossibility of achieving both mutual authentication and any reasonable notion of RFID privacy in their model. Moreover, they show that the strongest privacy notion (narrow-strong privacy) cannot be achieved simultaneously with reader authentication even under the strong assumption that tag corruption does not disclose temporary tag states. Further, they show other impossibility results that hold if the adversary can manipulate an RFID tag such that it resets its state or when tags are stateless.

In [134] the authors examine some recently proposed RFID privacy models and identify several weaknesses in these models. Several models are based on weak assumptions regarding corruption, lack generality or use uncommon modelling techniques that cause the impossibility of privacy levels. The authors propose a new RFID privacy model that is based on indistinguishability and that does not suffer from the identified drawbacks whilst maintaining the highest privacy level. This is the first model where wide-strong privacy can be attained.

3.2 Protocols Suitable for RFID Tokens

At the RFID Security Workshop 2007 [309], Adi Shamir presented a new challenge-response protocol well suited for RFIDs, although based on the Rabin public-key cryptosystem. This protocol, which is called SQUASH-0, was using a linear mixing function and has subsequently been withdrawn. Essentially, [172] shows how to mount an attack against SQUASH-0 with full window which could be used as a "known random coins attack" against Rabin-SAEP. It then extends it for SQUASH-0 with arbitrary window. Applied with the originally proposed modulus it is shown how to run a key recovery attack using 1024 chosen challenges. Since the security arguments equally apply to the final version of SQUASH [310] and to SQUASH-0, this attack challenges the blame-game argument for the security of SQUASH. Nevertheless, these attacks are inefficient when using non-linear mixing so the security of SQUASH remains open.

In [18] the authors present an anonymous authentication scheme that allows RFID tags to authenticate to readers without disclosing the tag identity or any other information that allows tags to be traced. The properties of the scheme are very useful for a variety of access control systems, where it is sufficient or mandatory to verify the authenticity of a tag without inferring its identity. The scheme is based on the recently proposed anoymizer-approach, where additional devices (called anonymizers) frequently interact with the tags to ensure anonymity and unlinkability of tags. This allows using cost-effective RFID tags that cannot perform public-key cryptography in an efficient and scalable way. The solution provides (i) anonymity and untracability of tags against readers, (ii) secure tag authentication even against collusions of malicious readers and anonymizers, and (iii) security against denial-of-service attacks.

In [92] the privacy of the EC-RAC protocol [290] is examined. The authors show that both the ID-Transfer and the ID&PWD-Transfer scheme do not provide the claimed privacy levels by using man-in-the-middle attacks. The existence of these attacks shows that the privacy proofs for EC-RAC are incorrect.

3.3 Location Privacy and RFID

RFID-enabled systems allow fully automatic wireless identification of objects and are rapidly becoming a pervasive technology with various applications. However, despite their benefits, RFID-based systems also pose challenging risks, in particular concerning user privacy. Indeed, improvident use of RFID can disclose sensitive information about users and their locations allowing detailed user profiles. Hence, it is crucial to identify and to enforce appropriate security and privacy requirements of RFID applications (that are also compliant to legislation). In [200] the authors first discusses security and privacy requirements for RFID-enabled systems, focusing in particular on location privacy issues. Then it explores the advances in RFID applications, stressing the security and privacy shortcomings of existing proposals. Finally, it presents new promising directions for privacy-preserving RFID systems, where as a case study the authors focus electronic tickets (e-tickets) for public transportation.

3.4 RFID Based E-Tickets

Recently, operators of public transportation in many countries started to roll out electronic tickets (e-tickets). E-tickets offer several advantages to transit enterprises as well as to their customers, e.g., they aggravate forgeries by cryptographic means whereas customers benefit from fast and convenient verification of tickets or replacement of lost ones. Existing (proprietary) e-ticket systems deployed in practice are mainly based on RFID technologies where RFID tags prove authorization by releasing spatio-temporal data that discloses customer-related data, in particular their location. Moreover, available literature on privacy-preserving RFID-based protocols lack practicability for real world scenarios. In [197] the authors discuss appropriate security and privacy requirements for e-tickets and point out the shortcomings of existing proposals. They then propose solutions for practical privacy-preserving e-tickets based on known cryptographic techniques and RFID technology.

3.5 RFID Based Supply-Chain Management

In [173] an application of RFIDs for supply-chain management is presented. In this application, two types of readers are considered. For one, there are readers that will mark tags at given points. Afterwards, these tags can be checked by a second type of readers to tell whether a tag has followed the correct path in the chain. This work formalizes this notion and defines adequate adversaries. Morever, requirements are derived in order to meet security against counterfeiting, cloning, impersonation and denial of service attacks.

Chapter 4

Work on Multi-Party Computation and Secure Function Evaluation

A lot of work in this section not only represents work partially supported by ECRYPT-II, but work which was also partially supported by the other FP7 Project CACE.

4.1 Secure Function Evaluation

Secure Evaluation of Private Functions (PF-SFE) allows two parties to compute a private function which is known by one party only on private data of both. It is known that PF-SFE can be reduced to Secure Function Evaluation (SFE) of a Universal Circuit (UC). Previous UC constructions only simulated circuits with gates of $d = 2$ inputs while gates with $d > 2$ inputs were decomposed into many gates with 2 inputs which is inefficient for large d as the size of UC heavily depends on the number of gates. In [194], the authors present generalized UC constructions to efficiently simulate any circuit with gates of $d \neq 2$ inputs having efficient circuit representation. The constructions are non-trivial generalizations of previously known UC constructions. As application it is shown how to securely evaluate private functions such as neural networks (NN) which are increasingly used in commercial applications. The provably secure PF-SFE protocol needs only one round in the semi-honest model (or even no online communication at all using non-interactive oblivious transfer) and evaluates a generalized UC that entirely hides the structure of the private NN. This enables applications like privacy-preserving data classification based on private NNs without trusted third party while simultaneously protecting user's data and NN owner's intellectual property.

Two-party Secure Function Evaluation (SFE) allows two parties to evaluate a function known to both parties on their private (secret) inputs. Some applications with sophisticated privacy needs require the function to be known only to one party and kept private (hidden) from the other one. However, existing solutions for SFE of private functions (PF-SFE) deploy Universal Circuits (UC) and are still very inecient in practice. In [185] the authors bridge the gap between SFE and PF-SFE with SFE of so-called semi-private functions (SPF-SFE), i.e., one function out of a given class of functions is evaluated without revealing which one. A general framework for SPF-SFE is presented allowing a fine-grained trade-off and tuning between SFE and PF-SFE covering both extremes. In the framework, semiprivate functions can be composed from several privately programmable blocks (PPB) which can be programmed with one function out of a class of functions. The framework allows efficient and secure embedding of constants into the resulting circuit to improve performance. To demonstrate practicability of the framework a compiler for SPF-SFE was implemented based on the Fairplay SFE framework. SPF-SFE is sufficient for many practically relevant privacy-preserving applications, such as privacy-preserving credit checking which can be implemented using the framework and compiler as described in the paper.

The work in [192] the authors describe an implementation of the Yao protocol for two-party secure fucntion evaluation, for a large circuit (in particular AES). The work shows this, previously considered theoretical, protocol can be used in real-life examples. In addition the paper develops a number of optimizations and shows these optimizations to be secure in the simulation based model.

In [132] the authors present TASTY, a novel tool for automating, i.e., describing, generating, executing, benchmarking, and comparing, efficient secure two-party computation protocols. TASTY is a new compiler that can generate protocols based on homomorphic encryption and efficient garbled circuits as well as combinations of both, which often yields the most efficient protocols available today. The user provides a high-level description of the computations to be performed on encrypted data in a domain-specific language. This is automatically transformed into a protocol. TASTY provides most recent techniques and optimizations for practical secure two-party computation with low online latency. Moreover, it allows to efficiently evaluate circuits generated by the well-known Fairplay compiler. TASTY is used to compare protocols for secure multiplication based on homomorphic encryption with those based on garbled circuits and highly efficient Karatsuba multiplication. Further, TASTY improves the online latency for securely evaluating the AES functionality by an order of magnitude compared to previous software implementations. TASTY allows to automatically generate efficient secure protocols for many privacy-preserving applications where the use cases for private set intersection and face recognition protocols is looked at.

In [153] generic Garbled Circuit (GC)-based techniques for Secure Function Evaluation (SFE) in the semi-honest model are considered. Efficient GC constructions are given for addition, subtraction, multiplication, and comparison functions. These circuits for subtraction and comparison are approximately two times smaller (in terms of garbled tables) than previous constructions. This implies corresponding computation and communication improvements in SFE of functions using their efficient building blocks. The techniques rely on recently proposed "free XOR" GC technique. Further, this paper presents concrete and detailed improved GC protocols for the problem of secure integer comparison, and related problems of auctions, minimum selection, and minimal distance. Performance improvement comes both from building on efficient basic blocks and several problem-specific GC optimizations. The authors provide precise cost evaluation of their constructions, which serves as a baseline for future protocols.

In [147] the authors consider Secure Function Evaluation (SFE) in the client-server setting where the server issues a secure token to the client. The token is not trusted by the client and is not a trusted third party. They show how to take advantage of the token to drastically reduce the communication complexity of SFE and computation load of the server. The main contribution is the detailed consideration of design decisions, optimizations, and trade-offs, associated with the setting and its strict hardware requirements for practical deployment. In particular, they model the token as a computationally weak device with small constant-size memory and limit communication between client and server. They consider semi-honest, covert, and malicious adversaries and show the feasibility of their protocols based on a FPGA implementation.

Secure set intersection protocols are the core building block for a manifold of privacy-preserving applications. The idea of using trusted hardware tokens for the set intersection problem was introduced in [277], devising protocols which improve over previous (in the standard model of two-party computation) protocols in terms of efficiency and secure composition. Their protocol uses only a linear number of symmetric-key computations and the amount of data stored in the token does not depend on the sizes of the sets. The security proof of the protocol is in the universal composability model and is based on the strong assumption that the token is trusted by both parties. In [105] the authors revisit the idea and model of hardware-based secure set intersection, and in particular consider a setting where tokens are not necessarily trusted by both participants to additionally cover threats like side channel attacks, firmware trapdoors and malicious hardware. Their protocols are very efficient and achieve the same level of security as those of [277] for trusted tokens. For untrusted tokens, the protocols ensure privacy against malicious adversaries, and correctness facing covert adversaries.

4.2 General Multi-Party Computation

Collusion-free protocols prevent subliminal communication (i.e., covert channels) between parties running the protocol. In the standard communication model, if one-way functions exist, then protocols satisfying any reasonable degree of privacy cannot be collusion-free. Prior approaches to building collusion-free protocols require exotic channels. By taking a conceptually new approach, in [16] the authors consider a communication channel which can filter and rerandomize message traffic. They then provide a new security definition that captures collusion-freeness in this new setting; their new setting even allows for the mediator to be corrupted in which case the security gracefully fails to providing standard privacy and correctness. This stronger notion makes the property useful in more settings. To illustrate feasibility, they construct a commitment scheme and a zero- knowledge proof of knowledge that meet their definition in its two variations. In [17], the authors strengthen the definition of [16] and resolve the main open questions in this area by showing a collusion-free protocol (in the mediated model) for computing any multi-party functionality.

In [88] the authors present a new MPC protocol, called SPDZ, in the case of dishonest majority and active adversaries. The protocol makes use of an offline phase based on homomorphic encryption, and a novel use of MAC's in the online phase. The online phase is essentially only a constant times more expensive than evaluating the underlying circuit in the clear; albeit the constant is large. This means that the protocol in [88] is essentially, bar constants, optimal in the online phase costs. For the offline phase, one run is very expensive, however this comes at the benefit of one run producing so much data than one only needs to execute the offline phase occasionally.

In [89] an implementation report is given on the SPDZ protocol based on the evaluation of the AES functionality. The report presents various optimizations for both active and covert security and shows that the SPDZ protocol is practical even for relatively large number of parties (say 10), whilst achieving comparable if not better performance than previous techniques.

In [184], [74] the authors consider aspects of Verifiable Secret Sharing in the context of asynchronous networks; and the associated applications to Multi-Party computation. The particular interest in asynchronous protocols is because these more closely match the type of network environment one finds in the real world. The work in these papers is focused on protocols which achieve information theoretic security.

4.3 Applications of MPC and SFE

Recently MPC and SFE have found a number of possible application niches. Some of these are currently purely hypothetical, whereas others are practical (and even deployed) today. In this section we outline a number of these niches which we have worked upon.

4.3.1 Privacy Preserving Data Base Lookup

Automatic recognition of human faces is becoming increasingly popular in civilian and law enforcement applications that require reliable recognition of humans. However, the rapid improvement and widespread deployment of this technology raises strong concerns regarding the violation of individuals' privacy. A typical application scenario for privacy-preserving face recognition concerns a client who privately searches for a specific face image in the face image database of a server. In [195], the authors present a privacy-preserving face recognition scheme that substantially improves over previous work in terms of communication- and computation efficiency: the most recent proposal of Erkin et al. (PETS'09) requires $\mathcal{O}(\log M)$ rounds and computationally expensive operations on homomorphically encrypted data to recognize a face in a database of M faces. The improved scheme requires only $\mathcal{O}(1)$ rounds and has a substantially smaller online communication complexity (by a factor of 15 for each database entry) and less computation complexity. The solution is based on known cryptographic building blocks combining homomorphic encryption with garbled circuits. The implementation results show the practicality of the scheme also for large databases (e.g., for $M = 1000$ less than 13 seconds and less than 4 MByte online communication are needed on two 2.4GHz PCs connected via Gigabit Ethernet).

4.3.2 Distributed Key Generation

In [122] the authors present a simple application of multi-party computation to enable the key distribution centre in a Sakai–Kasahara based IBE system to be distributed. This work was performed to answer a specific request from a company which is deploying such systems and is likely to be deployed in the "real–world" in the near future.

4.3.3 Pattern Matching

In [216] the author presents simple protocols for secure two-party computation of generalized pattern matching in the presence of malicious parties. The problem is to determine all positions in a text $\mathcal{T}$ where a pattern $\mathcal{P}$ occurs (or matches with few mismatches) allowing possibly both $\mathcal{T}$ and $\mathcal{P}$ to contain single character wildcards. The author proposes constant-round protocols that exhibit linear communication and quasilinear computational costs with simulation-based security. Its constructions rely on a well-known technique for pattern matching proposed by Fischer and Paterson in 1974 and based on the Fast Fourier Transform. The security of the new schemes is reduced to the semantic security of the ElGamal encryption scheme.

4.4 Side-Channel Secure Implementation

The power of side-channel leakage attacks on cryptographic implementations is evident. Today's practical defenses are typically attack-specific countermeasures against certain classes of side-channel attacks. The demand for a more general solution has given rise to the recent theoretical research that aims to build provably leakage-resilient cryptography. This direction is, however, very new and still largely lacks practitioners' evaluation with regard to both efficiency and practical security. A recent approach, One-Time Programs (OTPs), proposes using Yao's Garbled Circuit (GC) and very simple tamper-proof hardware to securely implement oblivious transfer, to guarantee leakage resilience. The authors of [148] present a generic architecture for using GC/OTP modularly, and a hardware implementation and efficiency analysis of GC/OTP evaluation. They implemented two FPGA-based prototypes: a system-on-a-programmable-chip with access to hardware crypto accelerator (suitable for smartcards and future smartphones), and a stand-alone hardware implementation (suitable for ASIC design). They chose AES as a representative complex function for implementation and measurements. As a result of this work, they are able to understand, evaluate and improve the practicality of employing GC/OTP as a leakage-resistance approach.

Chapter 5

Cryptography for Cloud Computing

The advent of cloud computing is producing a paradigm shift in the whole computing industry. However, it opens up a whole new set of security issues and also provides an opportunity for the deployment of advanced cryptographic algorithms. The main issue is how can one store and compute with data held by a cloud service provider whilst not having full trust in the cloud providers integrity or security? There is a strong link between the problems discussed and those found in MPC, since a key question is how can functions be computed on data which is not held in the clear?

5.1 General Cloud Computing/Storage Protocols

Users increasingly maintain data in the “cloud” at remote storage service providers. Such services allow users to collaborate with each other and to access the shared data from everywhere. It is important to guarantee the integrity of the data when the service is not trusted, and consistent operations in environments where multiple users access the data concurrently. We have developed efficient protocols that provide atomic storage when the service is correct and weaker so-called forking semantics when the server is faulty.

In [204], a service called *Venus* is presented, whose goal is to secure user interaction with untrusted cloud storage. Specifically, Venus guarantees integrity and consistency for applications accessing a key-based object store service, without requiring trusted components or changes to the storage provider. Venus completes all operations optimistically, guaranteeing data integrity. It then verifies operation consistency and notifies the application. Whenever either integrity or consistency is violated, Venus alerts the application. Venus has been implemented and evaluated with the Amazon S3 commodity storage service. The evaluation shows that it adds no noticeable overhead to storage operations.

The work [57] considers a group of mutually trusting clients, who outsource an arbitrary computation service to a remote provider. They do not fully trust the provider, which may also be subject to attacks. The clients do not communicate with each other and would like to verify the integrity of the stored data, the correctness of the remote computation process, and the consistency of the provider’s responses. The work presents a novel protocol that guarantees atomic operations to all clients when the provider is correct and fork-linearizable semantics when it is faulty; this means that all clients which observe each other’s operations are consistent, in the sense that their own operations, plus those operations whose effects they see, have occurred atomically in same sequence. This protocol generalizes previous approaches that provided such guarantees only for outsourced storage services.

5.2 MPC Based Solutions

Secure outsourcing of computation to an untrusted (cloud) service provider is becoming more and more important. Pure cryptographic solutions based on fully homomorphic and verifiable encryption, recently proposed, are promising but suffer from very high latency. Other proposals perform the whole computation on tamper-proof hardware and usually suffer from the the same problem. Trusted computing (TC) is another promising approach that uses trusted software and hardware components on computing platforms to provide useful mechanisms such as attestation allowing the data owner to verify the integrity of the cloud and its computation. However, on the one hand these solutions require trust in hardware (CPU, trusted computing modules) that are under the physical control of the cloud provider, and on the other hand they still have to face the challenge of run-time attestation. In [196] the authors focus on applications where the latency of the computation should be minimized, i.e., the time from submitting the query until receiving the outcome of the computation should be as small as possible. To achieve this they show how to combine a trusted hardware token (e.g., a cryptographic coprocessor or provided by the customer) with Secure Function Evaluation (SFE) to compute arbitrary functions on secret (encrypted) data where the computation leaks no information and is verifiable. The token is used in the setup phase only whereas in the time-critical online phase the cloud computes the encrypted function on encrypted data using symmetric encryption primitives only and without any interaction with other entities.

In [165] the authors look at an application scenario in which the server farm to which the outsourcing is done is equipped with simple trusted modules. The purpose of these trusted modules being to provide “multiplication triples” to each individual server. Thus eliminating the need for a complex offline phase. The modules are shown to be very cheap, and to need to implement only a few simple cryptographic operations.

Diagnostic and classification algorithms play an important role in data analysis, with applications in areas such as health care, fault diagnostics, or benchmarking. Branching programs (BP) is a popular representation model for describing the underlying classification/diagnostics algorithms. Typical application scenarios involve a client who provides data and a service provider (server) whose diagnostic program is run on client’s data. Both parties need to keep their inputs private. In [28] the authors present new, more efficient privacy-protecting protocols for remote evaluation of such classification/diagnostic programs. In addition to efficiency improvements, they generalize previous solutions – they show how to securely evaluate private linear branching programs (LBP), a useful generalization of BP that they introduce. The practical protocols are applied to the privacy-preserving classification of medical ElectroCardioGram (ECG) signals and implementation results are presented. Finally, a subtle security weakness of the most recent remote diagnostic proposal is discovered and fixed, which allowed malicious clients to learn partial information about the program.

5.3 OT Based Solutions

Privacy requirements can come from different sides. Imagine, for example, a DNA database containing information about the purpose of each gene. Such databases are extremely valuable and thus need appropriate cryptographic protection on their content. They are also not sold on a whole, but rather customers are charged per access to the database. On the other hand, the particular DNA sequences accessed by a customer reveal a lot of information about her interests, e.g., for which disease it is developing medication. Moreover, it is quite likely that subscription prices vary with the different species. The authors of [58] propose an oblivious transfer (OT) protocol with access control to address this problem. They consider the case of access to a database where the different records in the database have different access control conditions. These conditions could be certain attributes, roles, or rights that a user needs to have to access the records. The assigning of attributes to users is done by a separate entity called the issuer, external to the database. To provide the maximal amount of privacy, the protocol guarantees that:

- Only users satisfying the access conditions for a record can access that record;
- The service (database) provider does not learn which record a user accesses;
- The service (database) provider shall not learn which attributes, roles, etc. a user has when she accesses a record, i.e., access shall be completely anonymous, nor shall it learn which attributes the user was required to have to access the record.

5.4 FHE Based Solutions

For many years one of the holy-grails of cryptography has been the construction of a fully homomorphic encryption (FHE) scheme. In 2009 this was realised with the presentation of a scheme based on lattices by Gentry [268]. In [206] Smart and Vercauteren present an optimization of Gentry's construction in which ciphertexts consist of only one integer. The authors discuss the security, and relate the security to long standing problems in computational number theory, and also discuss the complexity of the reencryption proceedure in some depth.

It is well known that any encryption scheme which supports any form of homomorphic operation cannot be secure against adaptive chosen ciphertext attack. The question then arises as to what is the most stringent security definition which is achievable by homomorphic encryption schemes. Prior work has shown that various schemes which support a single homomorphic encryption scheme can be shown to be IND-CCA1, i.e. secure against lunchtime attacks. In [164] the authors extend this analysis to the recent fully homomorphic encryption scheme proposed by Gentry, as refined by Gentry, Halevi, Smart and Vercauteren. They show that the basic Gentry scheme is not IND-CCA1; indeed a trivial lunchtime attack allows one to recover the secret key. They then show that a minor modification to the variant of Smart and Vercauteren will allow one to achieve IND-CCA1, indeed PA-1, in the standard model assuming a lattice based knowledge assumption. They end by examining the security of the scheme against another security notion, namely security in the presence of ciphertext validity checking oracles.

In [207] the authors show that the Smart–Vercauteren variant of Gentry's scheme can support SIMD operations. That is when operating homomorphically on a ciphertext the user actually acts homomorphically on vectors of plaintext messages. This is done by using a plaintext space defined by a general cyclotomic polynomial, as opposed to the more specific choice of $X^{2^n} + 1$ in prior works. They discuss how the recryption/bootstrapping method of Gentry can be implemented when SIMD operations are required. In addition they examine a couple of applications of SIMD techniques. In the first they present the homomorphic evaluation of the AES encryption circuit, whereas in the second they examine database lookup procedures.

One key issue with the techniques of [207] is that at first glance it does not appear that the efficient key generation technique introduced by Gentry and Halevi [269] applies in this more general setting. In [202] the authors show that many of the key generation tricks from [269] can be extended to the more general setting of [207]. The authors provide run times of their new key generation methods and compare them across different cyclotomic polynomials.

In [124] the authors extend the SIMD idea of [207] and apply it to the more recent BGV ring-LWE based scheme of [239]. They show that not only does BGV support SIMD addition and multiplication operations, but it also supports homomorphic evaluation of an associated action on the plaintext vectors induced by the Galois action on the underlying cyclotomic field. This enables the authors to establish a scheme which will (asymptotically) evaluate any function homomorphically with only a *polylog* overhead compared to evaluating it in the clear. Albeit the *polylog* overhead comes with a huge implied constant. Despite the theoretical nature of the result, many of the ideas and underlying algebra within this paper can be used to dramatically improve the performance of FHE schemes in practice.

In [125] the prior ideas of [124] are extended even further, and a theoretically efficient bootstrapping procedure is described which makes use of the SIMD nature of the BGV plaintext space. Using the idea of a levelled scheme from [239] the authors use a special modulus for the lowest level, so as to enable a more efficient decryption procedure. The overall algorithm requires only a single ciphertext to represent the bootstrapping information, and it does not rely on assuming an additional assumption as in Gentry's original "squashing" idea.

In [126] the authors take the theoretical scheme from [124] and present a concrete implementation which is able to practically homomorphically evaluate the AES encryption circuit. Along the way they introduce a number of optimization tricks, mainly to reduce memory, including a novel key-switching technique which makes use of a upwards modulus switch which temporarily increases the noise level associated to a ciphertext.

This line of work is continued in [123] where a technique to perform ring-switching is presented. The basic idea is that as a homomorphic operation progresses the large moduli needed at the start of the computation has reduced (due to modulus switching). This means that the large ring needed at the start to ensure security could now be much smaller. This creates the need for a technique to enable one to switch from a large ring to a smaller one. The work in [123] shows how this can be done, whilst still preserving the algebraic "slots" needed for the SIMD performance enhancements.

Following Gentry's result, a conceptually simpler scheme was proposed by van Dijk et al. [257], based on approximate common divisor problems over the integers, rather than decoding problems in ideal lattices. The simplicity of that new scheme came at the expense of a very large public key size, in $\widetilde{O}(\lambda^{10})$ where λ is the security parameter. The authors of [77] reduce the public key size to $\widetilde{O}(\lambda^7)$ by encrypting with a quadratic form in the public key elements, instead of a linear form. They prove that the scheme remains semantically secure, based on a variant of the approximate common divisor problem already considered by van Dijk et al. They also describe an implementation of the resulting scheme, achieving fully homomorphic encryption over the integers for the first time. Borrowing some optimizations from the implementation of Gentry's scheme by Gentry and Halevi [269], they obtain roughly the same level of efficiency.

In [27], the authors propose a cryptographic primitive called Delegatable Homomorphic Encryption (DHE) that moves verifiable outsourcing of computation to the public-key setting.

The idea is that, e.g., a cloud client can delegate to the service provider computation tasks to be performed over encrypted data sent to her by other users, in such a way that the payload remains secret and the results of the computation are verifiable. This was not possible with either homomorphic encryption, functional encryption or secure outsourcing of computation, and DHE can be seen as an extension to each of these primitives. A construction is given by transforming a functional encryption scheme into a verifiable one, and then combining it with an homomorphic encryption scheme.

Chapter 6

New Signature Constructions

Considerable work has been conducted into various aspects of digital signatures, both constructions of schemes with new properties and analysis of the properties of various prior definitions.

6.1 Group Signatures

The authors of [208] provide a construction of an identity based group signature scheme from a HIBE. The construction is generic, but as an example instantiation they use the BBG HIBE. The construction is an application of many of the ideas behind wildcarded and wicked IBE schemes which were developed in the ECRYPT-I project.

The Fiat-Shamir (FS) transform is a popular tool to produce particularly efficient digital signature schemes out of identification protocols. It is known that the resulting signature scheme is secure (in the random oracle model) if and only if the identification protocol is secure against passive impersonators. A similar results holds for constructing ID-based signature schemes out of ID-based identification protocols. The transformation had also been applied to identification protocols with additional privacy properties. So, via the FS transform, ad-hoc group identification schemes yield ring signatures and identity escrow schemes yield group signature schemes. Unfortunately, results akin to those above are not known to hold for these latter settings and the security of the resulting schemes needs to be proved from scratch, or worse, it is often simply assumed. In [155] the authors provide the missing foundations for the use of the FS transform in these more complex settings. They start with defining a formal security model for identity escrow schemes (a concept proposed earlier but never rigorously formalized). The main result constists of necessary and sufficient conditions for an identity escrow scheme to yield (via the FS transform) a secure group signature schemes. In addition, using the similarity between group and ring signature schemes they give analogous results for the latter primitive.

Membership revocation is a crucial issue in group signatures. Group signatures with verifier-local revocation (VLR-GS) deal with it by having the group manager publicize a revocation list containing a revocation token for each revoked user. The revocation list is only used by verifiers and not by signers. Upon verification, it is the verifier's task to make sure that a signature was not generated by a revoked user (if it was, the signer's identity is revealed). In VLR-GS schemes providing backward unlinkability, the lifetime of the scheme is didvided into time periods and signatures that were issued by revoked members before their revocation remain anonymous and unlinkable (which is desirable if users voluntarily leave the group). Using Groth-Sahai proofs, the authors of [162] described a VLR-GS with backward unlinkability in the standard model. Previous VLR-GS were only known to be secure in the random oracle model. The problem to solve was to find an implicit revocation test which is compatible with NIZK proofs in the standard model (as, for certain relations, Groth-Sahai proofs do not always admit NIZK simulators) while enabling backward unlinkability.

In order to deal with the revocation problem in group signatures, the authors of [158, 159] suggested a new method, which is based on the Naor-Naor-Lotspiech (NNL) broadcast encryption framework. This method interacts nicely with the Groth-Sahai techniques for building group signatures in the standard model. In contrast with verifier-local revocation approaches, it gives a constant verification cost and at most polylog complexity (in the maximal number of group members) in other metrics. The initial mechanism [158] had the disadvantage of introducing important storage requirements at group members: membership certificates, which used to have constant size, were inflated to have polylog size in the maximal cardinality of the group. In [159], an improvement was shown to provide private keys of constant size using a new technique to leverage the NNL subset cover framework in the context of group signatures. This refinement yields revocable group signatures that are competitive with ordinary group signatures (i.e., without revocation) in the standard model. As an advantage over approaches that were sometimes used in the past, unrevoked members do not need to update their keys at each revocation.

In [36] the authors present a compact group signature scheme with the shortest known signature size and favorably comparing computation time, whilst still offering a strong and practically relevant security level that guarantees secure opening of signatures, protection against a cheating authority, and support for dynamic groups. Our construction departs from the popular sign-and-encrypt-and-prove paradigm, which we identify as one source of inefficiency. In particular, our proposal does not use standard encryption and relies on rerandomizable signature schemes that hide the signed message so as to preserve the anonymity of signers. Security is proved in the random oracle model assuming the XDDH, LRSW and SDLP assumptions and the security of an underlying digital signature scheme. Finally, we demonstrate how our scheme yields a group signature scheme with verifier-local revocation.

6.2 Blind Signatures

Blind signatures provide a mechanism for achieving privacy and anonymity whereby a user gets the signer to sign a message of his choice without the signer learning the content of the message, nor linking message/signature request pairs when he sees the final signature. In [129] the authors construct a blind signature that requires minimal interaction (two rounds) between the user and the signer. The signature request protocol is akin to the classic, blind-unblind methodology used for RSA blind signatures in the random oracle model. The output signature is a standard Camenisch-Lysyanskaya signature in pairing groups. The scheme is secure in the common reference string model,assuming two discrete logarithm related assumptions in bilinear groups; namely a new variant of the LRSW assumption and the SXDH problem. The authors provide evidence for the hardness of their new variant of the LRSW by showing it is intractable in the generic group model.

In [106], the authors explore the security of blind signatures under aborts where the user or the signer may stop the interactive signature issue protocol prematurely. Several works on blind signatures discuss security only in regard of completed executions and usually do not impose strong security requirements in case of aborts. One of the exceptions is the paper of Camenisch, Neven and shelat [242] where the notion of selective-failure blindness has been introduced. Roughly speaking, selective-failure blindness says that blindness should also hold in case the signer is able to learn that some executions have aborted. Here the authors augment the work of Camenisch et al. by showing how to turn every secure blind signature scheme into a selective-failure blind signature scheme. The transformation only requires an additional computation of a commitment and therefore adds only a negligible overhead. The authors also study the case of multiple executions and notions of selective-failure blindness in this setting. They then discuss the case of user aborts and unforgeability under such aborts. They show that every three-move blind signature scheme remains unforgeable under such user aborts. Together with their transformation for selective-failure blindness the authors thus obtain an easy solution to ensure security under aborts of either party and which is applicable for example to the schemes of Pointcheval and Stern [304]. The authors finally revisit the construction of Camenisch et al. for simulatable adaptive oblivious transfer protocols, starting from selective-failure blind signatures where each message only has one valid signature (uniqueness). While their transformation to achieve selective-failure blindness does not preserve uniqueness, it can still be combined with a modified version of their protocol. Hence, we can derive such oblivious transfer protocols based on unique blind signature schemes only (in the random oracle model), without necessarily requiring selective-failure blindness from scratch.

A fair blind signature is a blind signature with revocable anonymity and unlinkability: an authority can link an issuing session to the resulting signature and trace a signature to the user who requested it. In [115] the authors first strengthen the security model for fair blind signatures by Hufschmitt and Traoré [279]. They then give the first practical fair blind signature scheme with a security proof in the standard model, which moreover satisfies the new model.

Related to blind signatures; in [114] an efficient *blind certification protocol* is proposed. Since it falls in the Groth-Sahai framework for witness-indistinguishable proofs, extended to a certified signature the protocol immediately yields non-frameable group signatures. The blind certification is then used to build an efficient (offline) e-cash system that guarantees user anonymity and transferability of coins without increasing their size. As required for fair e-cash, in case of fraud, anonymity can be revoked by an authority, which is also crucial to deter from double spending.

6.3 Other Privacy Preserving Signature Primitives

In [113], the authors give a generic methodology to unlinkably anonymise cryptographic schemes in bilinear groups using the Boneh-Goh-Nissim cryptosystem and NIZK proofs in the line of Groth, Ostrovsky and Sahai. The techniques are illustrated by presenting the first concrete instantiation of anonymous proxy signatures (in the standard model), a primitive unifying the functionalities and strong security notions of group and proxy signatures. To construct the scheme, the authors introduce various efficient NIZK and witness-indistinguishable proofs.

6.4 Other Signatures With Special Properties

Encrypt-and-sign, where one encrypts and signs a message in parallel, is usually not recommended for confidential message transmission as the signature may leak information about the message. This motivates the investigation in [91] of confidential signature schemes, which hide all information about (high-entropy) input messages. The authors provide a formal treatment of confidentiality for such schemes and give constructions meeting the new notions, both in the random oracle model and the standard model. As part of this it is shown that full domain hash signatures achieve a weaker level of confidentiality than Fiat-Shamir signatures. The authors examine the connection of confidential signatures to signcryption schemes. They give formal security models for deterministic signcryption schemes for high-entropy and low-entropy messages, and prove encrypt-and-sign to be secure for confidential signature schemes and high-entropy messages. Finally, it is shown that one can derandomize any signcryption scheme in the new model and obtain a secure deterministic scheme.

In [193], the authors discuss the concept of verifiably encrypted signatures that was proposed by Boneh et al. at EUROCRYPT 2003 [236] along with a security model. In a verifiably encrypted signature scheme, signers encrypt their signature under the public key of a trusted third party and prove that they did so correctly. This paper proposes two novel fundamental requirements for verifiably encrypted signatures, called extractability and abuse-freeness, and analyzes its effects on the established security model (unforgeability and opacity). Extractability ensures that the trusted third party is always able to extract a valid signature from a valid verifiably encrypted signature and abuse-freeness guarantees that a malicious signer, who cooperates with the trusted party, is not able to forge a verifiably encrypted signature. The authors further show that both properties are not covered by the model of Boneh et al. The second main contribution of the paper is a verifiably encrypted signature scheme, provably secure without random oracles, that is more efficient and greatly improves the public key size of the only other construction in the standard model by Lu et al. (EUROCRYPT 2006) [294]. Moreover, the authors present strengthened definitions for unforgeability and opacity in the spirit of strong unforgeability of digital signature schemes.

Sanitizable signatures allow a signer of a message to give one specific receiver, called a sanitizer, the power to modify some designated parts of the signed message. Most of the existing constructions consider one single signer giving such a possibility to one single sanitizer. In [60], the authors formalize the concept with n signers and m sanitizers, taking into account recent models (for 1 signer and 1 sanitizer) on the subject. They next give a generic construction based on the use of both group signatures and a new cryptographic building block, called a trapdoor or proof, that may be of independent interest.

In [54] the authors revisit the security requirements for sanitizable signatures, which allow a signer to partly delegate signing rights to another party, called the sanitizer. The paper complements the work of Ateniese et al. [221], that identifies five security requirements for such schemes (unforgeability, immutability, privacy, transparency and accountability) but does not provide formal specifications for these properties. This paper presents the first comprehensive formal treatment of the security requirements and also investigates the relationship of the properties. Furthermore, the authors provide a full security proof for a modification of the original scheme by Ateniese et al. according to their model.

In [112] the authors define a general model for consecutive delegations of signing rights with the property that the delegatee actually signing and all intermediate delegators remain anonymous. Similarly to group signatures, in case of misuse, a special authority can open signatures to reveal the chain of delegations and the signer's identity. In this paper, the authors also propose a scheme which satisfies a strong notion of non-frameability generalizing the one for dynamic group signatures. They also give formal definitions of security and show them to be satisfiable by constructing an instantiation proven secure under general assumptions in the standard model. Their primitive is a proper generalization of both group signatures [248] and proxy signatures [295] and can be regarded as non-frameable dynamic hierarchical group signatures.

A modular approach for cryptographic protocols leads to a simple design but often inefficient constructions, while ad hoc constructions may offer efficiency at the cost of losing conceptual simplicity. To overcome this dilemma, Abe et al. [9] present commitments and signatures that enable construction of modular protocols with reasonable efficiency. They focus on schemes in bilinear groups that preserve the group structure, which makes it easy to combine them with other primitives such as Groth-Sahai proofs [275]. A signature scheme is "structure-preserving" if its verification keys, signatures and messages are elements in a bilinear group, and verification consists of checking pairing-product equations; if in addition the verification keys lie in the message space, it is called "automorphic". The authors present several efficient instantiations of automorphic and structure-preserving signatures, enjoying various other properties, such as simulatability. Among many applications, they give three concrete examples: adaptively secure round-optimal blind signatures, group signatures with efficient concurrent join, and efficient anonymous proxy signatures. Another contribution are length-reducing homomorphic trapdoor commitments to group elements, whereas the messages of previous homomorphic trapdoor commitments were exponents.

Randomizable encryption allows anyone to transform a ciphertext into a fresh ciphertext of the same message. Analogously, a randomizable signature can be transformed into a new signature on the same message. Blazy et al. [40] combine randomizable encryption and signatures to a new primitive as follows: given a signature on a ciphertext, anyone can randomize the ciphertext and adapt the signature to the fresh encryption, thus maintaining public verifiability. Moreover, given the decryption key, from a signature on a ciphertext one can compute ("extract") a signature on the encrypted plaintext. As adapting a signature to a randomized encryption contradicts the standard notion of unforgeability, a weaker notion states that no adversary can, after querying signatures on ciphertexts of its choice, output a signature on an encryption of a new message. The authors give several instantiations of their new primitive and prove them secure under classical assumptions in the standard model and the CRS setting. As an application, they show how to construct an efficient non-interactive receipt-free universally verifiable e-voting scheme. In such a scheme a voter cannot prove what his vote was, which precludes vote selling. Besides, the primitive also yields an efficient round-optimal blind signature scheme based on standard assumptions.

Verifiable encryption allows encryption of a signature while preserving its public verifiability. In [110] Fuchsbauer introduces a new primitive called *commuting signatures and verifiable encryption* which extends this in multiple ways, such as enabling to encrypt both a signature and a message and prove validity. More importantly, given a ciphertext, a signer can create a verifiably encrypted signature on the encrypted (unknown) message, which leads to the same result as first signing the message and then verifiably encrypting the pair of message and signature; thus, signing and encrypting commute. His instantiation is based on the recent *automorphic signatures* [9] and the Groth-Sahai proof system, of which he moreover proves a series of useful properties, which could be of independent interest. As an application, the author gives an instantiation of *delegatable anonymous credentials*, which is arguably simpler than previous ones and which is the first to provide *non-interactive* (and thus concurrently secure) issuing and delegation protocols. Moreover, the size of his credentials and the cost of verification are less than half of those of previous instantiations, and efficiency of issuing and delegation is increased even more significantly.

Network coding is a technique providing improved resilience to packet loss and increased throughput. Unlike traditional routing techniques, it allows network nodes to perform transformations on packets they receive before transmitting them. For this reason, packets cannot be authenticated using ordinary digital signatures, which makes it difficult to hedge against pollution attacks, where malicious nodes inject bogus packets in the network. To address this problem, recent works introduced signature schemes allowing to sign linear subspaces (namely, verification can be made w.r.t. any vector of that subspace) and which are well-suited to the network coding scenario. Before 2011, existing network coding signatures in the standard model were not homomorphic in that the signer was forced to sign all vectors of a given subspace at once. In 2011 [21], a piece of ECRYPT-associated work described the first homomorphic network coding signatures in the standard model: in that scheme, the security proof does not use random oracles and, at the same time, the scheme allows signing individual vectors on-the-fly and has constant per-packet overhead in terms of signature size. The construction is based on the dual encryption technique introduced by Waters (Crypto'09) to prove the security of hierarchical identity-based encryption schemes.

Chapter 7

Work on Schemes Related to Identity-Based Encryption

Work on Identity-Based Encryption (IBE) and its associated derivations has continued in the period covered by ECRYPT-2.

7.1 Foundations of Pairings

In [117] the authors discuss, in essentially non-mathematical terms various aspects of instantiation of pairing based protocols. The paper aims to make the various choices for a cryptographic designer clearer, since many of the choices produce subtle impacts not only on the implementation aspects of the scheme, but also upon the the provable security properties which the scheme achieves. This paper introduced the now-standard classification of pairings into Type-1, Type-2 and Type-3 and as such is highly cited. The paper has been highly influential on the presentation of the IEEE standard 1363.3 on pairing based cryptography and Identity Based Cryptography in particular.

7.2 Identity Based Encryption

Identity-Based Encryption offers an interesting alternative to PKI-enabled encryption as it eliminates the need for digital certificates. While revocation has been thoroughly studied in PKIs, few revocation mechanisms are known in the IBE setting. Until quite recently, the most convenient one was to augment identities with period numbers at encryption. All non-revoked receivers were thus forced to obtain a new decryption key at discrete time intervals, which places a significant burden on the authority. A more efficient method was suggested by Boldyreva, Goyal and Kumar at CCS'08 [233]. In their revocable IBE scheme, key updates have logarithmic (instead of linear in the original method) complexity for the trusted authority. Unfortunately, security could only be proved in the selective-ID setting where adversaries have to declare which identity will be their prey at the very beginning of the attack game. In [161] the authors describe an adaptive-ID secure revocable IBE scheme and thus solve a problem left open by Boldyreva et al.

Identity-based encryption is a very convenient tool to avoid key management. To address concerns about the privacy of a recipient, the notion of anonymous identity-based encryption has been proposed. In [142] the authors extend this notion to stronger adversaries (the authority itself). In particular, the authors discuss this new notion, together with a new kind of non-malleability with respect to the identity, for several existing schemes. Interestingly, the authors show that such a new anonymity property has an independent application to password-authenticated key exchange, by providing a new generic framework for it along with a concrete construction based on pairings.

In [182], the authors investigate the relationships between identity-based non-interactive key distribution and identity-based encryption. The authors provide constructions for these schemes that make use of general trapdoor discrete log groups. The authors then investigate the schemes that result in two concrete settings, obtaining new, provably secure, near-practical identity-based encryption schemes.

In [180], the authors consider the security of Identity-Based Encryption (IBE) in the setting of multiple Trusted Authorities (TAs). In this multi-TA setting, the authors envisage multiple TAs sharing some common parameters, but each TA generating its own master secrets and master public keys. The authors provide security notions and security models for the multi-TA setting which can be seen as natural extensions of existing notions and models for the single-TA setting. In addition, the authors study the concept of TA anonymity, which formally models the inability of an adversary to distinguish two ciphertexts corresponding to the same message and identity but generated using different TA master public keys. The authors argue that this anonymity property is a natural one of importance in enhancing privacy and limiting traffic analysis in multi-TA environments. The authors study a modified version of a Fujisaki-Okamoto conversion in the multi-TA setting, proving that their modification lifts security and anonymity properties from the CPA to the CCA setting. Finally, the authors apply these results to study the security of the Boneh-Franklin and Sakai-Kasahara IBE schemes in the multi-TA setting.

In [181], the authors extend the examination of the implications of TA anonymity for key-privacy from IBE to normal public-key encryption (PKE) schemes. Key-privacy for PKE captures the requirement that ciphertexts should not leak any information about the public-keys used to perform encryptions. Thus key-privacy guarantees recipient anonymity for a PKE scheme. Canetti, Halevi and Katz (CHK) gave a generic transform which constructs an IND-CCA secure PKE scheme using an identitybased encryption (IBE) scheme that is selective-id IND-CPA secure and a strongly secure one-time signature scheme. Their transform works in the standard model (i.e. does not require the use of random oracles). Here, the authors prove that if the underlying IBE scheme in the CHK transform is TA anonymous, then the resulting PKE scheme enjoys key-privacy. Whilst IND-CCA secure, key-private PKE schemes are already known in the standard-model, their result gives the first generic method of constructing a key-private PKE scheme in the standard model. The authors then go on to investigate the TA anonymity of multi-TA versions of well-known standard model secure IBE schemes. In particular, the authors prove the TA anonymity and selective-id IND-CPA security of a multi-TA version of Gentry's IBE scheme. Applying the CHK transform, the authors obtain a new, efficient key-private, IND-CCA secure PKE scheme in the standard model.

At Crypto'07, Goyal [273] introduced the concept of Accountable Authority Identity-Based Encryption as a convenient tool to reduce the amount of trust in authorities in Identity-Based Encryption. In this model, if the Private Key Generator (PKG) maliciously re-distributes users' decryption keys, it runs the risk of being caught and prosecuted. Goyal proposed two constructions: the first one is efficient but can only trace well-formed decryption keys to their source; the second one allows tracing obfuscated decryption boxes in a model (called weak black-box model) where cheating authorities have no decryption oracle. The latter scheme is unfortunately far less efficient in terms of decryption cost and ciphertext size. In [160] the authors describe a new construction that combines the efficiency of Goyal's first proposal with a very simple weak black-box tracing mechanism. The proposed scheme is presented in the selective-ID model but readily extends to meet all security properties in the adaptive-ID sense, which is not known to be true for prior black-box schemes.

In [5] the authors propose a methodology to construct verifiable random functions [297] from a class of identity based key encapsulation mechanisms (IB-KEM) [229] that they call VRF suitable. Informally, an IB-KEM is VRF suitable if it provides what is called *unique decryption* (i.e. given a ciphertext C produced with respect to an identity ID, all the secret keys corresponding to identity ID', decrypt to the same value, even if $ID \neq ID'$) and it satisfies an additional property that the authors call pseudorandom decapsulation. In a nutshell, pseudorandom decapsulation means that if one decrypts a ciphertext C, produced with respect to an identity ID, using the decryption key corresponding to any other identity ID' the resulting value looks random to a polynomially bounded observer. Interestingly, the authors show that most known IB-KEMs already achieve pseudorandom decapsulation. Their construction is of interest both from a theoretical and a practical perspective. Indeed, apart from establishing a connection between two seemingly unrelated primitives, their methodology is *direct* in the sense that, in contrast to most previous constructions, it avoids the inefficient Goldreich-Levin hardcore bit transformation [271].

Lewko and Waters [292] presented a fully secure HIBE with short ciphertexts. In [84], the authors show how to modify their construction to achieve anonymity. They prove the security of their scheme under static (and generically secure) assumptions formulated in composite order bilinear groups. In addition, in [84], the authors present a fully secure Anonymous IBE in the secret-key setting. Secret-Key Anonymous IBE was implied by the work of [311] which can be shown secure in the selective-id model. No previous fully secure construction of secret-key Anonymous IBE is known.

The paper [13] presents collusion attacks against a recently proposed Identity-based encryption scheme due to Chen et al.. The attacks recover the master secret key of the scheme and thereby invalidate the existing security analysis of this scheme. The attacks are flexible, allowing, for example, the amount of computation needed to be traded-off against the size of the collusion

7.3 Certificateless Encryption

In [90] the author examines the relationship between certificateless encryption schemes and traditional PKI structures. Certificateless encryption schemes are classified into three classes based on the way in which a user's secret decryption key is developed – these are termed AP, BSS and LK certificateless encryption schemes after their original inventors. The author demonstrates that secure BSS and LK certificateless encryption schemes can be constructed using a traditional PKI-based public-key encryption system, while noting that AP certificateless encryption schemes cannot be constructed from an arbitrary public-key encryption scheme in any black-box fashion.

7.4 Certified Encryption

The notion of certified encryption [46] had recently been suggested as a suitable setting for analyzing the security of encryption against adversaries that tamper with the key-registration process. The flexible syntax afforded by certified encryption suggests that identity-based [235] and certificateless [255] encryption schemes can be analyzed using the models for certified encryption. In [93] the authors explore the relationships between security models for these two primitives and that for certified encryption. The following results are obtained. The authors show that an identity-based encryption scheme is secure if and only if it is secure when viewed as a certified encryption scheme. This result holds under the (unavoidable) restriction that registration occurs over private channels. In the case of certificateless encryption it is observed that a similar result cannot hold. The reason is that existent models explicitly account for attacks against the non-monolithic structure of the secret keys whereas certified encryption models treat secret keys as whole entities. The paper proposes an extension for certified encryption where the adversary is allowed to partially modify the secret keys of honest parties. The extension that the authors propose is very general and may lead to unsatisfiable notions. Nevertheless, they exhibit one instantiation for which they can prove the desired result: a certificateless encryption is secure if and only if its associated certified encryption scheme is secure. As part of the analysis, and a result of separate interest this paper confirms the folklore belief that for both IBE and CLE, security in the single-user setting (as captured by existent models) is equivalent to security in the multi-user setting.

7.5 Identity Based Key Agreement

In [101] the authors present a new identity based key agreement protocol. In id-based cryptography (introduced by Adi Shamir in [308]) each party uses its own identity as public key and receives his secret key from a master Key Generation Center, whose public parameters are publicly known. The novelty of this protocol is that it can be implemented over any cyclic group of prime order, where the Diffie-Hellman problem is supposed to be hard. It does not require the computation of expensive bilinear maps, or additional assumptions such as factoring or RSA. The protocol is extremely efficient, requiring only twice the amount of bandwith and computation of the *unauthenticated* basic Diffie-Hellman protocol. The design of their protocol was inspired by MQV (the most efficient authenticated Diffie-Hellman based protocol in the public-key model) and indeed its performance is competitive with respect to MQV (especially when one includes the transmission and verification of certificates in the MQV protocol, which are not required in an id-based scheme). The proposed protocol requires a single round of communication in which each party sends only 2 group elements: a very short message, especially when the protocol is implemented over elliptic curves. The paper provides a full proof of security in the Canetti-Krawczyk security model for key exchange, including a proof that the protocol satisfies additional security properties such as perfect forward secrecy, and resistance to reflection and key-compromise impersonation attacks.

In [102] motivated by the previous work the authors examine the linkage between ID-based key agreement and certificateless encryption. The authors show generic transforms from ID-based key agreement to certificateless encryption. This work highlights a number of issues related to the different security requirements for both key agreement and certificateless encryption. It thus further enforces the view, explored in a number of papers, that the definition of security in both scenarios is a complex affair.

Chapter 8

Other Schemes and Protocols

8.1 Key Exchange and Key Agreement

Adaptively-secure key exchange allows the establishment of secure channels even in the presence of an adversary that can corrupt parties adaptively and obtain their internal states. In [4], the authors give a formal definition of contributory protocols and define an ideal functionality for password-based group key exchange with explicit authentication and contributiveness in the UC framework. As with previous definitions in the same framework, their definitions do not assume any particular distribution on passwords or independence between passwords of different parties. The authors also provide the first steps toward realizing this functionality in the above strong adaptive setting by analyzing an efficient existing protocol and showing that it realizes the ideal functionality in the random-oracle and ideal-cipher models based on the CDH assumption.

In ASIACRYPT 2005, Abdalla *et al.* [218] put forward the notion of gateway-based password-authenticated key exchange (GPAKE) protocol, which allows clients and gateways to establish a common session key with the help of an authentication server. In addition to the semantic security of the session key, their solution also provided additional security properties such as password protection with respect to malicious gateways and key privacy with respect to curious authentication servers. In [8] the authors further pursued this line of research and presented a new and stronger security model for GPAKE schemes, combining all above-mentioned security properties. In addition to allowing a security proof for all these security properties, the new security model has also other advantages over the previous one such as taking into account user corruptions. After describing the new security model, this paper then presents a new variant of the GPAKE scheme of Abdalla *et al.* with similar efficiency. Like the original scheme, the new scheme is also *transparent* in that it does not differ significantly from a classical PAKE scheme from the point of view of a client. Finally, this paper also shows how to add client anonymity with respect to the server to the basic GPAKE scheme by using private information retrieval protocols.

In [166] the author extends the classical notion of group key exchange (GKE) protocols by a new property that allows each pair of users to derive an independent peer-to-peer (p2p) key on-demand and without any subsequent communication; this, in addition to the classical group key shared amongst all the users. GKE protocols enriched in this way impose new security challenges concerning the secrecy and independence of both key types; a special attention is paid to possible collusion attacks aiming to break the secrecy of p2p keys possibly established between any two non-colluding users. The proposed constructions utilize the well-known parallel Diffie-Hellman key exchange (PDHKE) technique in which each party uses the same exponent for the computation of p2p keys with its peers. First, PDHKE is considered in GKE protocols where parties securely transport their secrets for the establishment of the group key based on an efficient multi-recipient ElGamal encryption scheme. Further, PDHKE is used to design a generic compiler for GKE protocols that extend the classical Diffie-Hellman method. The paper finally investigates possible optimizations of such protocols allowing parties to re-use their exponents to compute both group and p2p keys. The analysis shows that not all such GKE protocols can be optimized.

In [7], the authors generalize the notion of group key exchange protocols, enabling on-demand derivation of peer-to-peer keys in order to allow efficient derivation of independent secret keys for all potential subsets. In particular, they show how a group of users can agree on a secret group key while obtaining some additional information that they can use on-demand to efficiently compute independent secret keys for any possible subgroup. The security analysis relies on the Gap Diffie-Hellman assumption and uses random oracles.

So far, all solutions proposed for authenticated key agreement combine key agreement and authentication into a single cryptographic protocol. However, in many important application scenarios, key agreement and entity authentication are clearly separated protocols. This fact enables efficient attacks on the naive combination of these protocols. In [144] new compilers are proposed for two-party key agreement and authentication, which are provably secure in the standard Bellare-Rogaway model [228]. The constructions are generic: key agreement is executed first and results (without intervention of the adversary) in a secret session key on both sides. This key (or a derived key) is handed over, together with a transcript of all key exchange messages, to the authentication protocol, where it is combined with the random challenge(s) exchanged during authentication.

In [56] the authors examine composability properties for the fundamental task of key exchange. The main result is to show that key exchange protocols secure in the prevalent model of Bellare and Rogaway [228] can be composed with arbitrary protocols that require symmetrically distributed keys. This composition theorem holds if the key exchange protocol satisfies an additional technical requirement that our analysis brings to light: it should be possible to determine which sessions derive equal keys given only the publicly available information. An important characteristic of the results in the paper is that they use a game-based formalism (thus do not rely on simulation).

8.2 Key Assignment

In [109] the authors provide constructions for key assignment schemes that are provably secure under the factoring assumption in the standard model. Their first construction is for simple "chain" hierarchies, and achieves security against key recovery attacks with a tight reduction from the problem of factoring integers of a special form. Their second construction applies for general hierarchies, achieves the stronger notion of key indistinguishability, and has security based on the hardness of factoring Blum integers. The authors compare their constructions to previous schemes, in terms of security and efficiency.

8.3 Deriving Keys From Biometric Data

The paper [52] introduces a new way of generating strong keys from biometric data. Contrary to popular belief, the new method leads to biometric keys which are easy to obtain and renew. Their solution is based on two-factor authentication, involving a low-cost card and a biometric trait. In particular, this paper introduces a new biometric-based remote authentication scheme following the Boneh and Shacham group signature construction [237]. Surprisingly, no interaction with a biometric database is needed in an ordinary use of this scheme. One side effect of new proposal is that users will remain private, though their privacy can be removed, for instance, under a legal warrant.

8.4 Hybrid-Encryption

In [151] the authors present a new approach to the design of IND-CCA secure hybrid encryption schemes in the standard model. The approach revolves around a new and efficient generic transformation from 1-universal to 2-universal hash proof systems. The transformation involves a randomness extractor based on a 4-wise independent hash function as the key derivation function. The new methodology can be instantiated with efficient schemes based on standard intractability assumptions such as Decisional Diffie-Hellman, Quadratic Residuosity, and Paillier's Decisional Composite Residuosity. The authors also user their framework to prove IND-CCA security of a hybrid version of 1991's Damgård's ElGamal public-key encryption scheme under the DDH assumption.

8.5 Predicate and Attribute Based Encryption

Predicate encryption is a new powerful cryptographic primitive which allows for fine-grained access control for encrypted data: the owner of the secret key can release partial keys, called *tokens*, that can decrypt only a specific subset of ciphertexts. More specifically, in a predicate encryption scheme, ciphertexts and tokens have attributes and a token can decrypt a ciphertext if and only if a certain predicate of the two associated attributes holds.

In [2] a restricted variant of predicate and attribute based encryption is presented, namely a primitive called identity-based encryption with wildcards, or WIBE for short. It allows a sender to encrypt messages to a whole range of receivers whose identities match a certain pattern. This pattern is defined through a sequence of fixed strings and wildcards, where any string can take the place of a wildcard in a matching identity. Our primitive can be applied to provide an intuitive way to send encrypted email to groups of users in a corporate hierarchy. We propose a full security notion and give efficient implementations meeting this notion under different pairing-related assumptions, both in the random oracle model and in the standard model.

In [140, 42] the authors propose a new predicate encryption scheme relative to the predicate hidden vector encryption, which is more efficient that previous constructions. Predicate encryption schemes are encryption schemes in which each ciphertext Ct is associated with a binary attribute vector and keys K are associated with predicates. A key K can decrypt a ciphertext if and only if the attribute vector of the ciphertext satisfies the predicate of the key. Predicate encryption schemes can be used to implement fine-grained access control on encrypted data and to perform search on encrypted data. Hidden vector encryption schemes

[238] are particular predicate encryption schemes in which each ciphertext is associated with a binary vector and each key K is associated with binary vector with "don't care" entries (denoted with $\star$). Key K can decrypt ciphertext if and only if and agree for all i for which $y_i \neq \star$. Hidden vector encryption schemes are an important type of predicate encryption schemes as they can be used to construct more sophisticated predicate encryption schemes (supporting for example range and subset queries). The authors give a construction for hidden-vector encryption from standard complexity assumptions on bilinear groups of prime order. Previous constructions were in bilinear groups of composite order and thus resulted in less efficient schemes. Furthermore this new construction does not assume difficulty of factoring, but only relies on the difficulty of the Decision Linear Assumption.

Various security notions are relevant for predicate encryption schemes. First of all, one wants the ciphertexts to hide its attributes (this property is called semantic security). In addition, it makes sense also to consider the property of token security, a security notion in which the token is required not to reveal any information on the associated pattern. It is easy to see that predicate privacy is impossible to achieve in a public-key setting. In [311], the authors considered the notion of a predicate encryption scheme in the symmetric-key setting and gave the first construction with token security. In [43], the authors consider the notion of a partial public key encryption (as suggested in [311]) in which a partial public key allows a user to generate only a subset of the ciphertexts, for hidden-vector encryption [238]. They give a construction which is semantically secure and in which a token does not reveal any information on the associated pattern except for the locations of the $\star$'s. The proofs of security of their construction are based on hardness assumptions in bilinear groups of prime order in standard model. This greatly improves the efficiency of the construction when compared to previous constructions [311] which used groups of composite orders.

In [85] the authors give *fully secure* implementations of encryption schemes for binary Conjunctions and Disjunctions and k-CNF/DNF. For conjunctions they adhere to the standard terminology of *hidden vector encryption* (or HVE in short) as introduced by [238]. The constructions for Disjunctions and Conjunctions are linear in the number of variables. Previous fully secure constructions for Disjunction required time exponential in the number of variables while for Conjunctions the best previous construction was quadratic in the number of variables. The full security is proved under non-interactive constant sized assumptions on bilinear groups of composite order.

A hidden vector encryption scheme (HVE) is a derivation of identity-based encryption, where the public key is actually a vector over a certain alphabet. This was introduced by Boneh and Waters [238] and further developed in [312, 140]. The decryption key is also derived from such a vector, but this one is also allowed to have wildcard entries. Decryption is possible as long as these tuples agree on every position except where a wildcard occurs. These schemes are useful for a variety of applications: they can be used as a building block to construct attribute-based encryption schemes and sophisticated predicate encryption schemes (for e.g. range or subset queries). Another interesting application is to create searchable encryption schemes that support queries for keywords containing wildcards. The authors of [203] construct a new HVE scheme, based on bilinear groups of prime order, which supports vectors over any alphabet. The resulting ciphertext length is equally shorter than existing schemes, depending on a trade-off. The length of the decryption key and the computational complexity of decryption are both constant, unlike existing schemes where these are both dependent on the amount of non-wildcard symbols associated to the decryption key. The scheme hides both the plaintext and the public key used for encryption and it is proven secure in a selective model, under the decision linear assumption.

In [86] the authors alsoconsider hidden vector encryption. In a HVE scheme, the ciphertext attributes are vectors $\vec{x} = \langle x_1, \ldots, x_\ell \rangle$ of length ℓ over alphabet Σ, keys are associated with vectors $\vec{y} = \langle y_1, \ldots, y_\ell \rangle$ of length ℓ over alphabet $\Sigma \cup \{\star\}$ and we consider the $\mathsf{Match}(\vec{x}, \vec{y})$ predicate which is true if and only if, for all i, $y_i \neq \star$ implies $x_i = y_i$. HVE can be used as building block for several other predicates. Specifically in [238], it is shown that HVE implies predicate encryption schemes for conjunctions, comparison, range queries and subset queries. The authors describe also constructions of secure predicate encryption for Boolean predicates that can be expressed as k-CNF and k-DNF (for any constant k). Fully secure constructions of HVE can be derived, via the reduction given in [287], from the fully secure constructions for inner-product encryption given by [302] on bilinear groups of prime order. However, this reduction doubles the number of pairing computations needed to evaluate the HVE predicate. Instead, the authors in [86] give direct implementation of the HVE primitive and as in [302] their construction poses no restriction on the queries that adversaries can ask. The scheme can be proved *fully* secure against *unrestricted* queries by probabilistic polynomial-time adversaries under non-interactive constant sized (that is, independent of the length ℓ of the attribute vectors) hardness assumptions on bilinear groups of composite order. Their proof employs the dual system methodology of Waters [314], that gave one of the first fully secure construction in this area, blended with a careful design of intermediate security games that keep into account the relationship between challenge ciphertexts and key queries.

Attribute-based encryption (ABE), as introduced by Sahai and Waters, allows for fine-grained access control on encrypted data. In its key-policy flavor, ABE enables senders to encrypt messages under a set of attributes and private keys are associated with access structures that specify which ciphertexts the key holder will be allowed to decrypt. In most ABE systems, the ciphertext size grows linearly with the number of ciphertext attributes and the only known exceptions only support restricted forms of threshold access policies. In [22], ECRYPT-associated researchers proposed the first key-policy attribute-based encryption (KP-ABE) schemes allowing for non-monotonic access structures (i.e., that may contain negated attributes) and with constant ciphertext size. The downside of this new constructions is that private keys have quadratic size in the number of attributes. On the other hand, it reduces the number of pairing evaluations to a constant, which appears to be a unique feature among expressive KP-ABE schemes.

In attribute-based signatures, each user receives from an authority a secret key as a function of his atributes, which informally, can be thought as describing his role within an organization. Users may then sign messages for any policy satisfied by their attributes. The signature will convice a verifier of the fact that the signer's attributes satisfy the signing predicate while remaining completely ignorant of the identity of the signer. For this reason, attribute-based signatures is a natural solution for fine-grained access control with respect to security policies, for instance. In [HLLR12], the authors proposed the first two attribute-based signature schemes with constant size signatures for threshold signing policies, but extendable also to more general kinds of monotone predicates. In many scenarios where authentication and anonymity are required, like distributed access control mechanisms in ad hoc networks, the bandwidth is a crucial and sensitive concern and the signature size of all previous ABS schemes grows linearly in the number of attributes involved in the signing predicate. The security of the proposed schemes is proven in the selective-predicate and adaptive-message setting, in the standard model, under chosen message attacks, with respect to some algorithmic assumptions related to bilinear groups.

8.6 Time Based Encryption

In [178], the authors introduce and explore the new concept of Time-Specific Encryption (TSE). In (Plain) TSE, a Time Server broadcasts a key at the beginning of each time unit, a Time Instant Key (TIK). The sender of a message can specify any time interval during the encryption process; the receiver can decrypt to recover the message only if it has a TIK that corresponds to a time in that interval. The concept of Plain TSE is extended to the public-key and identity-based settings, where receivers are additionally equipped with private keys and either public keys or identities, and where decryption now requires the use of the private key as well as an appropriate TIK. The paper [178] introduces security models for the plain, public-key and identity-based settings. It also provides constructions for schemes in the different settings, showing how to obtain Plain TSE using identity-based techniques, how to combine Plain TSE with public-key and identity-based encryption schemes, and how to build schemes that are chosen-ciphertext secure from schemes that are chosen-plaintext secure. Finally, applications are suggested for the new primitive, and its relationships with existing primitives, such as Timed-Release Encryption and Broadcast Encryption, are discussed.

8.7 Puzzles and Prevention of DDoS Attacks

In [70] the authors present security definitions for client puzzles. Client puzzles have been proposed for use to prevent denial-of-service attacks, however up until this paper they have had no formal definitional treatment. The authors present two security notions, one related to unforgability of the puzzle and one related to how difficult the puzzle is to solve. They then demonstrate that puzzles that do not meet their definition do not necessarily provide a defence against denial-of-service attacks. Finally, present constructions of puzzles which meet their security definitions and the authors also show that some previous constructions do not meet their definitions.

8.8 Broadcast Encryption

In [189], the authors clarify the relationships between security notions for broadcast encryption. In the past, each new scheme came with its own definition of security, which made them hard to compare. In the spirit of similar work done for signature and encryption, the authors define a set of security notions for which they prove implications and separations, and relate the existing notions to the ones in their framework. They find some interesting relationships between the various notions, especially in the way these notions define the receiver set of the challenge message. In addition, the authors define a security notion that is stronger than all previous ones, and give an example of a scheme that fulfills this notion.

In [157] the authors consider anonymity in the context of broadcast encryption (BE). This issue has received very little attention so far and all but one of the currently available BE schemes fail to provide anonymity. Yet, it is intrinsically desirable to provide anonymity in standard applications of BE and this can be achieved at a moderate cost. The authors provide a security definition for Anonymous Broadcast Encryption (ANOBE) and show that it is achievable assuming only the existence of IND-CCA secure public key encryption (PKE). Focusing on reducing the size of ciphertexts, they give two generic constructions for ANOBE. The first is from any anonymous (key-private) IND-CCA secure PKE scheme, and the second is from any IBE scheme that satisfies a weak security notion in the multi-TA setting. Furthermore, the authors show how randomness re-use techniques can be deployed in the ANOBE context to reduce computational and communication costs, and how a new cryptographic primitive – anonymous hint systems – can be used to speed up the decryption process in our ANOBE constructions. Finally, the authors present a slightly modified version of the Kurosawa-Desmedt (KD) PKE scheme (establishing several results about this scheme that may be of independent interest) and use it to instantiate our first main construction, yielding the currently most efficient ANOBE scheme. All of the results are in the standard model, achieving fully collusion-resistant ANOBE schemes secure against adaptive IND-CCA adversaries.

In [188], the authors consider designing broadcast encryption schemes with constant-size secret keys and ciphertexts, achieving chosen-ciphertext security. They rst argue that known CPA-to-CCA transforms currently do not yield such schemes. They then propose a scheme, modifying a previous selective CPA secure proposal by Boneh, Gentry, and Waters. The proposed scheme has constant-size secret keys and ciphertexts and they prove that it is selective chosen-ciphertext secure based on standard assumptions. The scheme has ciphertexts that are shorter than those of the previous CCA secure proposals. The authors then propose a second scheme that provides the functionality of both broadcast encryption and revocation schemes simultaneously using the same set of parameters. Finally they show that it is possible to prove the rst scheme adaptive chosen-ciphertext secure under reasonable extensions of the bilinear Diffie-Hellman exponent and the knowledge of exponent assumptions. They prove both of these extended assumptions in the generic group model. Hence, their scheme becomes the first to achieve constant-size secret keys and ciphertexts (both asymptotically optimal) and adaptive chosen-ciphertext security at the same time.

A broadcast encryption system generally involves three kinds of entities: the group manager that deals with the membership, the encryptor that encrypts the data to the registered users according to a specific policy (the target set), and the users that decrypt the data if they are authorized by the policy. Public-key broadcast encryption can be seen as removing this special role of encryptor, by allowing anybody to send encrypted data. In [190], the authors go a step further in the decentralization process, by removing the group manager: the initial setup of the group, as well as the addition of further members to the system, do not require any central authority. The construction makes black-box use of well-known primitives and can be considered as an extension to the subset-cover framework. It allows for efficient concrete instantiations, with parameter sizes that match those of the subset-cover constructions, while at the same time achieving the highest security level in the standard model under the DDH assumption.

Traitor tracing is an important tool to discourage defrauders from illegally broadcasting multimedia content. However, the main techniques consist in tracing the traitors from the pirate decoders they built from the secret keys of dishonest registered users: with either a black-box or a white-box tracing procedure on the pirate decoder, one hopes to trace back one of the traitors who registered in the system. But new techniques for pirates consist either in sending the ephemeral decryption keys to the decoders for real-time decryption, or in making the full content available on the web for later viewing. This way, the pirate does not send any personal information. In order to be able to trace the traitors, one should embed some information, or watermarks, in the multimedia content itself to make it specific to the registered users. The paper [191] addresses this problem of tracing traitors from the decoded multimedia content or rebroadcasted keys, without increasing too much the bandwidth requirements. More precisely, the authors construct a message-traceable encryption scheme that has an optimal ciphertext rate, i. e. the ratio of global ciphertext length over message length is arbitrarily close to one.

8.9 e-Cash

Electronic cash (e-cash) refers to money exchanged electronically. The main features of physical cash are also desirable in the context of e-cash. One such property is *off-line transferability*, meaning the recipient of a coin can transfer it to a third person without contacting a central authority. Among security properties, anonymity of the payer in transactions has been widely studied. Blazy et al. [38] propose the first efficient and secure transferable e-cash scheme with the strongest achievable anonymity properties, introduced by Canard and Gouget. In particular, it should not be possible for adversaries who receive a coin to decide whether they have owned the coin before. This new scheme is based on two recent cryptographic primitives: the proof system by Groth and Sahai, whose randomizability enables strong anonymity, and the commuting signatures [110] by Fuchsbauer, which allow one to sign values that are only given as encryptions.

8.10 Keyword Search

In [59] Canard et al. study the problem of searching on encrypted data, where the search is performed using a plaintext message or a keyword, rather than a message-specific trapdoor as done by state-of-the-art schemes. The use cases include delegation of key-word search e.g. to a cloud data storage provider or to an email server, using a plaintext message. The paper introduces a new cryptographic primitive called *plaintext-checkable encryption* (PCE), which extends public-key encryption by the following functionality: given a plaintext, a ciphertext and a public key, anyone can check whether the ciphertext encrypts the plaintext under the key. The authors provide efficient generic random oracle constructions for PCE based on any probabilistic or deterministic encryption scheme; and they give a practical construction in the standard model. As another application it is shown how PCE can be used to improve the efficiency in group signatures with *verifier-local revocation* (VLR) and backward unlinkability. These group signatures provide efficient revocation of group members, which is a key issue in practical applications.

In a public key setting, Alice encrypts an email with the public key of Bob, so that only Bob will be able to learn the contents of the email. Consider a scenario where the computer of Alice is infected and unbeknown to Alice it also embeds a malware into the message. Bob's company, Carol, cannot scan his email for malicious content as it is encrypted so the burden is on Bob to do the scan. This is not efficient. In [139] the authors construct a mechanism that enables Bob to provide trapdoors to Carol such that Carol, given an encrypted data and a malware signature, is able to check whether the encrypted data contains the malware signature, without decrypting it. They refer to this mechanism as public-key encryption with delegated search (PKEDS). They give a construction based on ElGamal publickey encryption (PKE). The proposed scheme has ciphertexts which are both searchable and decryptable. This property of the scheme is crucial since an entity can search the entire content of the message, in contrast to existing searchable public-key encryption schemes where the search is done only in the metadata part. It is proven in the standard model that the scheme is ciphertext indistinguishable and trapdoor indistinguishable under the Symmetric External Diffie-Hellman (SXDH) assumption. The ciphertext one-wayness of the scheme is proven under the modified Computational Diffie-Hellman (mCDH) assumption. The authors show that the PKEDS scheme can be used in different applications such as detecting encrypted malware and forwarding encrypted email.

8.11 Anonymity Preserving Protocols

Anonymous credentials are protocols in which users obtain certificates from organizations and subsequently demonstrate their possession in such a way that transactions carried out by the same user cannot be linked. In [141] the authors present an anonymous credential scheme with non-interactive proofs of credential possession where credentials are associated with a number of attributes. Following recent results of Camenisch and Groß (CCS 2008), the proof simultaneously convinces the verifier that certified attributes satisfy a certain predicate. The construction relies on a new kind of P-signature, termed block-wise P-signature, that allows a user to obtain a signature on a committed vector of messages and makes it possible to generate a short witness that serves as a proof that the signed vector satisfies the predicate. A non-interactive anonymous credential is obtained by combining the block-wise P-signature scheme with the Groth-Sahai proof system. It allows efficiently proving possession of a credential while simultaneously demonstrating that underlying attributes satisfy a predicate corresponding to the evaluation of inner products (and therefore disjunctions or polynomial evaluations). The security of the proposed scheme is proved in the standard model under non-interactive assumptions.

Anonymous communication protocols must achieve two seemingly contradictory goals: *privacy* (informally, they must guarantee the anonymity of the parties that send/receive information), and *robustness* (informally, they must ensure that the messages are not tampered). However, the long line of research that defines and analyzes the security of such mechanisms focuses almost exclusively on the former property and ignores the latter. In [29] we initiate the rigorous study of robustness properties by identifying and formally defining two related but distinct flavors of robustness. The proposed definitions are general (*e.g.* they strictly generalize the few existent notions for particular protocols) and flexible (*e.g.* they can be easily adapted to purely combinatorial/probabilistic mechanisms). The utility of the definitions is demonstrated by analyzing several anonymity mechanisms: Crowds [305], broadcast-based mix-nets [219], Tor [258], and the solution for the dining cryptographer's problem proposed by Golle and Juels [272]

The notion of key privacy for asymmetric encryption schemes was formally defined by Bellare, Boldyreva, Desai and Pointcheval in 2001: it states that an eavesdropper in possession of a ciphertext is not able to tell which specific key, out of a set of known public keys, is the one under which the ciphertext was created. Since anonymity can be misused by dishonest users, some situations could require a tracing authority capable of revoking key privacy when illegal behavior is detected. Prior works on traceable anonymous encryption miss a critical point: an encryption scheme may produce a covert channel which malicious users can use to communicate illegally using ciphertexts that trace back to nobody or, even worse, to some honest user. In [143], the authors examine subliminal channels in the context of traceable anonymous encryption and they introduce a new primitive termed mediated traceable anonymous encryption that provides confidentiality and anonymity while preventing malicious users to embed subliminal messages in ciphertexts. In their model, all ciphertexts pass through a mediator (or possibly several successive mediators) and their goal is to design protocols where the absence of covert channels is guaranteed as long as the mediator is honest, while semantic security and key privacy hold even if the mediator is dishonest. The authors give security definitions for this new primitive and constructions meeting the formalized requirements. Their generic construction is fairly efficient, with ciphertexts that have logarithmic size in the number of group members, while preventing collusions. The security analysis requires classical complexity assumptions in the standard model.

8.12 Password Based Cryptography

The paper [3] introduces the notion of distributed password-based public-key cryptography, where a virtual high-entropy private key is implicitly defined as a concatenation of low-entropy passwords held in separate locations. The users can jointly perform private-key operations by exchanging messages over an arbitrary channel, based on their respective passwords, without ever sharing their passwords or reconstituting the key. Focusing on the case of ElGamal encryption as an example, this paper starts by formally defining ideal functionalities for distributed public-key generation and virtual private-key computation in the UC model [243]. It then constructs efficient protocols that securely realize these functionalities in either the RO model (for efficiency) or the CRS model (for elegance). Finally, this paper concludes by showing that their distributed protocols generalize to a broad class of “discrete-log”-based public-key cryptosystems, which notably includes identity-based encryption. This opens the door to a powerful extension of IBE with a virtual PKG made of a group of people, each one memorizing a small portion of the master key.

The construction of [3] relied on the DDH assumption, and in [48] the techniques are extended to pairing-based schemes to obtain efficient (simulation-sound) zero-knowledge proofs. These are then used to provide distributed-password protocols for Linear decryption and extraction of several identity-based cryptosystems, all proven secure in the standard model.

8.13 Cryptographic APIs

The paper [154] proposes a much-needed formal definition of security for cryptographic key management APIs. The advantages of the new definition are that it is general, intuitive, and applicable to security proofs in both symbolic and computational models of cryptography. The core of the definition is an idealized API which allows only the most essential functions for generating, exporting and importing keys, and takes into account dynamic corruption of keys. More expressive APIs that offer a richer functionality can then be built on top of the idealized one.

Chapter 9

Foundational Aspects

There has been numerous work on foundational aspects of the area of provable security conducted in ECRYPT-2. In particular we have looked at basic building blocks of how schemes, protocols and proofs are constructed. We now summarize these foundational results.

9.1 Analysis of Underlying Hard Problems

The security of asymmetric cryptographic systems relies on assumptions that certain computational problems, mostly from number theory and algebra, are intractable. Since proving useful lower complexity bounds in a general model of computation seems to be impossible with currently available techniques, these assumptions have been analyzed in various restricted models. A natural and very general class of algorithms is considered in the *generic ring model*. This model captures all algorithms solving problems defined over an algebraic ring without exploiting specific properties of a given representation of ring elements. Such algorithms work in a similar way for arbitrary representations of ring elements, thus are *generic*. In [145] the authors prove a general theorem which states that solving certain subset membership problems in the ring $\mathbb{Z}_n$ is equivalent to factoring n. This main theorem allows us to provide an example for a computational problem with high cryptographic relevance which is easy to solve in general, but equivalent to factoring in the generic model. Concretely, the authors show that computing the *Jacobi symbol* is equivalent to factoring in the generic ring model.

In pairing-based cryptography the Generic Group Model (GGM) is used frequently to provide evidence towards newly introduced hardness assumptions. Unfortunately, the GGM does not reflect many known properties of bilinear group settings and thus hardness results in this model are of limited significance. In [146] a novel computational model is proposed for pairing-based cryptography, called the Semi-Generic Group Model (SGGM), that is closer to the standard model and allows to make more meaningful security guarantees. In fact, the best algorithms currently known for solving pairing-based problems are semi-generic in nature. The usefulness of the new model is demonstrated by applying it to study several important assumptions (BDDH, Co-DH). Furthermore, master theorems are developed for facilitating an easy analysis of other (future) assumptions. These master theorems imply that (unless there are better algorithms than the semi-generic ones) great parts of the zoo of novel assumptions over bilinear groups are reducible to just two (more or less) standard assumptions over finite fields. Finally, appropriateness of the SGGM is examined as a tool for analyzing the security of practical cryptosystems without random oracles by applying it to the BLS signature scheme.

In [11], the formal treatment of cryptographic constructions ("Polly Cracker") based on the hardness of computing remainders modulo an ideal in multvariate polynomial rings is initiated. The authors start by formalising and studying the relation between the ideal membership problem and the problem of computing a Gröbner basis. They show both positive and negative results. On the negative side, they define a symmetric Polly Cracker encryption scheme and prove that this scheme only achieves bounded chosen plaintext security under the hardness of the ideal membership problem. Furthermore, they show that a large class of algebraic transformations cannot convert this scheme to a fully secure Polly Cracker-style scheme. On the positive side, they formalise noisy variants of the ideal related problems. These problems can be seen as natural generalisations of the LWE problem and the approximate GCD problem over polynomial rings. After formalising and justifying the hardness of the noisy assumptions they show that noisy encoding of messages results in a fully chosen plaintext secure somewhat homomorphic encryption scheme. Together with a standard symmetric-to- asymmetric transformation for additively homomorphic schemes, this provides a positive answer to the long standing open problem of constructing a secure Polly Cracker-style cryptosystem reducible to the hardness of solving a random system of equations. The results go beyond that by also providing a new family of somewhat homomorphic encryption schemes based on generalised hard problems. Finally, the results also imply that Regev's LWE-based public-key encryption scheme is (somewhat) multiplicatively homomorphic for appropriate choices of parameters.

9.2 Obfuscation Techniques

In [138] the authors propose and investigate two new variants of obfuscation definitions. Loosely speaking, an obfuscation of a function should satisfy two requirements: firstly, using the obfuscation, it should be possible to evaluate the original function; secondly, the obfuscation should not reveal anything about the original function that cannot be learnt from oracle access to the function alone. Contrary to most prior definitions, the definitions in this paper are simulation-based and demand only security on average. Despite the existence of generic impossibility results, the new definitions are both useful and achievable. In particular, it is shown that, while it is hard to avoid generic impossibilities, useful and reasonable obfuscation definitions are possible when considering specific tasks.

9.3 Smooth Projective Hash Functions

The notion of smooth projective hash functions was proposed by Cramer and Shoup [253] and can be seen as special type of zero-knowledge proof system for a language. Though originally used as a means to build efficient chosen-ciphertext secure public-key encryption schemes, some variations of the Cramer-Shoup smooth projective hash functions also found applications in several other contexts, such as password-based authenticated key exchange [267] and oblivious transfer [286]. In [6] the authors first address the problem of building smooth projective hash functions for more complex languages. More precisely, they show how to build such functions for languages that can be described in terms of disjunctions and conjunctions of simpler languages for which smooth projective hash functions are known to exist. Next, they illustrate how the use of smooth projective hash functions with more complex languages can be efficiently associated to extractable commitment schemes and avoid the need for zero-knowledge proofs. Finally, the authors explain how to apply these results to provide more efficient solutions to two well-known cryptographic problems: a public-key certification which guarantees the knowledge of the private key by the user without random oracles or zero-knowledge proofs and adaptive security for password-based authenticated key exchange protocols in the universal composability framework with erasures.

In 2008, Groth and Sahai proposed a powerful suite of techniques for constructing non-interactive zero-knowledge proofs in bilinear groups. Their proof systems have found numerous applications, including group signature schemes, anonymous voting, and anonymous credentials. In [41], the authors demonstrate that the notion of smooth projective hash functions can be useful to design round-optimal privacy-preserving interactive protocols. They show that this approach is suitable for designing schemes that rely on standard security assumptions in the standard model with a common-reference string and are more efficient than those obtained using the Groth-Sahai methodology. As an illustration of their design principle, they construct an efficient oblivious signature-based envelope scheme and a blind signature scheme, both round-optimal.

9.4 Commitment Schemes

In [174] the authors consider commitment schemes that are secure against concurrent man-in-the-middle (cMiM) attacks. Under such attacks, two possible notions of security for commitment schemes have been proposed in the literature: concurrent non-malleability with respect to commitment and concurrent non-malleability with respect to decommitment (i.e., opening). After the original notion of non-malleability, introduced by Dolev, Dwork and Naor, that is based on the independence of the committed messages, a new and stronger simulation-based notion of non-malleability has been proposed with respect to openings or with respect to commitment by requiring that for any man-in-the-middle adversary there is a stand-alone adversary that succeeds with the same probability. When commitment schemes are used as sub-protocols (which is often the case) the simulation-based notion is much more powerful and simplifies the task of proving the security of the larger protocols. The main result is a commitment scheme that is simulation-based concurrent non-malleable with respect to both commitment and decommitment. This property protects against cMiM attacks mounted during both commitments and decommitments which is a crucial security requirement in several applications, as in some digital auctions, in which players have to perform both commitments and decommitments. The scheme uses a constant number of rounds of interaction in the plain model and is the first scheme that enjoys all these properties under the simulation-based definitions.

In [61] the authors give a construction of a statistically binding commitment scheme which is concurrent non-malleable with respect to both commitment and decommitment. The construction relies on the existence of a family of pairs of claw-free permutations and only needs a constant number of communication rounds in the plain model. The proof of security uses non-black-box techniques and satisfies the (most powerful) simulation-based definitions of non-malleability. This is the first scheme that guarantees simultaneously the unconditional binding property, and both forms of non-malleability in a simulation-based sense, in a constant number of rounds.

Universally composable (UC) commitments are commitments that remain secure when composed with arbitrary other protocols, as initially formalized by Canetti and Fischlin in 2001. In 2011, a collaboration between ECRYPT associated members [104] provided the first constructions of UC-secure commitments (in groups with a bilinear map) that simultaneously combine the key properties of being non-interactive, supporting commitments to strings (instead of bits only), and offering re-usability of the common reference string for multiple commitments. The new commitment schemes are also adaptively secure assuming reliable erasures.

In [259, 260], Dwork et al. opened the fundamental question of the existence of commitment schemes that are secure against selective opening attacks (SOA, for short). In [224] Bellare, Hofheinz, and Yilek, and Hofheinz in [278] solved this open problem by presenting a scheme based on non-black-box use of a one-way permutation and super-constant number of rounds. The recent work of Xiao ([315]) investigates on how to achieve nearly optimal SOA-secure commitment schemes where optimality is in the sense of both the round complexity and the black-box use of cryptographic primitives. The work of Xiao focuses on a simulation-based security notion of SOA. Moreover, results in [315] focus either on parallel or concurrent SOA. In [177] the authors first point out various issues in the claims of [315] that actually re-open several of the questions left open in [224, 278]. Then they provide different schemes and lower bounds that produce a very different state-of-the-art compared to the one given in [315] (i.e., they contradict some of the theorems claimed in [315]). More specifically, by specifying as (x, y) the round complexity of a scheme that requires x rounds in the commitment phase and y rounds in the opening phase, and by considering only (like in [315]) the setting of black-box simulation for SOA-security, they show that:

1. There is an issue in the result of [315] on the existence of $(3, 1)$-round schemes for parallel SOA; in fact, they are able to contradict the impossibility result by presenting a $(3, 1)$-round scheme based on black-box use of trapdoor commitments. Moreover they can instantiate such a scheme with a non-black-box use of a one-way function, therefore producing a $(3, 1)$-round scheme based on any one-way function that improves the result of [224, 278] from logarithmic round complexity to 3 (optimal) under optimal complexity assumptions. They also show a $(3, 3)$-round scheme based on black-box use of any one-way permutation.

2. There is an issue in the proof of security for parallel composition of the $(4, 1)$-round scheme given in [315], thus that scheme may not be secure. They show instead a $(4, 1)$-round scheme based on black-box use of any weak trapdoor commitment scheme, and a $(5, 1)$-round scheme based on black-box use of any one-way permutation.

3. There is an issue in the proof of security of the concurrent SOA-secure scheme of [315] when the simulator does not know the distribution of committed messages by itself. In fact, they contradict the claimed security of this scheme by showing that there can not exist such a scheme, regardless of its round complexity and of the (black-box or non-black-box) use of cryptographic primitives.

All their schemes are secure for parallel SOA composition and also secure for concurrent SOA composition under the restriction that all commitment phases are played before any opening phase. Moreover, in all their constructions the simulator does not need to know the distribution of the messages committed to by the sender. In light of our result on the impossibility of a scheme that is SOA-secure under full-fledged concurrent composition (see Item 3 above), the concurrency achieved by their schemes is essentially optimal.

9.5 Secret Sharing

Rational cryptography tries to apply game-theoretic methods to cryptography; instead of modelling users as “honest” players that follow the protocol and “malicious” ones that behave arbitrarily, users act in self-interest. In [111] the authors propose a new methodology for *rational secret sharing* leading to various instantiations that are simple and efficient in terms of computation, share size, and round complexity. The protocols do not require physical assumptions or simultaneous channels, and can even be run over asynchronous, point-to-point networks. They moreover propose new equilibrium notions and show that the protocols satisfy them. In particular, these notions ensure that protocol messages cannot be used as subliminal channels, something achieved in prior work only by making strong assumptions on the communication network.

9.6 Zero-Knowledge

Efficient-knowledge proofs knowledge (ZK-PoK) are basic building blocks of many practical cryptographic applications such as identification schemes, group signatures, and secure multiparty computation (MPC). Currently, first applications that essentially rely on ZK-PoKs are being deployed in the real world. The most prominent example is the Direct Anonymous Attestation (DAA) protocol, which was adopted by the Trusted Computing Group (TCG) and implemented as one of the functionalities of the cryptographic chip Trusted Platform Module (TPM).

Implementing systems using ZK-PoK turns out to be challenging, since ZK-PoK are significantly more complex than standard crypto primitives (e.g., encryption and signature schemes). As a result, the design-implementation cycles of ZK-PoK are time-consuming and error-prone. To overcome this, the authors of [23] present a compiler with corresponding languages for the automatic generation of sound and efficient ZK-PoK based on Σ-protocols. The protocol designer using the compiler formulates the goal of a ZK-PoK proof in a high-level protocol specification language, which abstracts away unnecessary technicalities from the designer. The compiler then automatically generates the protocol implementation in Java code; alternatively, the compiler can output a description of the protocol in LaTeX which can be used for documentation or verification.

The authors of [15] present a comprehensive specification language and a compiler for ZK-PoK protocols based on Σ-protocols. The compiler allows the fully automatic translation of an abstract description of a proof goal into an executable implementation. Moreover, the compiler overcomes various restrictions of previous approaches, e.g., it supports the important class of exponentiation homomorphisms with hidden-order co-domain, needed for privacy-preserving applications such as DAA. Finally, the compiler is certifying, in the sense that it automatically produces a formal proof of the soundness of the compiled protocol for a large class of protocols using the Isabelle/HOL theorem prover.

In 2008, Groth and Sahai [275] proposed a general methodology for constructing non-interactive zero-knowledge (and witness-indistinguishable) proofs in bilinear groups. In [127] the authors provide an implementation of the recent Groth–Sahai NIZK proofs based on pairings. They compare their efficiency to schemes based on Σ-protocols in the Random Oracle Model. In [128] the authors discuss Groth–Sahai proofs in more detail, showing how they can be extended to work with Type-2 pairings; as well as correcting some errors in the original full version of the Groth–Sahai paper.

Groth–Sahai proofs are still somewhat inefficient due to a number of pairing computations required for verification. In [39] recent techniques of *batch verification* are applied to the Groth-Sahai proof systems in order to significantly reduce the complexity of proof verification. The paper gives explicit batch-verification formulæ for generic Groth-Sahai equations (whose cost is less than a tenth of the original) and furthermore for specific popular protocols relying on their methodology, such as Groth's group signatures.

In [215] the authors present two variations of the notion of co-soundness previously defined and used by [274] in the common reference string model. The first variation holds in the Bare Public-Key (BPK, for short) model and closely follows the one of [274]. The second variation (which they call weak co-soundness) is a weaker notion since it has a stronger requirement, and it holds in the Registered Public-Key model (RPK, for short). They then show techniques to construct co-sound argument systems that can be proved secure under standard assumptions, more specifically:

- In the main result they show a constant-round resettable zero-knowledge argument system in the BPK model using black-box techniques only (previously it was achieved in [245, 256] with complexity leveraging)
- Additionally, they show an efficient statistical non-interactive zero- knowledge argument system in the RPK model (previously it was achieved in [254] with complexity leveraging).

In [176], the authors study the complexity of efficient zero-knowledge reductions, from honest-verifier zero knowledge (i.e., zero-knowledge protocols where the malicious verifier is required to be honest) to concurrent non-malleable zero-knowledge (i.e., zero-knowledge protocols where the adversary can play as a man-in-the-middle with multiple provers and verifiers). More precisely, under a standard complexity assumption (DDH), on input a public-coin honest-verifier statistical zero knowledge argument of knowledge π' for a language L, they show a compiler that produces an argument system π for L that is concurrent non-malleable zero-knowledge (under non-adaptive inputs which is the best one can hope to achieve [1, 2]). If κ is the security parameter, the overhead of their compiler is as follows:

1. The round complexity of π is $r + \tilde{O}(\log \kappa)$ rounds, where r is the round complexity of π'.
2. The new prover (resp., the new verifier) incurs an additional overhead of (at most) $r + \kappa \cdot \tilde{O}(\log^2 \kappa)$ modular exponentiations. If tags of length $\tilde{O}(\log \kappa)$ are provided, the overhead is only $r + \tilde{O}(\log^2 \kappa)$ modular exponentiations.

This work therefore proposes the first proof systems that are of practical relevance when concurrent and man-in-the-middle attacks are considered.

In a cryptographic range proof, the prover proves in zero knowledge that for given C and H, C is a commitment of some element $x \in [0, H]$ (modifying it to general ranges $[L, H]$ is trivial when one uses a homomorphic commitment scheme). Range proofs are needed in various applications like e-voting, e-auctions, e-cash, etc. In [66], Chaabouni, Lipmaa and shelat show how to express an arbitrary integer interval $\mathcal{I} = [0, H]$ as a sumset $\mathcal{I} = \sum_{i=1}^{\ell} G_i * [0, u-1] + [0, H']$ of smaller integer intervals for some small values ℓ, u, and $H' < u - 1$, where $b * A = \{ba : a \in A\}$ and $A + B = \{a + b : a \in A \wedge b \in B\}$. They show how to derive such expressions of $\mathcal{I}$ as a sumset for any value of $1 < u < H$, and in particular, how the coefficients G_i can be found by using a nontrivial but efficient algorithm. Note that this result itself is interesting in the context of additive combinatorics. Given the sumset-representation of $\mathcal{I}$, the authors show how to decrease both the communication complexity and the computational complexity of the recent pairing-based range proof in [241] of Camenisch, Chaabouni and shelat by a factor of 2. Hence, this new result in additive combinatorics has direct relevance in practice.

Two central notions of Zero Knowledge that provide strong, yet seemingly incomparable security guarantees against malicious verifiers are those of Statistical Zero Knowledge and Resettable Zero Knowledge. The current state of the art includes several feasibility and impossibility results regarding these two notions *separately*. However, the question of achieving Resettable Statistical Zero Knowledge (i.e., Resettable Zero Knowledge and Statistical Zero Knowledge *simultaneously*) for non-trivial languages remained open. In [121], the authors show:

- Resettable Statistical Zero Knowledge with unbounded prover: under the assumption that sub-exponentially hard one-way functions exist, $rSZK = SZK$. In other words, every language that admits a Statistical Zero-Knowledge (SZK) proof system also admits a Resettable Statistical Zero-Knowledge ($rSZK$) proof system. (Further, the result can be re-stated unconditionally provided there exists a sub-exponentially hard language in SZK). Moreover, under the assumption that (standard) one-way functions exist, all languages L such that the complement of L is random self reducible, admit a $rSZK$.

- Resettable Statistical Zero Knowledge with efficient prover: efficient-prover Resettable Statistical Zero-Knowledge proof systems exist for all languages that admit hash proof systems (e.g., QNR, QR, DDH, DCR). Furthermore, for these languages they construct a two-round resettable statistical witness-indistinguishable argument system.

The round complexity of their proof systems is $\tilde{O}(\log \kappa)$, where κ is the security parameter, and all their simulators are *black-box*.

Security under man-in-the-middle attacks is extremely important when protocols are executed on asynchronous networks, as the Internet. Focusing on interactive proof systems, one would like also to achieve unconditional soundness, so that proving a false statement is not possible even for a computationally unbounded adversarial prover. Motivated by such requirements, in [62] the authors address the problem of designing constant-round protocols in the plain model that enjoy simultaneously non-malleability (i.e., security against man-in-the-middle attacks) and unconditional soundness (i.e., they are proof systems). They first give a construction of a constant-round one-many (i.e., one honest prover, many honest verifiers) concurrent non-malleable zero-knowledge *proof* (in contrast to argument) system for every NP language in the plain model. Then they give a construction of a constant-round concurrent non-malleable witness-indistinguishable proof system for every NP language. Compared with previous results, their constructions are the first constant-round proof systems that in the plain model guarantee simultaneously security against some non-trivial concurrent man-in-the-middle attacks and against unbounded malicious provers.

The standard man-in-the-middle attack for zero-knowledge interactive protocols involves an adversary M interacting simultaneously with an honest prover on left hand side, and an honest verifier on the right hand side. In [175] the authors proposes a strengthening of the standard model, where M — in addition to the usual interaction with the honest prover and the honest verifier – can also *reset* one of them. This gives rise to two different models depending on which party can be reset by M. In [175] the authors construct interactive proofs for all languages in NP, that remain *simulation-extractable* (i.e., they enjoy a strong form of non-malleability) under these two attack models. All constructions are based on standard and general cryptographic assumptions and can be used to obtain improved identification schemes secure against reset attacks.

In the shared random string (SRS, in short) model there exist *one-message* zero-knowledge proofs for all NP under the seemingly stronger assumption of the existence of one-way trapdoor permutations. If instead one would like to achieve the stronger notion of a proof of knowledge, then the even stronger assumption of dense secure cryptosystems is necessary and sufficient. In [PV11], the author define the *Two-Message* model for Zero Knowledge. In the Two-Message model, prover and verifier have access to the same SRS and, in addition, the prover is allowed to send one message to the verifier before the SRS is made available. As in the SRS model, the verifier needs not to reply to this message. The random string and initial prover message can then be used by the prover to prove any polynomial number of theorems using a single message for each of them. They show that the Two-Message model allows one to design non-interactive zero knowledge proofs of knowledge without having to assume dense secure cryptosystem. Moreover, non-interactive zero-knowledge proofs and arguments of knowledge in the Two-Message model can be used in applications in place of non-interactive zero-knowledge proofs and arguments of knowledge in the SRS model thus resulting in weaker complexity assumptions without any significant penalty in the round complexity. Concerning more sophisticated notions of one-message zero knowledge, they also show how to construct Two-Message Non-Malleable Zero-Knowledge Proofs of Knowledge by only requiring the existence of one-way trapdoor permutations. Finally, they give examples of cryptographic constructions in which non-interactive zero-knowledge in the Two-Message model can be used in order to reduce the needed complexity assumptions.

In [72] , the authors study simultaneously resettable arguments of knowledge. As main result, they show a construction of a constant-round simultaneously resettable witness-indistinguishable argument of knowledge for any NP language. They also show two applications of the above result: the first constant-round simultaneously resettable zero-knowledge argument of knowledge in the Bare Public-Key Model; and the first simultaneously resettable identification scheme which follows the knowledge extraction paradigm.

9.7 Oblivious Transfer

Oblivious transfer (OT, for short) is a fundamental primitive in the foundations of Cryptography. While in the standard model OT constructions rely on public-key cryptography, only very recently Kolesnikov in [289] showed a truly efficient string OT protocol by using tamper-proof hardware tokens. His construction only needs few evaluations of a block cipher and requires stateless (therefore resettable) tokens that is very efficient for practical applications. However, the protocol needs to be interactive, that can be an hassle for many client-server setting and the security against malicious sender is achieved in a *covert* sense, meaning that a malicious sender can actually obtain the private input of the receiver while the receiver can detect this malicious behavior with probability 1/2. Furthermore the protocol does not enjoy forward security (by breaking a token one violates the security of all previously played OTs).

In [DSV11], the authors propose new techniques to achieve efficient *non-interactive* string

OT using tamper-proof hardware tokens. While from one side their tokens need to be stateful, their protocol enjoys several appealing features: 1) it is secure against malicious receivers and the input privacy of honest receivers is guaranteed unconditionally against malicious senders, 2) it is forward secure, 3) it enjoys adaptive input security, therefore tokens can be sent before parties know their private inputs. This gracefully fits a large number of client-server settings (digital TV, e-banking) and thus many practical applications. On the bad side, the output privacy of honest receivers is not satisfied when tokens are reused for more than one execution.

9.8 Threshold Cryptography

Threshold cryptography enhances the availability and security of public-key encryption and signature schemes by splitting private keys into several (say n) shares. In these schemes, a quorum of at least $t \leq n$ servers needs to act upon a message to produce the result, while corrupting less than t servers maintains the scheme's security. So far, most practical threshold signatures, where servers act non-interactively, were analyzed in the limited static corruption model (where the adversary chooses which servers will be corrupted at the system's initialization stage). Existing threshold public-key encryption schemes that withstand the strongest combination of adaptive malicious corruptions (allowing the adversary to corrupt servers at any time based on its complete view), and chosen-ciphertext attacks (CCA) all require interaction and attempts to remedy this problem resulted in schemes suffering from certain limitations. Before 2011, it was an open question whether there exist non-interactive threshold schemes providing the highest security with short private key shares and adaptive security. In 2011, affirmative answers to this question were given [163] by presenting such efficient decryption and signature schemes within a unified algebraic framework.

9.9 Message Transmission

The problem of reliable message transmission (RMT) and the secure message transmission (SMT) in asynchronous networks are fundamental problems in secure distributed computing. In RMT, a sender S and a receiver R are connected by several disjoint channels, some of which can be under the control of a computationally unbounded adversary. The goal is to design a protocol using which S can reliably send a message to the R, irrespective of the disruptions done by the adversary. In SMT, we require an additional property that the message should be information theoretically from the adversary. Unfortunately, the RMT and the SMT problem have not been investigated in the asynchronous settings. In [73] the authors establish tight bounds on the communication complexity of asynchronous RMT and SMT protocols. Moreover, they considered two variants of the problem, namely perfect (where the protocol satisfies all the properties without any error) and statistical (where the protocol satisfies all the properties except with a negligible error probability).

9.10 Refining the Random Oracle Methodology

Many efficient cryptographic protocols and primitives make use of a hash function in a way that it is hard to pin down exactly how the security of the overarching scheme relates to that of the hash function. The Random Oracle Model (ROM) was introduced to argue formally about these schemes [227]. In [103] the authors investigate the Random Oracle Model feature known as *programmability*, which allows security reductions in the ROM to dynamically choose the range points of an ideal hash function. This property is interesting for at least two reasons: first, because of its seeming artificiality (no standard model hash function is known to support such adaptive programming); second, the only known security reductions for many important cryptographic schemes rely fundamentally on programming. The authors of [103] provide formal tools to study the role of programmability in provable security. This includes a framework describing three levels of programming in reductions (none, limited, and full). It is proven that *no* black-box reductions can be given for FDH signatures when only limited programming is allowed, giving formal support for the intuition that full programming is fundamental to the provable security of FDH. It is also shown that Shoup's trapdoor-permutation-based key-encapsulation is provably CCA-secure with limited programmability, but no black-box reduction succeeds when no programming at all is permitted. The negative results use a new concrete-security variant of Hsiao and Reyzin's two-oracle separation technique.

9.11 Computational Soundness

There are essentially two approaches towards relating security of protocols proved in symbolic models with security in the stronger computational models. One approach, the "trace mapping approach" relies on carefully mapping computational executions to symbolic executions. The other approach, "the reactive simulatability approach" relies on linking symbolic and computational executions in a much stronger way, akin to the way real executions and ideal executions are realized in the universal composability setting. In [169] the authors demonstrate that in important situations, namely when the adversary can adaptively corrupt encryption keys, the reactive simulatability approach cannot be applied whereas the trace mapping still works. This result complements the obvious observation that when a reactive simulatability result can be established, a related trace mapping result also holds.

A recent line of research aims at bridging the gap between the symbolic and the cryptographic approaches, the two main approaches for rigorously analyzing security protocols. Soundness results typically show that security of symbolic protocols implies security of implemented protocols against any polynomial Turing machine. However, each soundness result is established for a small subset of primitives and gathering all primitives together would requires a huge amount of work. An alternative that alleviates this state of affairs is proposed in [80]. Specifically, this paper proposes the notion of deduction soundness which defines what it means for a symbolic deductionsystem to soundly abstract a set of primitives. The main advantage of deduction soundness is that it is *composable* which allows to consider each primitive separately and then compose them together. As an application, it is shown that a deduction sound set of primitives can be extended to asymmetric encryption and to public data-structures (such as pairing or list). Moreover, deduction soundness abstracts away the structure of the protocols, allowing to use any protocol specification language.

9.12 General Foundations

In [149] a conceptual approach for probabilistic analysis of adaptive adversaries via Maurers methodology of random systems (Eurocrypt02) is given. The authors first consider a well-known comparison theorem of Maurer according to which, under certain hypotheses, adaptivity does not help for achieving a certain event. This theorem has subsequently been misinterpreted, leading to a misrepresentation with one of Maurers hypotheses being omitted in various applications. In particular, the only proof of (a misrepresentation of) the theorem available in the literature contained a flaw. The authors clarify the theorem by pointing out a simple example illustrating why the hypothesis of Maurer is necessary for the comparison statement to hold and provide a correct proof. Furthermore, they prove several technical statements applicable in more general settings where adaptivity might be helpful, which can be seen as the random system analogue of the game-playing arguments.

9.13 Foundations of Public Key Encryption

In [25] the authors study relations among notions of complete non-malleability, where an adversary can tamper with both ciphertexts and public-keys, and ciphertext indistinguishability along the pattern of relations previously established for standard non-malleability. To this end, they propose a more convenient and conceptually simpler indistinguishability-based security model to analyse completely non-malleable schemes. Their model is based on strong decryption oracles, which provide decryptions under arbitrarily chosen public keys. The authors give the first precise definition of a strong decryption oracle, pointing out the subtleties in different approaches that can be taken. They extend indistinguishability of ciphertexts, comparison-based non-malleability and simulation non-malleability under various attack models to allow strong decryption queries. They conclude that these models can be seen as alternative formulations of complete non-malleability. Finally, they construct the first *practical* scheme, which is fully secure against strong chosen-ciphertext attacks, and therefore completely non-malleable, without random oracles. The security analysis of this scheme shows that their characterisation of complete non-malleability via indistinguishability provides a setting where one can apply the proof-techniques normally employed in the analysis of IND-CCA2 schemes.

In [26] the authors introduce two extractor-based properties that allow one to gain insight into the design of such schemes and to go beyond known feasibility results in this area. They formalise *strong plaintext awareness* and *secret key awareness* and prove their suitability in realising these goals. Strong plaintext awareness imposes that it is infeasible to construct a ciphertext under *any* public key without knowing the underlying message. Secret key awareness requires it to be infeasible to produce a new public key without knowing a corresponding secret key. The authors study the relations among these and existing notions in the literature and show that if such properties are realisable (and one admits non-black-box simulators) then the impossibility result established for the construction of completely non-malleable schemes under non-assisted simulators no longer holds. They also look at how such notions can be realised in the standard model and in the random oracle model. More precisely, they propose a generic transformation to construct secret key aware schemes in the random oracle model and give preliminary steps towards building such schemes in the standard model. To this end, they introduce a novel factorisation-based knowledge assumption, which roughly speaking, requires it to be infeasible to construct integers of the form P^2Q without knowing the corresponding factorisation.

In [1], the authors consider the problem in which the ciphertext produced by an encryption scheme decrypts correctly under two different public-keys or identities. This can be problematic in a setting where the encryption scheme provides anonymity and data privacy since it can jeopardize the correct operation of the application built on top of the encryption scheme. To address this problem, the authors introduce the notion of robustness, which reflects the difficulty of producing a ciphertext valid under two different encryption keys. The value of robustness is conceptual, "naming" something that has been undefined yet at times implicitly (and incorrectly) assumed. Essentially, robustness helps make encryption more mis-use resistant. In addition to providing formal definitions of several variants of robustness, the authors consider and dismiss natural approaches to achieve it; provide two general robustness-adding transforms; test robustness of existing schemes and patch the ones that fail; and discuss some applications.

Lossy encryption was originally studied as a means of achieving efficient and composable oblivious transfer. Bellare, Hofheinz and Yilek showed that lossy encryption is also selective opening secure. In [131] the authors present new and general constructions of lossy encryption schemes and of cryptosystems secure against selective opening adversaries. They show that every re-randomizable encryption scheme gives rise to efficient encryptions secure against a selective opening adversary. The authors show that statistically-hiding 2-round Oblivious Transfer implies Lossy Encryption and so do smooth hash proof systems. This shows that private information retrieval and homomorphic encryption both imply Lossy Encryption, and thus Selective Opening Secure Public Key Encryption. Applying their constructions to well-known cryptosystems, they obtain selective opening secure commitments and encryptions from the Decisional Diffie-Hellman, Decisional Composite Residuosity and Quadratic Residuosity assumptions. In an indistinguishability-based model of chosen-ciphertext selective opening security, they obtain secure schemes featuring short ciphertexts under standard number theoretic assumptions. In a simulation-based definition of chosen-ciphertext selective opening security, the authors also handle non-adaptive adversaries by adapting the Naor-Yung paradigm and using the perfect zero-knowledge proofs of Groth, Ostrovsky and Sahai.

9.14 Foundations of Public Key Signatures

A powerful abstraction of a class of mathematical structures that underlies digital signature schemes is studied in [64]. More precisely, the paper identifies, motivates, and explores the concept of *adatpive pseudo-free groups* an extension of an earlier notion proposed by Rivest at TCC 2004. In addition to providing a precise definition and that identifies the limits of its achievability this work also provides generic constructions of digital signature schemes and network coding scheme starting from arbitrary adaptive pseudofree groups. Concrete instantiations are then obtained by proving that the RSA group is pseudo-free.

9.15 Foundations of Symmetric Encryption

Bellare and Kohno [225] introduced a formal framework for the study of related-key attacks against blockciphers. They established sufficient conditions (output-unpredictability and collision-resistance) on the set of related-key-deriving (RKD) functions under which an ideal cipher is secure against related-key attacks, and suggested this could be used to derive security goals for real blockciphers. However, to do so requires the reinterpretation of results proven in the ideal-cipher model for the standard model (in which a blockcipher is modelled as, say, a pseudorandom permutation family). In [12] the authors show this is a fraught activity.

In particular, building on a recent idea of Bernstein, they first demonstrate a related-key attack that applies generically to a large class of blockciphers. The attack exploits the existence of a short description of the blockcipher, and so does not apply in the ideal-cipher model. However, the specific RKD functions used in the attack are provably output-unpredictable and collision-resistant. In this sense, the attack can be seen as a separation between the ideal-cipher model and the standard model. Second, the authors investigate how the related-key attack model of Bellare and Kohno can be extended to include sets of RKD functions that themselves access the ideal cipher. Precisely such related-key functions underlie the generic attack, so their extended modelling allows one to capture a larger universe of related-key attacks in the ideal-cipher model. The authors establish a new set of conditions on related-key functions that is sufficient to prove a theorem analogous to the main result of Bellare and Kohno, but for their extended model. They then exhibit non-trivial classes of practically relevant RKD functions meeting the new conditions. They go on to discuss standard model interpretations of this theorem, explaining why, although separations between the ideal-cipher model and the standard model still exist for this setting, they can be seen as being much less natural than their previous separation. In this manner, the authors argue that their extension of the Bellare–Kohno model represents a useful advance in the modelling of related-key attacks. Third, they consider the topic of key-recovering related-key attacks and its relationship to the Bellare–Kohno formalism. In particular, they address the question of whether lowering the security goal by requiring the adversary to perform key-recovery excludes separations of the type exhibited by us in the Bellare–Kohno model.

Chapter 10

General Cryptanalysis

In [152] a new approach to analysing key strength is presented which tries to economically quantify the cost of breaking keys associated to specific schemes. The approach presented provides a notion of repeatability and scalability over time; which previous approaches fail to do. The main idea is to utilize the pricing model of cloud computing providers to estimate the total-cost of key recovery. On the basis that cloud computing providers behave as rational entities, this provides a robust mechanism to attach an economic cost to a key recovery exercise.

10.1 Factoring with Partial Information Oracles

The factorization problem is one of the most important number theoretic problems of cryptography and lies at the heart of RSA's security. Since the invention of RSA, there was a significant improvement of algorithms for factoring large numbers resulting in the famous Number Field Sieve algorithm with sub-exponential time complexity. A different line of research asks for classes of oracles that are sufficient to factor in *polynomial time.* The goal is to find an oracle class as weak as possible. A result of Coppersmith states that an oracle that on input $N = pq$ provides half of the bits of the prime factor p yields an efficient factoring algorithm. This result has been used to prove the security of RSA-OAEP.

In [168], the authors show that even weaker oracles are sufficient for polynomial time factoring. Namely, it suffices to use an oracle that on input $N = pq$ answers with a modulus $N' = p'q'$ such that p and p' share some least significant bits. Notice that as opposed to the result of Coppersmith, where an attacker gets bits of a prime factor *explicitly*, in the present approach the oracle does only provide *implicit* information about the prime factorization. Therefore, this approach is called implicit factorization. As one would expect in terms of the amount of bits, an attacker needs more implicit information than explicit information. The authors of [168] provide bounds on the number of shared bits and the number of oracle calls that are sufficient to factor N in polynomial time.

The authors of [95] investigated the problem of integer factoring given *implicit* information of a special kind. The problem is as follows: let $N_1 = p_1q_1$ and $N_2 = p_2q_2$ be two RSA moduli of same bit-size, where q_1, q_2 are α-bit primes. We are given the *implicit* information that p_1 and p_2 share t most significant bits. The authors of [95] presented a novel and rigorous lattice-based method that leads to the factorization of N_1 and N_2 in polynomial time as soon as $t \geq 2\alpha + 3$. Subsequently, the authors of [95] heuristically generalize the method to k

RSA moduli $N_i = p_i q_i$ where the p_i's all share t most significant bits (MSBs) and obtain an improved bound on t that converges to $t \geq \alpha + 3.55\ldots$ as k tends to infinity. The authors of [95] extend the work of May and Ritzenhofen in [168], where similar results were obtained when the p_i's share least significant bits (LSBs). In [307], Sarkar and Maitra describe an alternative but heuristic method for only two RSA moduli, when the p_i's share LSBs and/or MSBs, or bits in the middle. In the case of shared MSBs and two RSA moduli, they get better experimental results in some cases, but [95] uses much lower (at least 23 times lower) lattice dimensions. The results [95] relies on the the following surprinsingly simple algebraic relation in which the shared MSBs of p_1 and p_2 cancel out: $q_1 N_2 - q_2 N_1 = q_1 q_2 (p_2 - p_1)$. This relation allows the authors of [95] to build a lattice whose shortest vector yields the factorization of the N_i's.

One of the most prominent candidate of pseudorandom number generators is the power generator, that computes a sequence $s_i = s_{i-1}^e \bmod N$ from a secret seed s_0. For $e = 2$ the generator is called the Blum Blum Shub generator, and for $e = 3$ it is called the RSA generator. In each iteration of a power generator, one outputs a certain fraction of the bits of s_i. There is a classical security tradeoff for the output rate of such a pseudorandom number generator. On the one hand, we would like to output as many bits as possible per iteration. On the other hand, a large fraction of output bits might help an attacker to distinguish the sequence from a pseudorandom sequence. It was known that the Blum Blum Shub and the RSA generator can successfully attacked when we output a $\frac{2}{3}$-fraction or a $\frac{3}{4}$-fraction of the bits, respectively. In [137], the authors improve on these attack bounds. Namely, for the Blum Blum Shub generator the bound is decreased from $\frac{2}{3}$ to $\frac{1}{2}$, and for the RSA generator the bound is decreased from $\frac{3}{4}$ to $\frac{2}{3}$. This improvement shows that we cannot output too many bits per iteration and comes closer to the bounds for which we can prove the pseudorandomness of the output bits. The improvement is achieved by a new technique that combines lattice-based linearization with Coppersmith's lattice technique.

The same technique is used by the authors in [136] in the context of RSA cryptanalysis. It is known that RSA can be attacked in polynomial time whenever the secret RSA key d is too small, i.e. we have an oracle which reveals such partial information. The size of d serves as a benchmark for cryptanalytic efforts. In [136], the authors show for the first time an elementary proof for the best known bound $d \leq N^{0.292}$. Moreover, the authors show that for so-called small CRT-RSA exponents one has a polynomial time attack up to the bound $N^{0.073}$.

In many side-channel attacks, such as e.g. cold boot attacks, one recovers only an error-prone version of a secret cryptographic key as the partial information. But many cryptographic keys are stored with a lot of redundancy. E.g. for RSA with modulus $N = pq$ one usually stores in addition to the secret exponent d the prime factorization p, q and additional data, that helps to speed up the decryption process. Thus, the redundancy of the stored data serves as an error correction code that allows to correct some faulty bits. In [133] the authors provide a polynomial time error correction algorithm for faulty RSA keys that recomputes the original key with high probability as long as at most an 0.237-fraction of the key's bits are flipped. In principle, the algorithm is not limited to the RSA setting and maybe transferred to other settings with faulty secret key material as well.

In most past work on factoring with partial information oracles the attacker knows some of the bits of one of the factors, usually the most significant bits or chunks of bits spread over one of the factors. The authors of [50] consider the particular case of factoring unbalanced RSA moduli with known bits from the larger factor. More precisely, they show that, using

Coppersmith and Boneh-Durfee techniques, an unbalanced RSA modulus $n = pq > q^3$ can be factored efficiently given $2\log_2 q$ contiguous bits of p, or fewer depending on the position of the known bit pattern.

At TCC 2005, Groth [270] underlined the usefulness of working in small RSA subgroups of hidden order. In assessing the security of the relevant hard problems, however, the best attack considered for a subgroup of size $2^{2\ell}$ had a complexity of $\widetilde{O}2^{\ell}$. Accordingly, $\ell = 100$ bits was suggested as a concrete parameter. The authors of [76] exhibit a baby step, giant step-like attack with a complexity of roughly $2^{\ell/2}$ operations, suggesting that Groth's original choice of parameters was overly optimistic.

10.2 General Factoring

One of the best general factorization methods available is the Elliptic-Curve Method (ECM), introduced in the 1987 paper [291]. The state-of-the-art implementation is GMP-ECM described in [316]. The authors of [33] have built a new ECM implementation, "EECM-MPFQ", that uses fewer modular multiplications than GMP-ECM, takes less time than GMP-ECM, and finds more primes than GMP-ECM. The first prototype of EECM-MPFQ was "GMP-EECM", a program that added various improvements to GMP-ECM. The article [33] presents the background and speed results for EECM-MPFQ. The authors of [33] analyze the impact of Edwards curves on ECM, not just in multiplication counts but also in real-world software speeds. The main improvements above the modular-arithmetic level are as follows:

1. use Edwards curves instead of Montgomery curves;
2. use extended Edwards coordinates;
3. use signed-sliding-window addition-subtraction chains;
4. batch primes to increase the window size;
5. choose curves with small parameters and base points;
6. choose curves with large torsion.

10.3 Discrete Logarithms

Gaudry and Schost [266] developed, in the context of point counting, a versatile approach to low storage algorithms for variants of the discrete logarithm problem (DLP). Galbraith and Ruprai [118] gave some general improvements to this method. They then focussed attention on the discrete logarithm problem in an interval of size N, namely: given g and h such that $h = g^a$ for some $0 \leq a < N$, to compute a. The Pollard kangaroo algorithm was previously the standard method to attack this problem. In the formulation using distinguished points (as proposed by van Oorschot and Wiener), it has heuristic average-case expected running time approximately $2\sqrt{N}$ group operations.

Galbraith, Pollard and Ruprai [120] have shown how to reduce this to (again, heuristic average-case expected running time) approximately $1.66\sqrt{N}$ group operations.

A further speedup is available in groups (such as elliptic curves) with a very fast inversion map. Galbraith and Ruprai [119] give an algorithm to solve the DLP in an interval of size N

in such groups with heuristic average-case expected running time of close to $1.36\sqrt{N}$ group operations.

10.4 Code Based Systems

The McEliece cryptosystem [296] is one of the oldest public-key scheme. Since its invention thirty years ago, no efficient attack had been devised that managed to recover the private key. The work of [96] shows that the private key of the cryptosystem satisfies a system of overdetermined bi-linear polynomial equations [99]. This property is due to the particular class of codes considered which are alternant codes. The authors of [96] used these highly structured algebraic equations to mount an efficient key-recovery attack against two recent variants of McEliece that aim at reducing public key sizes [230, 298]. These two compact variants of McEliece managed to propose keys with less than 20,000 bits. To do so, [230, 298] proposed to use quasi-cyclic or dyadic structures. According to [96], an implementation of the algebraic attack using the computer algebra system MAGMA allows to find the secret-key in a negligible time (less than one second) for almost all the proposed challenges. For instance, a private key designed for a 256-bit security can be recovered in 0.06 seconds with about $2^{17.8}$ operations.

The authors of [97] have investigated the difficulty of the so-called Goppa Code Distinguishing (GD) problem introduced by Courtois, Finiasz and Sendrier at Asiacrypt 2001 [251]. GD is the problem of distinguishing the public matrix in the McEliece cryptosystem from a random matrix. It is widely believed that this problem is computationally hard as proved by the increasing number of papers using this hardness assumption. Disproving/mitigating this hardness assumption is a breakthrough in code-based cryptography and may open a new direction to attack McEliece cryptosystems. The paper presents an efficient distinguisher for alternant and Goppa codes of high rate over binary/non binary fields. The distinguisher is based on a recent algebraic attack against compact variants of McEliece which reduces the key-recovery to the problem of solving an algebraic system of equations [96]. The paper exploits a defect of rank in the (linear) system obtained by linearizing this algebraic system. It turns out that the distinguisher is highly discriminant. Indeed, one can then precisely quantify the defect of rank for "generic" binary and non-binary random, alternant and Goppa codes. The paper have verifies these formulas with practical experiments, and a theoretical explanation for such defect of rank is also provided. According to [97], this work permits to shed some light on the choice of secure parameters for McEliece cryptosystems; a topic thoroughly investigated recently. The technique of [97] permits to indeed distinguish a public key of the CFS signature [251] scheme for all parameters proposed by Finiasz and Sendrier at Asiacrypt 2009 [263]. Moreover, some realistic parameters of McEliece scheme also fit in the range of validity of such distinguisher.

Computing loci of rank defects of linear matrices (also called the MinRank problem) is a fundamental NP-hard problem of linear algebra which has applications in Cryptology, in Error Correcting Codes and in Geometry. Given a square linear matrix (i.e. a matrix whose entries are k-variate linear forms) of size n and an integer r, the problem is to find points such that the evaluation of the matrix has rank less than $r + 1$. In [98], the authors try to obtain the most efficient algorithm to solve this problem. To this end, the paper uses the theoretical and practical complexity of computing Gröbner bases of two algebraic formulations of the MinRank problem [252]. Both modelings lead to structured algebraic systems. The first modeling, proposed by Kipnis and Shamir [288] generates bihomogeneous equations of bi-degree $(1,1)$. The second one is classically obtained by the vanishing of the $(r+1)$-minors of the given matrix, giving rise to a determinantal ideal. In both cases, under genericity assumptions on the entries of the considered matrix, the authors of [98] give new bounds on the degree of regularity of the considered ideal which allows us to estimate the complexity of the whole Gröbner bases computations. For instance, the exact degree of regularity of the determinantal ideal formulation of a generic well-defined MinRank problem is $r(n-r)+1$. The paper also gives optimal degree bounds of the loci of rank defect which are reached under genericity assumptions; the new bounds are much lower than the standard multi-homogeneous Bézout bounds (or mixed volume of Newton polytopes). As a by-product, it is proved that the generic MinRank problem could be solved in polynomial time in n (when $n-r$ is fixed) as announced in a previous paper of Faugère, Levy-dit-Vehel and Perret [262]. Moreover, using the determinental ideal formulation, these results are used to break a cryptographic challenge – which was untractable so far – and allow us to evaluate precisely the security of the cryptosystem w.r.t. n, r and k. The practical results suggest that, up to the software state of the art, this latter formulation is more suitable in the context of Gröbner bases computations.

10.5 Attacks on Other Proposals

The authors of [100] have fully broken the Algebraic Surface Cryptosystem (ASC for short) proposed at PKC'2009 [220]. This system is based on an unusual problem in multivariate cryptography: the Section Finding Problem. Given an algebraic surface $X(x,y,t) \in \mathbb{F}_p[x,y,t]$ such that $\deg_{xy} X(x,y,t) = w$, the question is to find a pair of polynomials of degree d, $u_x(t)$ and $u_y(t)$, such that $X(u_x(t), u_y(t), t) = 0$. In ASC, the public key is the surface, and the secret key is the section. This asymmetric encryption scheme enjoys reasonable sizes of the keys: for recommended parameters, the size of the secret key is only 102 bits and the size of the public key is 500 bits. The propose a message recovery attack whose complexity is quasi-linear in the size of the secret key. The main idea of this algebraic attack is to decompose ideals deduced from the ciphertext in order to avoid to solve the section finding problem. Experimental results show that we can break the cipher for recommended parameters (the security level is 2^{102}) in 0.05 seconds. Furthermore, the attack still applies even when the secret key is very large (more than 10000 bits). The complexity of the attack is $\widetilde{\mathcal{O}}(w^7 d \log(p))$ which is polynomial with respect to all security parameters. In particular, it is quasi-linear in the size of the secret key which is $(2d+2)\log(p)$. This result is rather surprising since the algebraic attack is often more efficient than the legal decryption algorithm.

The authors of [94] presented an efficient cryptanalysis of the so-called HM cryptosystem which was published at Asiacrypt'1999, and one perturbed version of HM. Until now, this scheme was exempt from cryptanalysis. The authors first provided a distinguisher which uses a differential property of the public key. This distinguisher permits to break one perturbed version of HM. After that, the authors describe a practical message-recovery attack against HM using Gröbner bases. The attack can be mounted in few hundreds seconds for recommended parameters. It turns out that algebraic systems arising in HM are easier to solve than random systems of the same size. This fact provides another distinguisher for HM. Interestingly enough, the authors offere an explanation why algebraic systems arising in HM are easy to solve in practice. Briefly, this is due to the apparition of many new linear and quadratic equations during the Gröbner basis computation. More precisely, the paper provides an upper bound on the maximum degree reached during the Gröbner basis computation (a.k.a. the degree of regularity) of HM systems. For $\mathbb{F}_2$, which is the initial and usual setting of HM, the degree of regularity is upper-bounded by 3. In general, this degree of regularity is upper-bounded by 4. These bounds allow a polynomial-time solving of the system given by the public equations in any case. All in all, the paper shows that the HM scheme is broken for all practical parameters.

The authors of [35] present an improved approach to solve multivariate systems over finite fields. The approach is a tradeoff between exhaustive search and Gröbner bases techniques. The authors give theoretical evidences that our method brings a significant improvement in a very large context and we clearly define its limitations. The efficiency depends on the choice of the tradeoff. The analysis gives an explicit way to choose the best tradeoff as well as an approximation. From the analysis, a new general algorithm to solve multivariate polynomial systems is given. The theoretical results are experimentally supported by successful cryptanalysis of several multivariate schemes (TRMS, UOV, ...). As a proof of concept, the authors of were able to break the proposed parameters assumed to be secure until now. Parameters that resists to this method are also explicitly given. This works permits to refine the parameters to be chosen for multivariate schemes.

The authors of [212] broke the Double-Layer Square and Square+ encryption schemes using a refined MinRank key recovery attack over the ground field and extension field respectively. Both schemes are variants of the multivariate quadratic encryption scheme Square and where proposed at PQCrypto 2010. It is also outlined how possible variants such as Square- or multi-Square can be attacked.

The authors of [213] extended the algorithm from Kipnis-Patarin-Goubin (extended version of Eurocrypt '99) to solve underdetermined systems of multivariate quadratic equations mainly over fields of even characteristic. They showed a gradual decrease of complexity for the number of variables n between m, the number of equations, and m(m+1). This new algorithm forced to increase parameters of the Unbalanced Oil and Vinegar public key signature scheme.

In [10] the relationship between techniques for solving polynomial systems of equations as proposed in cryptography and well-known technique from computer algebra are investigated. In particular, the the MXL family of algorithms (MXL, MXL2, MXL3) is compared with the F4 algorithm for computing Grbner bases. The paper maps all novel concepts from the MXL family of algorithms to their well-known Grbner basis equivalents. Using previous results that had shown the relation between the original XL algorithm and F4, the paper concludes that the MXL family of algorithms can be fundamentally reduced to redundant variants of the F4 algorithm.

The authors of [210] prove a theoretical bound on the number of linearly independent equations produced by special equations, so-called mutants, in a variant of the well known XL algorithm.

The authors of [211] give a full overview form Relinearization over XL to MutantXL and provide some additional proofs. They show that MutantXL solves as soon as mutants occur, which always happens at the degree of regularity or at least one degree above.

The Rainbow signature scheme is a layered variant of the well-known Unbalanced Oil and Vinegar signature scheme reducing the length of the signature. But still the public and secret keys are comparably large. At CT-RSA 2012 a new variant of Rainbow was published, which used non-commutative rings to reduce the key size. The author of [209] revealed some weaknesses of this new variant against MinRank and HighRank attacks and showed how to use the additional structure to attack the scheme.

The authors of [81] reviewed the latest cryptanalysis of the three multivariate quadratic signature schemes Unbalanced Oil and Vinegar, Rainbow and enhTTS. They provided parameters for the same level of security and implemented those schemes on an 8-bit microcontroller. This way they were able to compare those schemes in terms of key length, number of operations, running time and code size.

The authors of [214] presented a generalization of equivalent keys which allowed to generalize a large class of algebraic key recovery attacks against multivariate quadratic schemes. Using this new framework they managed to break the STS signature scheme and all its variants by an algebraic key recovery attack.

Chapter 11

Implementation Research

11.1 Elliptic Curve Cryptography

Efficiently computable homomorphisms allow elliptic curve point multiplication to be accelerated using the Gallant-Lambert-Vanstone [265] (GLV) method. Iijima, Matsuo, Chao and Tsujii [285] gave suitable homomorphisms for a large class of elliptic curves by working over $\mathbb{F}_{p^2}$. However, they did not use their construction for the GLV method. Galbraith, Lin and Scott [116] extended their results and demonstrate that they can be applied to the GLV method. In general the method is expected to require about 0.75 the time of previous best methods (except for subfield curves, for which Frobenius expansions can be used). Detailed implementation results are given in [116], which show that the method runs in between 0.70 and 0.83 the time of the previous best methods for elliptic curve point multiplication on general curves. Further work has been done by other authors. For example, Hankerson, Karabina and Menezes [276] analysed the method in characteristic 2 and also showed good speedups compared with random curves. However, when working in characteristic 2 one might prefer to use Koblitz curves and Frobenius expansions to obtain even faster elliptic curve exponentiation.

There have been many recent developments in formulae for efficient composite elliptic curve operations of the form $dP + Q$ for a small integer d and points P and Q where the underlying field is a prime field. To make best use of these in a scalar multiplication kP, it is necessary to generate an efficient "division chain" for the scalar where divisions of k are by the values of d available through composite operations. An algorithm-generating algorithm for this is presented in [217] that takes into account the different costs of using various representations for curve points. This extends the applicability of methods presented by Longa and Gebotys [293] to using specific characteristics of the target device. It also enables the transfer of some scalar recoding computation details to design time. An improved cost function also provides better evaluation of alternatives in the relevant addition chain. One result of these more general and improved methods includes a slight increase over the scalar multiplication speeds for the particular implementations reported in [293]. [217] presents examples which show that by the straightforward removal of rules for unusual cases, some particularly concise yet efficient presentations can be given for algorithms in the target device.

The use of elliptic curves in cryptography makes the key sizes smaller but the arithmetic of the underlying group is more tedious (for example, with the widely-used Jacobian coordinates, the general addition of two points on an elliptic curve typically requires 16 field multiplications). Therefore a huge amount of research has been devoted to the analysis of the performance of various forms of elliptic curves proposed in the mathematical literature: Weierstraß cubics, Jacobi intersections, Hessian curves, Jacobi quartics, or the more recent forms of elliptic curves due to Montgomery, Doche-Icart-Kohel or Edwards. The authors of [150] revisit yet another model for elliptic curves. This model was originally considered by G. Huff in 1948 over the field of rational numbers, to study a diophantine problem. Huff's model readily extends to any field of odd characteristic. Every elliptic curve over such a field and containing a copy of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is birationally equivalent to a Huff curve. The paper extends and generalizes Huff's model. It presents fast explicit formulas for point addition and doubling on Huff curves, featuring a number of useful properties, including completeness and independence from curve parameters. It also addresses the problem of the efficient evaluation of pairings over Huff curves.

In [63], the authors take a much more general approach and develop an algorithm to automatically scan a very large class of one-parameter families of elliptic curves for efficient arithmetic. The construction of the class is inspired by toric geometry, which provides a natural framework for the study of various forms of elliptic curves. The class both encompasses many prominent known forms and includes thousands of new forms. The algorithm that is described automatically computes the most compact group operation formulas for any parameterized family of elliptic curves. The generality of this algorithm is further illustrated by computing uniform addition formulas and formulas for generalized Montgomery arithmetic.

11.2 Pairing Based Systems

Many pairing based schemes, such as the IBE scheme of Boneh and Franklin [235], require a hash function which maps numeric values to points on an elliptic curve. The standard approach is to use a hash function of the form $m \mapsto f(h(m))$, where f is a suitably defined, constant-time, usually algebraic encoding function from the base field to the elliptic curve. Finding a suitable encoding f to ordinary curves is more complicated, but constructions are known for most cases; notable examples include the construction by Shallue and van de Woestijne [306], and the one by Icart [284]. However, it turns out that such functions f are not surjective. In fact, Icart conjectured in his paper that the image of the encoding he defined should contain about 5/8 of all points on the elliptic curve. This was proved using tools from algebraic number theory (particularly the Chebotarev density theorem) by the authors of [107] (a similar result was also established independently in [261]). They also demonstrate how similar techniques extend to any other encoding defined in algebraic terms, such as the simplified (univariate) Shallue-van de Woestijne encoding, which reaches about 3/8 of all curve points.

This last result implies in particular that if f is any of the known encodings to ordinary elliptic curves, it is easy to construct an efficient distinguisher between a "hash function" of the form $m \mapsto f(h(m))$ and a random oracle to the curve, even when h is modeled as a random oracle with values in the base field. This prompted the authors of [49] to investigate the problem of finding functions F for which $m \mapsto F(h(m))$ is indifferentiable from a random oracle to the curve. They first give a set of axiomatic conditions that F must satisfy, and then prove using algebraic geometry that these conditions are satisfied by $F(x, y) = f(x) + f(y)$, where f is Icart's function and $+$ is the addition of curve points. In particular, $m \mapsto f(h_1(m)) + f(h_2(m))$ can be used as a random oracle to the curve provided that h_1, h_2 are modeled as random oracles to the base field.

The authors of [108] propose a very simple and efficient encoding function from $\mathbb{F}_q$ to points of a hyperelliptic curve over $\mathbb{F}_q$ of the form $H\colon y^2 = f(x)$ where f is an odd polynomial. Hyperelliptic curves of this type have been frequently considered in the literature to obtain Jacobians of good order and pairing-friendly curves. The new encoding is nearly a bijection to the set of $\mathbb{F}_q$-rational points on H. This makes it easy to construct well-behaved hash functions to the Jacobian J of H, as well as injective maps to $J(\mathbb{F}_q)$ which can be used to encode scalars for such applications as El Gamal encryption. The new encoding is already interesting in the genus 1 case, where it provides a well-behaved encoding to Joux's supersingular elliptic curves.

11.3 Post-Quantum Systems

The best known non-structural attacks against code-based cryptosystems are based on information-set decoding. Stern's algorithm and its improvements are well optimized and the complexity is reasonably well understood. However, these algorithms only handle codes over $\mathbb{F}_2$. Several articles have suggested to use base fields other than $\mathbb{F}_2$ for the McEliece cryptosystem. This idea is interesting as it has the potential to reduce the public-key size. The analysis in [231] showed that in order to achieve 128-bit security the McEliece private key should be a binary Goppa code of length 2960 and dimension 2288 with a degree-56 Goppa polynomial and 57 added errors. Using an equal-size code over $\mathbb{F}_q$ would save a factor of $\lg q$: row and column dimension of the generator matrix both shrink by a factor of $\lg q$ at the cost of the matrix entries having size $\lg q$. However, information-set-decoding algorithms do not scale purely with the code size. It is important to understand the implications of changing from $\mathbb{F}_2$ to $\mathbb{F}_q$ for arbitrary prime powers q on the attacks. The article [186] generalizes Lee–Brickell's algorithm and Stern's algorithm to decoding algorithms for codes over arbitrary fields and extends the improvements from [231] and [263]. In [186] a precise analysis of these improved and generalized algorithms is given. For $q = 31$, Goppa code parameters (length n, dimension k, and degree t of the Goppa polynomial) are presented that require 2^{128} bit operations to compute the closest codeword, i.e., to break McEliece's system using a Goppa code over $\mathbb{F}_{31}$.

In particular, [186] showed that codes over $\mathbb{F}_{31}$ offer advantages in key size compared to codes over $\mathbb{F}_2$ while maintaining the same security level against all attacks known. However, codes over smaller fields such as $\mathbb{F}_3$ are still not competitive in key size with codes over $\mathbb{F}_2$. The authors of [34] present a generalized cryptosystem that uses length-n codes over small finite fields $\mathbb{F}_q$ with dimension $\geq n - m(q-1)t$ efficiently correcting $\lfloor qt/2 \rfloor$ errors where $q^m \geq n$. These so-called "wild Goppa codes" are subfield codes over small $\mathbb{F}_q$ that have an increase in error-correcting capability by a factor of about $q/(q-1)$. McEliece's construction using binary Goppa codes is the special case $q = 2$ of that construction. Previously proposed cryptosystems with the same length and dimension corrected only $\lfloor (q-1)t/2 \rfloor$ errors for $q \geq 3$. The extra factor $q/(q-1)$ in the error-correction capability makes "larger tiny fields" attractive and bridges the gap between $\mathbb{F}_2$ and $\mathbb{F}_{31}$. The authors of [34] also present list-decoding algorithms that efficiently correct even more errors for the same codes over $\mathbb{F}_q$. They show that the increase from $\lfloor (q-1)t/2 \rfloor$ errors to more than $\lfloor qt/2 \rfloor$ errors allows considerably smaller keys to achieve the same security level against all known attacks. Moreover, [34] contains parameter sizes for different finite fields to achieve 128-bit security against the information-set-decoding attack presented in [186].

Decoding random linear codes is a fundamental problem in complexity theory and lies at the heart of almost all code-based cryptography. The best attacks on the most prominent code-based cryptosystems such as McEliece directly use decoding algorithms for linear codes. The asymptotically best decoding algorithm for random linear codes of length n was for a long time Sterns variant of information-set decoding running in time $2^{0.05563n}$. Following on from the work of [34], which provided an exponential speed-up over Sterns algorithm by improving the running time to $2^{0.05558n}$, the paper [167] presents a new algorithm for decoding linear codes that is inspired by a representation technique due to Howgrave-Graham and Joux in the context of subset sum algorithms. The new decoding algorithm brings the time complexity down to $2^{0.05363n}$. The paper [31] shows how to further increase the number of representations which eventually yields a new information set decoding algorithm with running time $2^{0.0494n}$.

The authors of [187] showed how post-quantum signature schemes based on multivariate quadratic polynomials can be improved up by 88% and 59%, respectively, in terms of public key size and verification time. Their new scheme is a variant of the so-called Unbalanced Oil and Vinegar scheme. Using the theory of equivalent keys they provided evidence that their reduction does not affect security and that it is also optimal in terms of possible attacks.

Bibliography

[1] M. Abdalla, M. Bellare and G. Neven. Robust Encryption. *Theory of Cryptography Conference – TCC 2010*, Springer LNCS 5978, 480–497, 2010.

[2] M. Abdalla, J. Birkett, D. Catalano, A.W. Dent, J. Malone-Lee, G. Neven, J.C.N. Schuldt and N.P. Smart. Wildcarded Identity-Based Encryption. *Journal of Cryptology*, **24**, 42–82, 2011.

[3] M. Abdalla, X. Boyen, C. Chevalier, and D. Pointcheval. Distributed Public-Key Cryptography from Weak Secrets. *Public Key Cryptography – PKC 2009*, Springer LNCS 5443, 139–159, 2009

[4] M. Abdalla, D. Catalano, C. Chevalier, and D. Pointcheval. Password-Authenticated Group Key Agreement with Adaptive Security and Contributiveness. *Progress in Cryptology – AFRICACRYPT 2009*, Springer LNCS 5580, 254–271, 2009.

[5] M. Abdalla, D. Catalano and D. Fiore. Verifiable Random Functions from Identity-Based Key-Encapsulation. *Advances in Cryptology – EUROCRYPT 2009*, Springer LNCS 5479, 554–571, 2009.

[6] M. Abdalla, C. Chevalier, and D. Pointcheval. Smooth Projective Hashing for Conditionally Extractable Commitments. *Advances in Cryptology – CRYPTO 2009*, Springer LNCS 5677, 671–689, 2009.

[7] M. Abdalla, C. Chevalier, M. Manulis and D. Pointcheval. Flexible Group Key Exchange with On-demand Computation of Subgroup Keys. *Progress in Cryptology – AFRICACRYPT 2010*, Springer LNCS 6055, 351–368, 2010.

[8] M. Abdalla, M. Izabachène, and D. Pointcheval. Anonymous and Transparent Gateway-based Password-Authenticated Key Exchange. *Cryptology and Network Security – CANS 2008*, Springer LNCS 5339, 133–148, 2008.

[9] M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M. Ohkubo. Structure-preserving signatures and commitments to group elements. *Advances in Cryptology – CRYPTO 2010* , Springer LNCS 6223, 209–236, 2010.

[10] M.R. Albrecht, C.Cid, J.-C. Faugère and L. Perret. On the Relation Between the Mutant Strategy and the Normal Selection Strategy in Gröbner Basis Algorithms. To appear *Journal for Symbolic Computation.*

[11] M.R. Albrecht, P. Farshim, J.-C. Faugére and L. Perret. Polly Cracker, Revisited. *Advances in Cryptology – ASIACRYPT 2011*, Springer LNCS 7073, 179–196, 2011.

[12] M.R. Albrecht, P. Farshim, K.G. Paterson, and G.J. Watson. On Cipher-Dependent Related-Key Attacks in the Ideal-Cipher Model. *Fast Software Encryption – FSE 2011*, Springer LNCS 6733, 128–145, 2011.

[13] M.R. Albrecht and K.G. Paterson. Breaking An Identity-Based Encryption Scheme based on DHIES. *Cryptography and Coding – 2011*, Springer LNCS 7089, 344–355, 2011.

[14] M.R. Albrecht, G.J. Watson and K.G. Paterson. Plaintext Recovery Attacks Against SSH. *IEEE Symposium on Security and Privacy – 2009*, IEEE Computer Society 2009, 16–26, 20009.

[15] J.B. Almeida, E. Bangerter, M. Barbosa, S. Krenn, A.-R. Sadeghi and T. Schneider. A Certifying Compiler for Zero-Knowledge Proofs of Knowledge Based on Sigma-Protocols. *European Symposium on Research in Computer Security – ESORICS 2010*, Springer LNCS 6345, 151–167, 2010.

[16] J. Alwen and a. shelat and I. Visconti. Collusion-Free Protocols in the Mediated Model *Advances in Cryptology – CRYPTO 2008*, Springer LNCS 5157, 497–514, 2008.

[17] J. Alwen, J. Katz, Y. Lindell, G. Persiano, a. shelat and I. Visconti. Collusion-Free Multiparty Computation in the Mediated Model. *Advances in Cryptology – CRYPTO 2009*, Springer LNCS 5677, 524–540, 2009.

[18] F. Armknecht, L. Chen, A.-R. Sadeghi and C. Wachsmann. Anonymous Authentication for RFID Systems. *Workshop on RFID Security – RFIDSec 10*, 2010. Springer LNCS 6370, 158–175, 2010.

[19] F. Armknecht, A.-R. Sadeghi, I. Visconti and C. Wachsmann. On RFID Privacy with Mutual Authentication and Tag Corruption. *Applied Cryptography and Network Security – ACNS 2010*, Springer LNCS 6123, 493–510, 2010.

[20] F. Armknecht, A-R. Sadeghi, A. Scafuro, I. Visconti and C. Wachsmann. Impossibility Results for RFID Privacy Notions. *Transactions on Computational Science*, **11**, 457–473, 2010.

[21] N. Attrapadung and B. Libert. Homomorphic Network Coding Signatures in the Standard Model. *Public Key Cryptography 2011 (PKC'11)*, Springer LNCS 6571, 17–34, 2011.

[22] N. Attrapadung, B. Libert and E. de Panafieu. Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts. *Public Key Cryptography 2011 (PKC'11)*, Springer LNCS 6571, 90–108, 2011.

[23] E. Bangerter, T. Briner, W. Henecka, S. Krenn, A.-R. Sadeghi and T. Schneider. Automatic Generation of Sigma-Protocols. *European Workshop on Public Key Services, Applications and Infrastructures – EUROPKI 2009*, Springer LNCS 6391, 67–82, 2009.

[24] M. Barbosa and P. Farshim. Security Analysis of Standard Authentication and Key Agreement Protocols Utilising Timestamps. *Progress in Cryptology – AFRICACRYPT 2009*, Springer LNCS 5580, 235–253, 2009.

[25] M. Barbosa and P. Farshim. Relations Among Notions of Complete Non-Malleability: Indistinguishability Characterisation and Efficient Construction without Random Oracles. *Information Security and Privacy – ACISP 2010*, Springer LNCS 6168, 145–163, 2010.

[26] M. Barbosa and P. Farshim. Strong Knowledge Extractors for Public-Key Encryption Schemes. *Information Security and Privacy – ACISP 2010*, Springer LNCS 6168, 164–181, 2010.

[27] M. Barbosa and P. Farshim. Delegatable homomorphic encryption with applications to secure outsourcing of computation. In *Topics in Cryptology – CT-RSA 2012* Springer LNCS 7178, 296–312, 2012.

[28] M. Barni, P. Failla, V. Kolesnikov, R. Lazzeretti, A.-R. Sadeghi and T. Schneider. Secure Evaluation of Private Linear Branching Programs with Medical Applications. *European Symposium on Research in Computer Security – ESORICS 09*, Springer LNCS 5789, 424–439, 2009.

[29] G. Barthe, A. Hevia, Z. Luo, T. Rezk and B. Warinschi. Robustness Guarantees for Anonymity. IEEE Computer Security Foundations Symposium – CSF 2010, IEEE Computer Society, 91–106, 2010.

[30] A. Bauer, J.-S. Coron, D. Naccache, M. Tibouchi and D. Vergnaud. On the Broadcast and Validity-Checking Security of PKCS#1 v1.5 Encryption. *Applied Cryptography and Network Security - ACNS 2010*, Springer LNCS 6123, 1–18, 2010.

[31] A. Becker, A.Joux, A.May and A. Meurer. Decoding Random Binary Linear Codes in $2^{n/20}$: How $1 + 1 = 0$ Improves Information Set Decoding *Advances in Cryptology – EUROCRYPT 2012*, Springer LNCS 7237, 520–536, 2012.

[32] D. Bernhard, E. Ghadafi, G. Fuschbauer, N.P. Smart and B. Warinschi. Anonymous attestation with user-controlled linkability. *Cryptology ePrint Archive*, Report 2011/658.

[33] D. J. Bernstein, P. Birkner, T. Lange, and C. Peters. ECM using Edwards curves. *Cryptology ePrint Archive*, Report 2008/016.

[34] D. J. Bernstein, T. Lange, and C. Peters. Wild McEliece. *Selected Areas in Cryptography – SAC 2010*, Springer LNCS 6544, 143–158, 2011.

[35] L. Bettale, J.-C. Faugère, and L. Perret. Hybrid approach for solving multivariate systems over finite fields. *Journal of Mathematical Cryptology*, **3**, 177–197, 2010.

[36] P. Bichsel, J. Camenisch, G. Neven, N.P. Smart and B. Warinschi. Get shorty via group signatures without encryption. *Security and Cryptography for Networks – SCN 2010*, Springer LNCS 6280, 381–398, 2010.

[37] M. Björkqvist, C. Cachin, R. Haas, X. Hu, A. Kurmus, R. Pawlitzek and M. Vukolić Design and Implementation of a Key-Lifecycle Management System. *Financial Cryptography and Data Security – FC 2010*, Springer LNCS 6052, 160–174, 2010.

[38] O. Blazy, S. Canard, G. Fuchsbauer, A. Gouget, H. Sibert, and J. Traoré. Achieving Optimal Anonymity in Transferable E-cash with a Judge. *Progress in Cryptology – AFRICACRYPT 2011*, Springer LNCS 6737, 206–223, 2011.

[39] O. Blazy, G. Fuchsbauer, M. Izabachène, A. Jambert, H. Sibert, and D. Vergnaud. Batch Groth-Sahai. *Applied Cryptography and Network Security – ACNS 2010*, Springer LNCS 6123, 218–235, 2010.

[40] O. Blazy, G. Fuchsbauer, D. Pointcheval, and D. Vergnaud. Signatures on Randomizable Ciphertexts. *Public-Key Cryptography – PKC 2011*, Springer LNCS 6571, 403–422, 2011.

[41] O. Blazy, D. Pointcheval, and D. Vergnaud. Round-Optimal Privacy-Preserving Protocols with Smooth Projective Hash Functions. *Theory of Cryptography Conference, TCC 2012*, Springer LNCS 7194, 94-111, 2012.

[42] C. Blundo, V. Iovino and G. Persiano. Private-Key Hidden Vector Encryption with Key Confidentiality *Cryptology and Network Security - CANS 2009*, Springer LNCS, to appear, 2009.

[43] C. Blundo, V. Iovino and G. Persiano. Predicate Encryption with Partial Public Keys. *Cryptology and Network Security – CANS 2010*, Springer LNCS 6467, 298–313, 2010.

[44] C. Blundo, G. Persiano, A.-R. Sadeghi and I. Visconti. Improved Security Notions and Protocols for Non-Transferable Identification *European Symposium on Research in Computer Security – ESORICS 2008*, Springer LNCS 5283, 364–368, 2008.

[45] A. Boldyreva, J.P. Degabriele, K.G. Paterson and M. Stam. Security of Symmetric Encryption in the Presence of Ciphertext Fragmentation. *Advances in Cryptology – EUROCRYPT 2012*, Springer LNCS 7237, 682–699, 2012.

[46] A. Boldyreva, M. Fischlin, A. Palacio and B. Warinschi. A closer look at PKI: security and efficiency. *Public Key Cryptography – PKC 2007*, Springer LNCS 4450, 458–475, 2007.

[47] M. Bond, G. French, N.P. Smart and G.J. Watson. The low-call diet: Authenticated Encryption for call counting HSM users. To appear *Topics in Cryptology – CT-RSA 2012.*

[48] X. Boyen, C. Chevalier, G. Fuchsbauer, and D. Pointcheval. Strong cryptography from weak secrets. *Progress in Cryptology – AFRICACRYPT 2010*, Springer LNCS 6055, 297–315, 2010.

[49] E. Brier, J.-S. Coron, T. Icart, D. Madore, H. Randriam and M. Tibouchi. Efficient Indifferentiable Hashing into Ordinary Elliptic Curves. *Advances in Cryptology - CRYPTO 2010*, Springer LNCS 6223, 237–254, 2010.

[50] E. Brier, D. Naccache and M. Tibouchi. Factoring Unbalanced Moduli with Known Bits. *Information, Security and Cryptology - ICISC 2009*, Springer LNCS 5984, 65–72, 2009.

[51] E. Brier, D. Naccache, P.Q. Nguyen and M. Tibouchi. Modulus Fault Attacks against RSA-CRT Signatures. *Cryptographic Hardware and Embedded Systems - CHES 2011*, Springer LNCS 6917, 192–206, 2011.

[52] J. Bringer, H. Chabanne, D. Pointcheval, and S. Zimmer. An Application of the Boneh and Shacham Group Signature Scheme to Biometric Authentication. *International Workshop on Security – IWSEC 2008*, Springer LNCS 5312, pages 219-230, 2008.

[53] B. Brumley, M. Barbosa, D. Page, and F. Vercauteren. Practical realisation and elimination of an ecc-related software bug attack. *Topics in Cryptology – CT-RSA 2012*, Springer LNCS 7178, 171–186, 2012.

[54] C. Brzuska, M. Fischlin, T. Freudenreich, A. Lehmann, M. Page, J. Schelbert, D. Schröder and F. Volk. Security of Sanitizable Signatures Revisited. *Public-Key Cryptography – PKC 2009*, Springer LNCS 5443, 317–336, 2009.

[55] C. Brzuska, M. Fischlin, N.P. Smart, B. Warinschi and S. Williams. Less is More: Relaxed yet Composable Security Notions for Key Exchange. *Cryptology ePrint Archive*, Report 2012/242.

[56] C. Brzuska, M. Fischlin, B. Warinschi, and S. Williams. Composability of Bellare-Rogaway key exchange protocols. *ACM Conference on Computer and Communications Security – CCS 2011*, ACM, 51–62, 2011.

[57] C. Cachin. Integrity and consistency for untrusted services. *Current Trends in Theory and Practice of Computer Science – SOFSEM 2011*, Springer LNCS 6543, 1–14, 2011.

[58] J. Camenisch, M. Dubovitskaya and G. Neven. Oblivious Transfer with Access Control. *Computer and Communications Security – ACM CCS 2009*, 131–140, 2009.

[59] S. Canard, G. Fuchsbauer, A. Gouget, and F. Laguillaumie. Plaintext-Checkable Encryption. *Topics in Cryptology – CT-RSA 2012*, Springer LNCS 7178, 332–348, 2012.

[60] S. Canard, A. Jambert and R. Lescuyer. Signatures with Several Signers and Sanitizers. *Progress in Cryptology - AFRICACRYPT 2012*, Springer LNCS 7374, 35-52, 2012.

[61] Z. Cao, I. Visconti and Z. Zhang. Constant-Round Concurrent Non-Malleable Statistically Binding Commitments and Decommitments. *Public-Key Cryptography – PKC 2010*, Springer LNCS 6056, 193–208, 2010.

[62] Z. Cao, I. Visconti and Z. Zhang. On constant-round concurrent non-malleable proof systems. *Inf. Process. Lett.*, **111**, 883–890, 2011.

[63] W. Castryck and F. Vercauteren. Toric forms of elliptic curves and their arithmetic. *Journal of Symbolic Computation*, **46**, 943–966, 2011.

[64] D. Catalano, D. Fiore, and B. Warinschi Adaptive pseudofree groups and applications *Advances in Cryptology-EUROCRYPT 2011*, Springer LNCS 6632, 207-223, 2011.

[65] E. Cesena, H. Löhr, G. Ramunno, A.-R. Sadeghi and D. Vernizzi. Anonymous Authentication with TLS and DAA. *Trust and Trustworthy Computing – TRUST 2010*, Springer LNCS 6101, 47–62, 2010.

[66] R. Chaabouni, H. Lipmaa, and a. shelat. Additive combinatorics and discrete logarithm based range proofs. *Information Security and Privacy – ACISP 2010*, Springer LNCS 6168, 336–351, 2010.

[67] R. Chaabouni and S. Vaudenay. The Extended Access Control for Machine Readable Travel Documents. *Biometrics and Electronic Signatures – BIOSIG 2009*, GI LNI 155, 93–103, 2009

[68] L. Chen, M.-F. Lee and B. Warinschi. Security of the TCG Privacy-CA Solution. *Embedded and Ubiquitous Computing – EUC 2010*, IEEE, 609–616, 2010.

[69] L. Chen, P. Morrissey and N.P. Smart. On proofs of security for DAA schemes *Provable Security – ProvSec 2008*, Springer LNCS 5324, 167–175, 2008.

[70] L. Chen, P. Morrissey, N.P. Smart and B. Warinschi. Security notions and general construcitons for client puzzles. *Advances in Cryptology – ASIACRYPT 2009*, Springer LNCS 5912, 505–523, 2009.

[71] C. Chevalier, P.-A. Fouque, D. Pointcheval and S. Zimmer. Optimal Randomness Extraction from a Diffie-Hellman Element. *Advances in Cryptology – EUROCRYPT 2009*, Springer LNCS 5479, 572–589, 2009.

[72] C. Cho, R. Ostrovsky, A. Scafuro and I. Visconti. Simultaneously resettable arguments of knowledge. *Theory of Cryptography Conference – TCC 2012*, Springer LNCS 7194, 530–547, 2012.

[73] A. Choudhury and A. Patra. On the Communication Complexity of Reliable and Secure Message Transmission in Asynchronous Networks. *Conference on Information Security and Cryptology — ICISC 2011*, Springer LNCS 7259, 450–466, 2012.

[74] A. Choudhury and Arpita Patra. Brief Announcement: Efficient Optimally Resilient Statistical AVSS and Its Applications. *Principles of Distributed Computing – PODC 2012*, ACM, 103–104, 2012.

[75] A. Choudhury. Brief Announcement: Optimal Amortized Secret Sharing with Cheater Identification. *Principles of Distributed Computing – PODC 2012*, ACM, 101–102. 2012.

[76] J.-S. Coron, A. Joux, A. Mandal, D. Naccache and M. Tibouchi. Cryptanalysis of the RSA Subgroup Assumption from TCC 2005. *Public Key Cryptography - PKC 2011*, Springer LNCS 6571, 147–155, 2011.

[77] J.-S. Coron, A. Mandal, D. Naccache and M. Tibouchi. Fully Homomorphic Encryption over the Integers with Shorter Public Keys. *Advances in Cryptology - CRYPTO 2011*, Springer LNCS 6841, 487–504, 2011.

[78] J.-S. Coron, D. Naccache, M. Tibouchi and R.-P. Weinmann. Practical Cryptanalysis of ISO/IEC 9796-2 and EMV Signatures. *Advances in Cryptology - CRYPTO 2009*, Springer LNCS 5677, 428–444, 2009.

[79] J.-S. Coron, D. Naccache and M. Tibouchi. Fault Attacks Against EMV Signatures. *Topics in Cryptology - CT-RSA 2010*, Springer LNCS 5985, 208–220, 2010.

[80] V. Cortier and B. Warinschi. A composable computational soundness notion. *ACM Conference on Computer and Communications Security – CCS 2011*, ACM, 63–74, 2011.

[81] P. Czypek, S. Heyse and E. Thomae, Efficient Implementations of MQPKS on Constrained Devices. *Cryptographic Hardware and Embedded Systems – CHES 2012*, Springer LNCS, 2012.

[82] P. D'Arco, A. Scafuro, I. Visconti Revisiting DoS Attacks and Privacy in RFID-Enabled Networks. *Algorithmic Aspects of Wireless Sensor Networks – ALGOSENSORS 2009*, Springer LNCS 5804, 76–87, 2009.

[83] P. D'Arco and A. Scafuro and I. Visconti. Semi-Destructive Privacy in RFID Systems. *Workshop on RFID Security – RFIDSec 09*, 2009.

[84] A. De Caro, V. Iovino and G. Persiano. Fully Secure Anonymous HIBE and Secret-Key Anonymous IBE with Short Ciphertexts. *Pairing-Based Cryptography – Pairing 2010*, Springer LNCS 6487, 347–366, 2010.

[85] A. De Caro, V. Iovino and G. Persiano Efficient Fully Secure Predicate Encryption for Conjunctions, Disjunctions and k-CNF/DNF formulae. *Cryptology ePrint Archive*, Report 2010/492.

[86] A. De Caro and V. Iovino and G. Persiano Hidden Vector Encryption Fully Secure Against Unrestricted Queries. *Cryptology ePrint Archive*, Report 2011/546.

[87] J.P. Degabriele, A. Lehmann, K.G. Paterson, N.P. Smart and M. Strefler. On the joint security of encryption and signature in EMV. *Topics in Cryptology - CT-RSA 2012*, Springer LNCS 7178, 116–135, 2012.

[88] I. Damgård, V. Pastro, N.P. Smart and S. Zakarias. Multiparty computation from somewhat homomorphic encryption. *Advances in Cryptology – CRYPTO 2012*, Springer LNCS 7417, 643–662, 2012.

[89] I. Damgård, M. Keller, E. Larraia, C. Miles and N.P. Smart. Implementing AES via an Actively/Covertly Secure Dishonest-Majority MPC Protocol. *Security and Cryptography for Networks – SCN 2012*, Springer LNCS 7485, 241–263, 2012.

[90] A. W. Dent. A Brief Introduction to Certificateless Encryption Schemes and their Infrastructures. *Public Key Infrastructures – EuroPKI 2009*, Springer LNCS 6391, 1–16, 2009.

[91] A.W. Dent, M. Fischlin, M. Manulis, M. Stam and D. Schroder. Confidential Signatures and Deterministic Signcryption. *Public Key Cryptography - PKC 2010*, Springer LNCS 6056, 462–479, 2010.

[DSV11] M. Dubovitskaya, A. Scafuro and I. Visconti. Efficient non-interactive oblivious transfer with tamper-proof hardware. Technical Report, 2011.

[92] J. Fan, J. Hermans, and F. Vercauteren On the claimed privacy of EC-RAC III. *Workshop on RFID Security 2010*, Springer LNCS 6370, 66-74, 2010.

[93] P. Farshim and B. Warinschi. Certified encryption revisited. *Progress in Cryptology – AFRICACRYPT 2009*, Springer LNCS 5580, 179–197, 2009.

[94] J.-C. Faugère, A. Joux, L. Perret, and J. Treger. Cryptanalysis of the Hidden Matrix Cryptosystem. *Progress in Cryptology - LATINCRYPT 2010*, Springer LNCS 6212, 241–254, 2010.

[95] J.-C. Faugère, R. Marinier, and G. Renault. Implicit Factoring with Shared Most Significant and Middle Bits. *Public Key Cryptography – PKC 2010*, Springer LNCS 6056 , 70–87, 2010.

[96] J.-C. Faugère, A. Otmani, L. Perret, and J.-P. Tillich. Algebraic Cryptanalysis of McEliece variants with compact keys. *Advances in Cryptology – EUROCRYPT 2010*, Springer LNCS 6110, 279–298, 2010.

[97] J.-C. Faugère, A. Otmani, L. Perret, and J.-P. Tillich. A Distinguisher for High Rate McEliece Cryptosystems. *Cryptology ePrint Archive*, Report 2010/331.

[98] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Computing Loci of Rank Defects of Linear Matrices using Gröbner Bases and Applications to Cryptology. *Symbolic and Algebraic Computation – ISSAC '10*, ACM, 257–264, 2010.

[99] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Gröbner Bases of Bihomogeneous Ideals Generated by Polynomials of Bidegree (1,1): Algorithms and Complexity. *Journal of Symbolic Computation*, **46**, 406–437, 2011.

[100] J.-C. Faugère and P.-J. Spaenlehauer. Algebraic Cryptanalysis of the PKC'09 Algebraic Surface Cryptosystem. *Public Key Cryptography – PKC 2010*, Springer LNCS 6056, 35–52, 2010.

[101] D. Fiore and R. Gennaro. Making the Diffie–Hellman protocol identity-based. *Topics in Cryptology - CT-RSA 2010*, Springer LNCS 5985, 165–178, 2010.

[102] D. Fiore, R. Gennaro and N.P. Smart. Constructing certificateless encryption and ID-based encryption from ID-based key agreement. *Pairing-Based Cryptography – PAIRING 2010*, Springer-Velrag LNCS 6487, 167–186, 2010.

[103] M. Fischlin, A. Lehmann, T. Ristenpart, T. Shrimpton, M. Stam and S. Tessaro Random Oracles With(out) Programmability em Advances in Cryptology - Asiacrypt 2010, Springer LNCS 6477, 303-320, 2010

[104] M. Fischlin, B. Libert, M. Manulis. Non-interactive and Re-Usable Universally Composable String Commitments with Adaptive Security. *Advances in Cryptology – ASIACRYPT 2011*, Springer LNCS 7073, 468–485, 2011.

[105] M. Fischlin, B. Pinkas, A.-R. Sadeghi and T. Schneider. Secure Set Intersection with Untrusted Hardware Tokens. *Topics in Cryptology - CT-RSA 2011*, Springer LNCS 6558, 1–16, 2011.

[106] M. Fischlin and D. Schröder. Security of Blind Signatures under Aborts *Public-Key Cryptography – PKC 2009*, Springer LNCS 5443, 297–316, 2009.

[107] P.-A. Fouque and M. Tibouchi. Estimating the Size of the Image of Deterministic Hash Functions to Elliptic Curves. *Progress in Cryptology - LATINCRYPT 2010*, Springer LNCS 6212, 81–91, 2010.

[108] P.-A. Fouque and M. Tibouchi. Deterministic Encoding and Hashing to Odd Hyperelliptic Curves. *Pairing-Based Cryptography - Pairing 2010*, Springer , LNCS 6487, 265–277, 2010.

[109] E.S.V. Freire and K.G. Paterson. Provably Secure Key Assignment Schemes from Factoring. *Information Security and Privacy – ACISP 2011*, Springer LNCS 6812, 292–309, 2011.

[110] G. Fuchsbauer. Commuting Signatures and Verifiable Encryption. *Advances in Cryptology – EUROCRYPT 2011*, Springer LNCS 6632, 224–245, 2011.

[111] G. Fuchsbauer, J. Katz, and D. Naccache. Efficient rational secret sharing in standard communication networks. *Theory of Cryptography Conference – TCC 2010*, Springer LNCS 5978, 419–436, 2010.

[112] G. Fuchsbauer and D. Pointcheval. Anonymous Proxy Signatures. *Security and Cryptography for Networks – SCN 2008*, Spinger-Verlag LNCS 5229, 201–217, 2008.

[113] G. Fuchsbauer and D. Pointcheval. Proofs on Encrypted Values in Bilinear Groups and an Application to Anonymity of Signatures. *Pairing-Based Cryptography – PAIRING 2009*, Springer LNCS 5671, 132–149, 2009.

[114] G. Fuchsbauer, D. Pointcheval, and D. Vergnaud. Transferable constant-size fair e-cash. *Cryptology and Network Security – CANS 2009*, Springer LNCS 5888, 226–247, 2009.

[115] G. Fuchsbauer and D. Vergnaud. Fair blind signatures without random oracles. *Progress in Cryptology – AFRICACRYPT 2010*, Springer LNCS 6055, 16–33, 2010.

[116] S. D. Galbraith, X. Lin, and M. Scott. Endomorphisms for faster elliptic curve cryptography on a large class of curves. *Advances in Cryptology – EUROCRYPT 2009*, Springer LNCS 5479, 518–535, 2009.

[117] S.D. Galbraith, K.G. Paterson and N.P. Smart. Pairings for Cryptographers *Discrete Applied Mathematics*, **156**, 3113–3121, 2008.

[118] S.D. Galbraith and R.S. Ruprai. An improvement to the Gaudry-Schost algorithm for multidimensional discrete logarithm problems. *Coding and Cryptography 2009.* Springer LNCS 5921, 368–382, 2009.

[119] S.D. Galbraith and R.S. Ruprai. Using Equivalence Classes to Accelerate Solving the Discrete Logarithm Problem in a Short Interval. *Public Key Cryptography – PKC 2010*, Springer LNCS 6056, 368–383, 2010.

[120] S.D. Galbraith, J.M. Pollard, and R.S. Ruprai. Computing discrete logarithms in an interval. *Cryptology ePrint Archive*, Report 2010/617.

[121] S. Garg, R. Ostrovsky, I. Visconti and A. Wadia. Resettable statistical zero knowledge. *Theory of Cryptography Conference – TCC 2012*, Springer LNCS 7194, 494–511, 2012.

[122] M. Geisler and N.P. Smart. Distributing the key distribution centre in Sakai–Kasahara based systems. *Coding and Cryptography 2009*. Springer LNCS 5921, 252–262, 2009.

[123] C. Gentry, S. Halevi, C. Peikert and N.P. Smart. Ring switching in BGV-syle homomorphic encryption. *Security and Cryptography for Networks – SCN 2012*, Springer LNCS 7485, 19–37, 2012.

[124] C. Gentry, S. Havlevi and N.P. Smart Fully homomorphic encryption with polylog overhead. To appear *Advances in Cryptology – EUROCRYPT 2012*, Springer LNCS 7237, 465–482, 2012.

[125] C. Gentry, S. Havlevi and N.P. Smart Better bootstrapping in fully homomorphic encryption. To appear *Public Key Cryptography – PKC 2012*, Springer LNCS 7293, 1–16, 2012.

[126] C. Gentry, S. Havlevi and N.P. Smart Homomorphic evaluation of the AES circuit. *Advances in Cryptology – CRYPTO 2012*, Springer LNCS 7417, 850–867, 2012.

[127] E. Ghadafi, N.P. Smart and B. Warinschi. Practical zero-knowledge proofs for circuit evaluation. *Coding and Cryptography 2009*, Springer LNCS 5921, 469–494, 2009.

[128] E. Ghadafi, N.P. Smart and B. Warinschi. Groth–Sahai proofs revisited. *Public Key Cryptography – PKC 2010*, Springer LNCS 6056, 177–192, 2010.

[129] E. Ghadafi and N.P. Smart. Efficient Two-Move Blind Signatures in the Common Reference String Model. *Information Security – ISC 2012*, Springer LNCS 7483, 274–289, 2012.

[130] M.I. Gonzalez Vasco, F. Hess, R. Steinwandt. Combined (identity-based) public key schemes. In submission.

[131] B. Hemenway, B. Libert, R. Ostrovsky, and D. Vergnaud. Lossy Encryption: Constructions from General Assumptions and Efficient Selective Opening Chosen Ciphertext Security. *Advances in Cryptology – ASIACRYPT 2011*, Springer LNCS 7073, 70–88, 2011.

[132] W. Henecka, S. Kögl, A.-R. Sadeghi, T. Schneider and I. Wehrenberg. TASTY: Tool for Automating Secure Two-partY Computations. *Computer and Communications Security – ACM CCS 2010*, 451–462, 2010.

[133] W. Henecka, A. May and A. Meurer Correcting Errors in RSA Private Keys. *Advances in Cryptology - CRYPTO 2010*, Springer LNCS 6223, 351–369, 2010.

[134] J. Hermans, A. Pashalidis, F. Vercauteren, and B. Preneel. A New RFID Privacy Model. *European Symposium on Research in Computer Security – ESORICS 2011*, Springer LNCS 6879, 568–587, 2011.

[135] J. Herranz, F. Laguillaumie, B. Libert and C. Ràfols. Short Attribute-Based Signatures for Threshold Predicates. *Topics in Cryptology – CT-RSA 2012*, Springer LNCS 7178, 51–67, 2012.

[136] M. Herrmann and A. May Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA. *Public Key Cryptography - PKC 2010*, Springer LNCS 6056, 53–69, 2010.

[137] M. Herrmann and A. May Attacking Power Generators Using Unravelled Linearization: When Do We Output Too Much?. *Advances in Cryptology - ASIACRYPT 2009*, Springer LNCS 5912, 487–504, 2010.

[138] D. Hofheinz, J. Malone-Lee and M. Stam. Obfuscation for Cryptographic Purposes *Journal of Cryptology*, **23**, 121–168, 2010.

[139] L. Ibraimi and S. I. Nikova and P. H. Hartel and W. Jonker. Public-Key Encryption with Delegated Search. *Applied Cryptography and Network Security – ACNS 2011*, Springer LNCS 6715, 532–549, 2011.

[140] V. Iovino and G. Persiano. Hidden Vector Encryption with prime order groups *Pairing-Based Cryptography – PAIRING 2008*, Springer LNCS 5209, 75–88, 2008.

[141] M. Izabachène, B. Libert, and D. Vergnaud. Block-Wise P-Signatures and Non-interactive Anonymous Credentials with Efficient Attributes. *Cryptography and Coding 2011*, Springer LNCS 7089, 431–450, 2011.

[142] M. Izabachène and D. Pointcheval. New Anonymity Notions for Identity-Based Encryption. *Security and Cryptography for Networks – SCN 2008*, Springer LNCS 5229, 375-391, 2008.

[143] M. Izabachène, D. Pointcheval, and D. Vergnaud. Mediated Traceable Anonymous Encryption *Progress in Cryptology - LATINCRYPT 2010*, Springer LNCS 6212, 40-60, 2010.

[144] T. Jager, F. Kohlar, S. Schäge and J. Schwenk. Generic Compilers for Authenticated Key Exchange. *Advances in Cryptology - ASIACRYPT 2010*, Springer LNCS 6477, 232–249, 2010.

[145] T. Jager and J. Schwenk. On the Analysis of Cryptographic Assumptions in the Generic Ring Model. *Advances in Cryptology – ASIACRYPT 2009*, Springer LNCS 5912, 399–416, 2009.

[146] T. Jager and A. Rupp. The Semi-Generic Group Model and Applications to Pairing-based Cryptography. *Advances in Cryptology - ASIACRYPT 2010*, Springer LNCS 6477, 539–556 2010.

[147] K. Järvinen, V. Kolesnikov, A.-R. Sadeghi and T. Schneider. Embedded SFE: Offloading Server and Network using Hardware Tokens. *Financial Cryptography – FC 2010*, Springer LNCS 6052, 207–221, 2010.

[148] K. Järvinen, V. Kolesnikov, A.-R. Sadeghi and T. Schneider. Garbled Circuits for Leakage-Resilience: Hardware Implementation and Evaluation of One-Time Programs. *Cryptographic Hardware and Embedded Systems – CHES 2010*, Springer LNCS 6225, 383–397, 2010.

[149] D. Jetchev, O. Ozen and M. Stam. Understanding Adaptivity: Random Systems Revisited. *Advances in Cryptology – ASIACRYPT 2012*, Springer LNCS 7658, 313–330, 2012.

[150] M. Joye, M. Tibouchi and D. Vergnaud. Huff's Model for Elliptic Curves. *Algorithmic Number Theory - ANTS-IX*, Springer LNCS 6197, 234–250, 2010.

[151] E. Kiltz, K. Pietrzak, M. Stam and M. Yung. A new randomness extraction paradigm for hybrid encryption. *Advances in Cryptology – EUROCRYPT 2009*, Springer LNCS 5479, 590–609, 2009.

[152] T. Kleinjung, A.K. Lenstra, D. Page and N.P. Smart Using the Cloud to Determine Key Strengths. *Progress in Cryptology – INDOCRYPT 2012*, Springer LNCS 7669, 17–39, 2012.

[153] V. Kolesnikov, A.-R. Sadeghi and T. Schneider. Improved Garbled Circuit Building Blocks and Applications to Auctions and Computing Minima. *Cryptology And Network Security – CANS 2009*, Springer LNCS 5888, 1–20, 2009.

[154] S. Kremer, G. Steel, and B. Warinschi. Security for Key Management Interfaces. IEEE Computer Security Foundations Symposium – CSF 2011, IEEE Computer Society, 266-280, 2011.

[155] M.-F. Lee, N.P. Smart and B. Warinschi. The Fiat–Shamir transform for group and ring signatures. *Security and Cryptography for Networks – SCN 2010*, Springer LNCS 6280, 363–380, 2010.

[156] G. Leurent and P.Q. Nguyen. How risky in the random oracle model?. *Advances in Cryptology – CRYPTO 2009*, Springer LNCS 5677, 445–464, 2009.

[157] B. Libert, K.G. Paterson and E.A. Quaglia Anonymous broadcast encryption: adaptive security and efficient constructions in the standard model *Public Key Cryptography–PKC 2012*, Springer LNCS 7293, 206–224, 2012.

[158] B. Libert, T. Peters, and M. Yung. Scalable Group Signatures with Revocation. *Advances in Cryptology – EUROCRYPT 2012*, Sringer LNCS 7237, 609-627, 2012.

[159] B. Libert, T. Peters, and M. Yung. Group Signatures with Almost-for-free Revocation. *Advances in Cryptology – CRYPTO 2012*, Springer, LNCS 7417, 571-589, 2012.

[160] B. Libert and D. Vergnaud. Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys. *Public Key Cryptography 2009*, Springer LNCS 5443, 235–255, 2009.

[161] B. Libert and D. Vergnaud. Adaptive-ID Secure Revocable Identity-Based Encryption. *Topics in Cryptology - CT-RSA 2009*, Springer LNCS 5473, 1–15, 2009.

[162] B. Libert and D. Vergnaud. Group Signatures with Verifier-Local Revocation and Backward Unlinkability in the Standard Model. *Cryptology and Network Security 2009 (CANS'09)*, Springer LNCS 5888, 498–517, 2009.

[163] B. Libert and M. Yung. Adaptively Secure Non-Interactive Threshold Cryptosystems. *International Colloquium on Automata, Languages and Programming – ICALP 2011*, Springer LNCS 6756, 588–600, 2011.

[164] J. Loftus, A. May, N.P. Smart and F. Vercauteren. On CCA-Secure Fully Homomorphic Encryption. *Selected Areas in Cryptology – SAC 2011*, Springer LNCS 7118, 55–72, 2012.

[165] J. Loftus and N.P. Smart Secure Outsourced Computation. *Progress in Cryptology – AFRICACRYPT 2011*, Springer LNCS 6737, 1–20, 2011.

[166] M. Manulis. Group Key Exchange Enabling On-Demand Derivation of Peer-to-Peer Keys. *Applied Cryptography and Network Security – ACNS 2009*, Springer LNCS 5536, 1–19, 2009.

[167] A. May, A. Meurer and E.Thomae. Decoding Random Linear Codes in $2^{0.054n}$. *Advances in Cryptology – ASIACRYPT 2011*, Springer LNCS 7073, 107–124, 2011.

[168] A. May and M. Ritzenhofen Implicit Factoring: On Polynomial Time Factoring Given Only an Implicit Hint. *Public Key Cryptography - PKC 2009*, Springer LNCS 5443, 1–14, 2009.

[169] L. Mazare and B. Warinschi. Separating Trace Mapping and Reactive Simulatability Soundness: The Case of Adaptive Corruption. To appear *Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security – WITS-ARSPA 2009.*

[170] P. Morrissey, N.P. Smart and B. Warinschi. A modular security analysis of the TLS handshake protocol. *Advances in Cryptology – ASIACRYPT 2008*, Springer LNCS 5350, 55–73, 2008.

[171] G. Neven, N.P. Smart and B. Warinschi. Hash function requirements for Schnorr signatures. *J. Mathematical Cryptology*, **3**, 69–87, 2009.

[172] K. Ouafi and S. Vaudenay. Smashing SQUASH-0. *Advances in Cryptology – EUROCRYPT 2009*, Springer LNCS 5479, 300–312, 2009.

[173] K. Ouafi and S. Vaudenay. Pathchecker: An RFID application for tracing products in supply-chains. *Workshop on RFID Security – RFIDSec 2009.*

[174] R. Ostrovsky, G. Persiano and I. Visconti. Simulation-Based Concurrent Non-Malleable Commitments and Decommitments. *Theory of Cryptography Conference – TCC 2009*, Springer LNCS 5444, 91–108, 2009.

[175] R. Ostrovsky, O. Pandey, A. Sahai and I. Visconti. Non-malleability under reset attacks. Technical Report, 2011.

[176] R. Ostrovsky, O. Pandey and I. Visconti. Efficiency Preserving Transformation for Concurrent Non-Malleable Zero Knowledge. *Theory of Cryptography Conference – TCC 2010*, Springer LNCS 5978, 535–552, 2010.

[177] R. Ostrovsky, V. Rao, A. Scafuro and I. Visconti. Revisiting lower and upper bounds for selective decommitments. Technical Report, 2012.

[178] K.G. Paterson and E.A. Quaglia. Time Specific Encryption. *Security and Cryptography for Networks – SCN 2010*, Springer LNCS 6280, 1–16, 2010.

[179] K.G. Paterson, J.C.N. Schuldt, M. Stam and S. Thomson. On the Joint Security of Encryption and Signature, Revisited. *Advances in Cryptology – ASIACRYPT 2011*, Springer LNCS 7073, 161–178, 2011.

[180] K.G. Paterson and S. Srinivasan. Security and Anonymity of Identity-Based Encryption with Multiple Trusted Authorities. *Pairing-Based Cryptography – PAIRING 2008*, Springer LNCS 5209, 354-375-, 2008.

[181] K.G. Paterson and S. Srinivasan. Building Key-Private Public-Key Encryption Schemes. *Information Security and Privacy – ACISP 2009*, Springer LNCS 5594, 276–292, 2009.

[182] K.G. Paterson and S. Srinivasan. On the relations between non-interactive key distribution, identity-based encryption and trapdoor discrete log groups. *Des. Codes Cryptography*, **52**, 219–241, 2009.

[183] K.G. Paterson and G.J. Watson. Plaintext-Dependent Decryption: A Formal Security Treatment of SSH-CTR. *Advances in Cryptology– EUROCRYPT 2010*, Springer LNCS 6110, 345–361, 2010.

[184] A.Patra, A. Choudhury and C. Pandu Rangan. Efficient Asynchronous Verifiable Secret Sharing and Multiparty Computation. *Cryptology ePrint Archive*, Report 2010/007.

[185] A. Paus, A.-R. Sadeghi and T. Schneider. Practical Secure Evaluation of Semi-Private Functions. *Applied Cryptography and Network Security – ACNS 09*, Springer LNCS 5536, 89–106, 2009.

[PV11] G. Persiano and I. Visconti. Two-message non-interactive zero knowledge. Technical Report, 2011.

[186] C. Peters. Information-set decoding for linear codes over $\mathbf{F}_q$. *Post-Quantum Cryptography – PQCrypto 2010*, Springer LNCS 6061, 81–94, 2010.

[187] A. Petzoldt, E. Thomae, S. Bulygin and C. Wolf. Small Public Keys and Fast Verification for Multivariate Quadratic Public Key Systems. *Cryptographic Hardware and Embedded Systems – CHES 2011*, Springer LNCS 6917, 475–490, 2011.

[188] D. H. Phan, D. Pointcheval, S. F. Shahandashti, and M. Strefler. Adaptive CCA Broadcast Encryption with Constant-Size Secret Keys and Ciphertexts. *Information Security and Privacy – ACISP 2012*, Springer LNCS 7372, 308–321, 2012.

[189] D.H. Phan, D. Pointcheval, and M. Strefler. Security notions for broadcast encryption. *Applied Cryptography and Network Security – ACNS 2011*, Springer LNCS 6715, 377–394, 2011.

[190] D. H. Phan, D. Pointcheval, and M. Strefler. Decentralized Dynamic Broadcast Encryption. *Security and Cryptography for Networks – SCN 2012*, Springer LNCS 7485, 166–183, 2012.

[191] D. H. Phan, D. Pointcheval, and M. Strefler. Message Tracing with Optimal Ciphertext Rate. *Progress in Cryptology - LATINCRYPT 2010*, Springer LNCS 6212, 241–254, 2010.

[192] B. Pinkas, T. Schneider, N.P. Smart and S. Williams. Secure Two-Party Computation is Practical *Advances in Cryptology – ASIACRYPT 2009*, Springer LNCS 5912, 250–267, 2009.

[193] M. Rückert and D. Schröder. Security of Verifiably Encrypted Signatures and a Construction Without Random Oracles. *Pairing-based Cryptography – PAIRING 2009*, Springer LNCS 5671, 17–34, 2009.

[194] A.-R. Sadeghi and T. Schneider. Generalized Universal Circuits for Secure Evaluation of Private Functions with Application to Data Classification. *International Conference on Information Security and Cryptology – ICISC 08*, Springer LNCS 5350, 336–353, 2008.

[195] A.-R. Sadeghi, T. Schneider and I. Wehrenberg. Efficient Privacy-Preserving Face Recognition. *International Conference on Information Security and Cryptology – ICISC 2009*, Springer LNCS 5984, 229–224, 2010.

[196] A.-R. Sadeghi, T. Schneider and M. Winandy. Token-Based Cloud Computing – Secure Outsourcing of Data and Arbitrary Computations with Lower Latency. *Trust and Trustworthy Computing – TRUST 2010*, Springer LNCS 6101, 417–429, 2010.

[197] A.-R. Sadeghi, I. Visconti and C. Wachsmann. User Privacy in Transport Systems Based on RFID E-Tickets *Workshop on Privacy in Location-Based Applications – PiLBA 2008*, CEUR Workshop Proceedings 397, 2008.

[198] A.-R. Sadeghi and I. Visconti and C. Wachsmann. Efficient RFID Security and Privacy with Anonymizers *Workshop on RFID Security – RFIDSec 09*, 2009.

[199] A.-R. Sadeghi and I. Visconti and C. Wachsmann. Anonymizer-Enabled Security and Privacy for RFID. *Cryptology and Network Security – CANS 2009*, Springer LNCS 5888, 134–153, 2009.

[200] A.-R. Sadeghi and I. Visconti and C. Wachsmann. Location Privacy in RFID Applications. *Privacy in Location-Based Applications*, Springer LNCS 5599, 127–150, 2009.

[201] A.-R. Sadeghi and I. Visconti and C. Wachsmann. PUF-Enhanced RFID Security and Privacy. *Secure Component and System Identification – SECSI 2010*, 2010.

[202] P. Scholl and N.P. Smart. Improved key generation for Gentry's fully homomorphic encryption scheme. *Coding and Cryptography 2011*, Springer LNCS 7089, 10–22, 2011.

[203] S. Sedghi and P. van Liesdonk and S. I. Nikova and P. H. Hartel and W. Jonker. Searching Keywords with Wildcards on Encrypted Data. *Security and Cryptography for Networks – SCN 2010*, Springer LNCS 6280, 138–153, 2010.

[204] A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y. Michalevsky, and D. Shaket. Venus: Verification for untrusted cloud storage. *Workshop on Cloud Computing Security – CCSW 2010*, ACM, 2010.

[205] N.P. Smart. Errors Matter: Breaking RSA-based PIN Encryption with thirty ciphertext validity queries. *Topics in Cryptology - CT-RSA 2010*, Springer LNCS 5985, 15–25, 2010.

[206] N.P. Smart and F. Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes. *Public Key Cryptography – PKC 2010*, Springer LNCS 6056, 420–443, 2010.

[207] N.P. Smart and F. Vercauteren. Fully homomorphic SIMD operations. To appear *Designs, Codes and Cryptography.*

[208] N.P. Smart and B. Warinschi. Identity Based Group Signatures from Heiarchical Identity-Based Encryption. *Pairing-Based Cryptography – PAIRING 2009*, Springer LNCS 5671, 150–170, 2009.

[209] E. Thomae, Quo Vadis Quaternion? Cryptanalysis of Rainbow over Non-Commutative Rings. *Security and Cryptography for Networks – SCN 2012*, Springer LNCS, 2012.

[210] E. Thomae and C. Wolf. Theoretical Analysis and Run Time Complexity of MutantXL. *International Conference Computational and Mathematical Methods in Science and Engineering – CMMSE 2011*, 2011.

[211] E. Thomae and C. Wolf. Solving Systems of Multivariate Quadratic Equations over Finite Fields or: From Relinearization to MutantXL. *Cryptology ePrint Archive*, Report 2010/596.

[212] E. Thomae and C. Wolf, Roots of Square: Cryptanalysis of Double-Layer Square and Square+. *Post-Quantum Cryptography – PQCrypto 2011*, Springer LNCS 7071, 83–97, 2011.

[213] E. Thomae and C. Wolf, Solving Underdetermined Systems of Multivariate Quadratic Equations revisited. *Practice and Theory in Public Key Cryptography – PKC 2012*, Springer LNCS 7293, 156–171, 2012.

[214] E. Thomae and C. Wolf, Cryptanalysis of Enhanced TTS, STS and all its Variants, or: Why Cross-Terms are Important. *International Conference on Cryptology in Africa – AfricaCrypt 2012*, Springer LNCS, 2012.

[215] C. Ventre and I. Visconti. Co-Sound Zero-Knowledge with Public Keys *Progress in Cryptology – AFRICACRYPT 2009*, Springer LNCS 5580, 287–304, 2009.

[216] D. Vergnaud. Efficient and Secure Generalized Pattern Matching via Fast Fourier Transform. *Progress in Cryptology – AFRICACRYPT 2011*, Springer LNCS 6737, 41-58, 2011.

[217] C.D. Walter Fast Scalar Multiplication for ECC over GF(p) using Division Chains. *Information Security Applications – WISA 2010*, Springer LNCS 6513, 61–75, 2010.

Referenced Papers Which Are Not ECRYPT-2 Outputs

[218] M. Abdalla, O. Chevassut, P.-A. Fouque, and D. Pointcheval. A Simple Threshold Authenticated Key Exchange from Short Secrets. *Advances in Cryptology – ASIACRYPT 2005*, Springer LNCS 3788, 566–584, 2005.

[219] M. Abe. Universally verifiable mix-net with verification work indendent of the number of mix-servers. *Advances in Cryptology – EUROCRYPT 1998*, Springer LNCS 1403, 437–447, 1998.

[220] K. Akiyama, Y. Goto, and H. Miyake. An Algebraic Surface Cryptosystem. *Public Key Cryptography – PKC 2009*, Springer LNCS 5443, 425–442, 2009

[221] G. Ateniese, D.H. Chou, B. de Medeiros and G. Tsudik. Sanitizable Signatures. *ESORICS 2005*, Springer LNCS 3679, 159–177, 2005.

[222] BSI. Technical Guidelines TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents. Extended Access Control (EAC), Version 2.01. Federal Ministry of the Interior, Bundesamt für Sicherheit in der Informationstechnik, 2009.

[223] M. Bellare, M. Fischlin, S. Goldwasser and S. Micali: Identification protocols secure against reset attacks. *Advances in Cryptology – EUROCRYPT 2001.* Springer LNCS 2045, 495–511, 2001.

[224] M. Bellare, D. Hofheinz and S. Yilek. Possibility and impossibility results for encryption and commitment secure under selective opening. *Advances in Cryptology – EUROCRYPT 2009*, Springer LNCS 5479, 1–35, 2009.

[225] M. Bellare and T. Kohno. A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. *Advances in Cryptology – EUROCRYPT 2003*, Springer LNCS 2656, 491–506, 2003.

[226] M. Bellare, D. Pointcheval and P. Rogaway. Authenticated key exchange secure against dictionary attacks. *Advances in Cryptology – EUROCRYPT 2000*, Springer LNCS 1807, 139–155, 2000.

[227] M. Bellare and P. Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. *ACM Conference on Computer and Communications Security – CCS 1993*, ACM, 62–73, 1993.

[228] M. Bellare and P. Rogaway. Entity Authentication and Key Distribution. *Advances in Cryptology – CRYPTO '93*, Springer LNCS 773, 232–249, 1994.

[229] K. Bentahar, P. Farshim, J. Malone-Lee, and N.P. Smart. Generic Constructions of Identity-based and Certificateless KEMs. *Journal of Cryptology*, **21**, 178–199, 2008.

[230] T. P. Berger, P.L. Cayrel, P. Gaborit, and A. Otmani. Reducing key length of the McEliece cryptosystem. *Progress in Cryptology – AFRICACRYPT 2009*, Springer LNCS 5580, 77–97, 2009.

[231] D. J. Bernstein, T. Lange, and C. Peters. Attacking and defending the McEliece cryptosystem. *Post-Quantum Cryptography – PQCrypto 2008*, Springer LNCS 5299, 31–46, 2008.

[232] D. Bleichenbacher. Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1. *Advances in Cryptology - CRYPTO '98*, Springer LNCS 1462, 1–12, 1998.

[233] A. Boldyreva, V. Goyal, and V. Kumar. Identity-based encryption with efficient revocation *Computer and Communications Security – ACM CCS 2008*, 417–426, 2008.

[234] D. Boneh, R.A. DeMillo and R.J. Lipton. On the Importance of Eliminating Errors in Cryptographic Computations. *J. Cryptology*, **14**, 101–119, 2001.

[235] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal on Computing*, **32**, 586–615, 2003.

[236] D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. *Advances in Cryptology – EUROCRYPT 2003*, Springer LNCS 2656, 416–432, 2003.

[237] D. Boneh and H. Shacham. Group Signatures with Verifier-local Revocation. *Computer and Communications Security – ACM CCS 2004*, 168–177, 2004.

[238] D. Boneh and B. Waters. Conjunctive, Subset, and Range Queries on Encrypted Data. *Theory of Cryptography Conference – TCC 2007*, Springer LNCS 4392, 535–554, 2007.

[239] Z. Brakerski, C. Gentry and V. Vaikuntanathan. Fully homomorphic encryption without bootstrapping. *Cryptology ePrint Archive*, Report 2011/277.

[240] C. Cachin and N. Chandran. A Secure Cryptographic Token Interface. *Computer Security Foundations Symposium (CSF-22)*, IEEE, 141–153, 2009.

[241] J. Camenisch, R. Chaabouni, and a. shelat. Efficient Protocols for Set Membership and Range Proofs. *Advances in Cryptology – ASIACRYPT 2008*, Springer LNCS 5350, 234–252, 2008.

[242] J. Camenisch, G. Neven and a. shelat. Simulatable Adaptive Oblivious Transfer. *Advances in Cryptology – EUROCRYPT 2007*, Springer LNCS 4515, 573–590, 2007.

[243] R. Canetti. Universally Composable Security: A New Paradigm for Cryptographic Protocols. *Annual Symposium on Foundations of Computer Science – FOCS 2001*, IEEE Computer Society Press, 136–145, 2001.

[244] R. Canetti, J. Friedlander, S. Konyagin, M. Larsen, D. Lieman, and I. Shparlinski. On the Statistical Properties of Diffie-Hellman Distributions. *Israel Journal of Mathematics*, **120**, 23–46, 2000.

[245] R. Canetti, O. Goldreich, S. Goldwasser, and S. Micali. Resettable Zero-Knowledge. *Symposium on Theory of Computing – STOC 2008*, ACM Press, 235–244, 2000.

[246] R. Canetti and H. Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. *Advances in Cryptology – EUROCRYPT 2001*, Springer LNCS 2045, 453–474, 2001.

[247] R. Canetti, R.L. Rivest, M. Sudan, L. Trevisan, S.P. Vadhan, and H. Wee. Amplifying Collision Resistance: A Complexity-Theoretic Treatment. *Advances in Cryptology – CRYPTO 2007*, Springer LNCS 4622, 264–283, 2007.

[248] D. Chaum and E. van Heyst. Group Signatures. *Advances in Cryptology – EUROCRYPT'91*, Springer LNCS 547, 257–265, 1991.

[249] J.-S. Coron, A. Joux, D. Naccache, I. Kizhvatov and P. Paillier. Fault Attacks on RSA Signatures with Partially Unknown Messages. *Cryptographic Hardware and Embedded Systems - CHES 2009*, Springer LNCS 5747, 444–456, 2009.

[250] J.-S. Coron, D. Naccache and J.P. Stern. On the Security of RSA Padding. *Advances in Cryptology - CRYPTO '99*, Springer LNCS 1666, 1–18, 1999.

[251] N. T. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. *Advances in Cryptology – ASIACRYPT 2001*, Springer LNCS 2248, 157–174, 2001.

[252] N.T. Courtois. Efficient zero-knowledge authentication based on a linear algebra problem MinRank. *Advances in Cryptology - ASIACRYPT 2001*, Springer LNCS 2248, 402–421, 2001.

[253] R. Cramer and V. Shoup. Universal Hash Proofs and A Paradigm for Adaptive Chosen Ciphertext Secure Public-key Encryption. *Advances in Cryptology – EUROCRYPT 2002*, Springer LNCS 2332, 45–64, 2002.

[254] I. Damgård, N. Fazio, and A. Nicolosi. Non-interactive zero-knowledge from homomorphic encryption. *Theory of Cryptography Conference – TCC 2006*, Springer LNCS 3876, 41–59, 2006.

[255] A.W. Dent. A survey of certificateless encryption schemes and security models. *International Journal of Information Security*, **7(5)**, 349–377, 2008.

[256] G. Di Crescenzo, G. Persiano, and I. Visconti. Constant-Round Resettable Zero Knowledge with Concurrent Soundness in the Bare Public-Key Model. *Advances in Cryptology – CRYPTO 2004*, Springer LNCS 3152, 237–253, 2004.

[257] M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan. Fully Homomorphic Encryption over the Integers. *Advances in Cryptology - EUROCRYPT 2010*, Springer LNCS 6110, 24–43, 2010.

[258] R. Dingledine, N. Mathewson and P.F. Syverson. Tor: The second-generation onion router. *USENIX Security Symposium – 2004*, 303–320. USENIX, 2004.

[259] C. Dwork, M. Naor, O. Reingold and L. Stockmeyer. Magic functions. *Symposium on Foundations of Computer Science – FOCS 1999*, IEEE Computer Society Press, 523–534, 1999.

[260] C. Dwork, M. Naor, O. Reingold and L. Stockmeyer. Magic functions. *J. ACM*, **50**, 852–921, 2003.

[261] R.R. Farashahi, I.E. Shparlinski and J.F. Voloch. On Hashing into Elliptic Curves. *J. Mathematical Cryptology*, **3**, 353–360, 2009.

[262] J.-C. Faugère, F. Levy-dit Vehel, and L. Perret. Cryptanalysis of minrank. *Advances in Cryptology – CRYPTO 2008*, Springer LNCS 5157, 280–296, 2008.

[263] M. Finiasz and N. Sendrier. Security bounds for the design of code-based cryptosystems. *Advances in Cryptology – ASIACRYPT 2009*, Springer LNCS 5912, 88–105, 2009.

[264] P.-A. Fouque, D. Pointcheval, J. Stern, and S. Zimmer. Hardness of Distinguishing the MSB or LSB of Secret Keys in Diffie-Hellman Schemes. *International Colloquium on Automata, Languages and Programming – ICALP 2006*, Springer LNCS 4052, 240–251, 2006.

[265] R.P. Gallant, R.J. Lambert and S.A. Vanstone. Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms. *Advances in Cryptology – CRYPTO 2001*, Springer LNCS 2139, 190–200, 2001.

[266] P. Gaudry and E. Schost, A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm. *Algorithm Number Theory Symposium – ANTS VI*, Springer LNCS 3076, 208–222, 2004.

[267] R. Gennaro and Y. Lindell. A Framework for Password-based Authenticated Key Exchange. *Advances in Cryptology – EUROCRYPT 2003*, Springer LNCS 2656, 524–543, 2003.

[268] C. Gentry. Fully homomorphic encryption using ideal lattices. *Symposium on Theory of Computing – STOC 2009*, ACM, 169–178, 2009.

[269] C. Gentry and S. Halevi. Implementing Gentry's fully-homomorphic encryption scheme. *Advances in Cryptology – EUROCRYPT 2011*, Springer LNCS 6632, 129–148, 2011.

[270] J. Groth. Cryptography in Subgroups of $\mathbb{Z}_n$. *Theory of Cryptography - TCC 2005*, Springer , LNCS 3378, 50–65, 2005.

[271] O. Goldreich and L.A. Levin. A hard-core predicate for all one-way functions. *Symposium on Theory of Computing – STOC 1989*, ACM Press, 25–32, 1989.

[272] P. Golle and A. Juels. Dining cryptographers revisited. *Advances in Cryptology – EUROCRYPT 2004*, Springer LNCS 3027, 46–473, 2004.

[273] V. Goyal. Reducing Trust in the PKG in Identity Based Cryptosystems. *Advances in Cryptology – CRYPTO 2007*, Springer LNCS 4622, 430–447, 2007.

[274] J. Groth, R. Ostrovsky, and A. Sahai. Perfect non-interactive zero knowledge for np. *Advances in Cryptology – EUROCRYPT 2006*, Springer LNCS 4004, 339–358, 2006.

[275] J. Groth, and A. Sahai. Efficient Non-interactive Proof Systems for Bilinear Groups. *Advances in Cryptology – EUROCRYPT 2008*, Springer LNCS 4965, 415–432, 2008.

[276] D. Hankerson, K. Karabina and A. J. Menezes. Analyzing the Galbraith-Lin-Scott point multiplication method for elliptic curves over binary fields. *IEEE Trans. Comput.*, **58**, 1411–1420, 2009.

[277] C. Hazay and Y. Lindell. Constructions of truly practical secure protocols using standard smartcards. *ACM Conference on Computer and Communications Security – CCS 2008*, ACM, 491–500, 2008.

[278] D. Hofheinz. Possibility and impossibility results for selective decommitments. *J. Cryptology*, **24**, 470–516, 2011.

[279] E. Hufschmitt and J. Traoré. Fair blind signatures revisited. *Pairing-based Cryptography – PAIRING 2007*, Springer LNCS 4575, 268–292, 2007.

[280] ICAO. Machine Readable Travel Documents. Part 1: Machine Readable Passport, Specifications for Electronically enabled Passports with Biometric Identification Capabilities. International Civil Aviation Organization – ICAO Doc 9303, 2006.

[281] ICAO. Machine Readable Travel Documents. Part 3: Machine Readable Official Travel Documents, Specifications for Electronically enabled Official Travel Documents with Biometric Identification Capabilities. International Civil Aviation Organization – ICAO Doc 9303, 2008.

[282] ISO/IEC. 9798-2: 1999, Information Technology – Security Techniques – Entity Authentication – Part 2: Mechanisms Using Symmetric Encipherment Algorithms.

[283] ISO/IEC. 9798-3: 1998, Information Technology – Security Techniques – Entity Authentication – Part 3: Mechanisms Using Digital Signature Techniques.

[284] T. Icart. How to Hash into Elliptic Curves. *Advances in Cryptology - CRYPTO 2009*, Springer LNCS 5677, 303–316, 2009.

[285] T. Iijima, K. Matsuo, J. Chao and S. Tsujii. Construction of Frobenius Maps of Twist Elliptic Curves and its Application to Elliptic Scalar Multiplication. *SCIS 2002*, IEICE Japan, 699–702, 2002.

[286] Y. T. Kalai. Smooth Projective Hashing and Two-message Oblivious Transfer. *Advances in Cryptology – EUROCRYPT 2005*, Springer LNCS 3494, 78–95, 2005.

[287] J. Katz, A. Sahai and B. Waters. Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products. *Advances in Cryptology – EUROCRYPT 2008*, Springer LNCS 4965, 146–162, 2008.

[288] A. Kipnis and A. Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. *Advances in Cryptology - CRYPTO 99*, Springer LNCS 1666, 19–30, 1999.

[289] V. Kolesnikov. Truly efficient string oblivious transfer using resettable tamper-proof tokens. *Theory of Cryptography Conference – TCC 2010*, Springer LNCS 5978, 327–342, 2010.

[290] Y.K. Lee, L. Batina, D. Singelée, and I. Verbauwhede Low-Cost Untraceable Authentication Protocols for RFID. *Wireless Network Security – WiSec 2010*, ACM, 55–64, 2010.

[291] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Mathematics*, **126**, 649–673, 1987.

[292] A. B. Lewko and B. Waters. Predicate Privacy in Encryption Systems. *Theory of Cryptography Conference – TCC 2010*, Springer LNCS 5978, 455–479, 2010.

[293] P. Longa and C. Gebotys Fast Multibase Methods and Other Several Optimizations for Elliptic Curve Scalar Multiplication. *Public Key Cryptography – PKC 2009*, Springer LNCS 5443, 443–462, 2009.

[294] S. Lu, R. Ostrovsky, A. Sahai, H. Shacham, and B. Waters. Sequential Aggregate Signatures and Multisignatures Without Random Oracles. *Advances in Cryptology – EUROCRYPT 2006*, Springer LNCS 4004, 465–485, 2006.

[295] M. Mambo, K. Usuda, E. Okamoto. Proxy Signatures for Delegating Signing Operation. *Computer and Communications Security – ACM CCS 1996*, 48–57, 1996.

[296] R. J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, pages 114–116. Jet Propulsion Lab, 1978. DSN Progress Report 44.

[297] S. Micali, M.O. Rabin, and S.P. Vadhan. Verifiable Random Functions. *Symposium on Foundations of Computer Science – FOCS 1999*, IEEE Computer Society Press, 120–130, 1999.

[298] R. Misoczki and P.S.L.M. Barreto. Compact McEliece keys from Goppa codes. *Selected Areas in Cryptography – SAC 2009*, Springer LNCS 5867, 376–392, 2009.

[299] P. Q. Nguyen and J. Stern. Merkle-Hellman Revisited: A Cryptoanalysis of the Qu-Vanstone Cryptosystem Based on Group Factorization. *Advances in Cryptology - CRYPTO '97*, Springer LNCS 1294, 198–212, 1997.

[300] R. Nithyanand. The Evolution of Cryptographic Protocols in Electronic Passports. *Cryptology ePrint Archive*, Report 2009/200.

[301] OASIS Key Management Interoperability Protocol Technical Committee. Key Management Interoperability Protocol, Version 1.0. *OASIS Standard*, available from `http://www.oasis-open.org/committees/documents.php?wg_abbrev=kmip`, 2010.

[302] T. Okamoto and K. Takashima. Adaptively Attribute-Hiding (Hierarchical) Inner Product Encryption *Cryptology ePrint Archive*, Report 2011/543.

[303] R-I. Paise and S. Vaudenay Mutual authentication in RFID: security and privacy. *ASIACCS 2008*, ACM press, 292–299, 2008.

[304] D. Pointcheval and J. Stern. Security Arguments for Digital Signatures and Blind Signatures. *Journal of Cryptology*, **13**, 361–396, 2000.

[305] M.K. Reiter and A.D. Rubin. Crowds: anonymity for web transactions. *ACM Trans. Inf. Syst. Secur.*, **1**, 66–92, 1998.

[306] A. Shallue and C. van de Woestijne. Construction of Rational Points on Elliptic Curves over Finite Fields. *Algorithmic Number Theory - ANTS-VII*, Springer LNCS 4076, 510–524, 2006.

[307] S. Sarkar and S. Maitra. Further Results on Implicit Factoring in Polynomial Time. *Advances in Mathematics of Communications*, **3**, 205–217, 2009.

[308] A. Shamir. Identity-Based Cryptosystems and Signature Schemes. *Advances in Cryptology – Proceedings of CRYPTO '84*, Springer LNCS 196, 47–53, 1985.

[309] A. Shamir. SQUASH: A new one-way hash function with provable security properties for highly constrained devices such as RFID tags. Invited lecture to the RFID Security'07 Workshop. Slides available from `http://mailman.few.vu.nl/pipermail/rfidsecuritylist/2007-August/000001.html`.

[310] A. Shamir. SQUASH - a new MAC with provable security properties for highly constrained devices such as RFID tags. *Fast Software Encryption – FSE 2008*, Springer LNCS 5086, 144–157, 2008.

[311] E. Shen, E. Shi and B. Waters. Predicate Privacy in Encryption Systems. *Theory of Cryptography Conference – TCC 2009*, Springer LNCS 5444, 457–473, 2009.

[312] E. Shi and B. Waters. Delegating Capabilities in Predicate Encryption Systems. *Automata, Languages and Programming – ICALP 2008*, Springer LNCS 5126, 560-578, 2008.

[313] S. Vaudenay. On privacy models for RFID. *Advances in Cryptology – ASIACRYPT 2007*, Springer LNCS 4833, 68–87, 2007.

[314] B. Waters. Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions. *Advances in Cryptology – CRYPTO 2009*, Springer LNCS 5677, 619-636, 2009.

[315] D. Xiao. (Nearly) round-optimal black-box constructions of commitments secure against selective opening attacks. *Theory of Cryptography Conference – TCC 2012*, Springer LNCS 7194, 541–558, 2011.

[316] P. Zimmermann and B. Dodson. 20 Years of ECM. *Algorithmic Number Theory – ANTS VII*, Springer LNCS 4076, 525–542, 2006.