Inicio > … > H2020 > Cryptography for Privacy and Integrity of Computation on Untrusted Machines

Cryptography for Privacy and Integrity of Computation on Untrusted Machines

Informe

Información del proyecto

PICOCRYPT

Identificador del acuerdo de subvención: 101001283

Sitio web del proyecto

DOI
10.3030/101001283

Fecha de la firma de la CE
4 Febrero 2021

Fecha de inicio
1 Junio 2021

Fecha de finalización
31 Mayo 2026

Financiado con arreglo a
EXCELLENT SCIENCE - European Research Council (ERC)

Coste total
€ 1 999 873,00

Aportación de la UE
€ 1 999 873,00

Coordinado por
FUNDACION IMDEA SOFTWARE
Spain

Periodic Reporting for period 2 - PICOCRYPT (Cryptography for Privacy and Integrity of Computation on Untrusted Machines)

Período documentado: 2022-12-01 hasta 2024-05-31

Resumen del contexto y de los objetivos generales del proyecto

Due to phenomena like the ubiquity of the Internet and cloud computing it is increasingly common to store and process data on third-party machines. In spite of its attractive aspects, this trend raises a number of security concerns, including:

How to ensure that the results computed by third parties are correct (integrity) and no unauthorized information is leaked (privacy)?

The current way to deal with these problems is to trust third parties under legislation guarantees. This approach assumes that third-party machines stay honest all time, even if they get hacked! This is unrealistic and contradicted by the numerous security incidents that are regularly reported. In contrast, our vision is that any computing device must be able to store and process data on untrusted machines without risking for privacy and integrity and without the need of trusting these machines. Recent trends in cryptography promise solutions to realize our vision but the existing generation of protocols is limited due to its high costs and its poor support of emerging applications such as data streams processing.

The main goal of PICOCRYPT is to invent a new generation of cryptographic protocols for computing securely on untrusted machines in a way that is cost-effective and suitable for future application scenarios. While existing solutions are either general but impractical or efficient but of limited applicability, in PICOCRYPT we will look for protocols that support a wide range of applications while staying efficient. In particular, to achieve our main goal, PICOCRYPT aims to achieve the following objectives:
- Design new design methodologies and techniques for scaling up the performance of cryptographic protocols for ensuring integrity of computation on untrusted machines.
- Advance the theory and practice of cryptographic primitives for ensuring authenticity of computation on untrusted machines;
- Design new protocols for privacy and integrity of computation on untrusted machines;
- Analyse the challenges imposed by computing on untrusted machines over data streams, and develop new foundations to fit this scenario;
- Assess the cost-effectiveness of our new cryptographic protocols via new evaluation methods and experiments.

The solutions developed in PICOCRYPT can enable a paradigm shift in the way privacy and integrity will be enforced and will have impact in the IT world by making remote computing safer not only for citizens but also for public and private organizations that due to the current risks renounce to these services.

Trabajo realizado desde el comienzo del proyecto hasta el final del período abarcado por el informe y los principales resultados hasta la fecha

The first half of the project focused mainly on the first two aforementioned objectives, namely achieving integrity and authenticity of computation performed on untrusted machines. Our work also addressed the last objective by generating, when appropriate, implementations and experiments to assess the costs of our solutions.

With respect to the problem of integrity of computation, we mainly focused on two cryptographic primitives: zero-knowledge succinct non-interactive arguments (aka zkSNARKs) and vector commitments. Both of these primitives are a form of succinct proof systems that enable an untrusted party to prove the correctness of data and computation by providing short and easy to verify proofs. Our most significant advances in these areas have been on expanding our modular design approach and developing techniques for specialize computations in order to build more efficient zkSNARKs, and on studying the foundations of vector commitments.

More specifically, our most significant results in this period are:
- the design of a new framework and techniques to build universal and updatable zkSNARKs with increased efficiency (published at Asiacrypt 2021);
- the proposal of new zkSNARKs for the problem of proving membership of a batch of elements in a large set (published at ACM CCS 2022);
- the design of a new modular framework to construct efficient zkSNARKs for sequential computations with applications to machine learning and image processing (published at ACM CCS 2023);
- the design of a new methodology for the design and analysis of simulation extractable zkSNARKs (published at TCC 2023);
- the construction of proofs of sequential work (published at Eurocrypt 2023);
- the study of vector commitments by proving that a significant class of these schemes is impossible to realize (published at TCC 2022);
- the realization (based on techniques from algebraic vector commitments) of the first registration-based encryption scheme with practical efficiency (published at ACM CCS 2023).

With respect to the problem of authenticity of computation, we focused on homomorphic signatures. Our most significant results in this period are:
- the introduction and realization of a new class of homomorphic signature schemes with increased expressivity and efficiency (published at ACM CCS 2022);
- the proposal of a new approach to build homomorphic signature schemes via functional commitments, and realizations of this primitive (published at Asiacrypt 2022);
- the construction of the first functional commitment schemes that support the evaluation of any circuit of unbounded depth and, given the previous result, the analogous implication for homomorphic signatures (published at TCC 2023);
- a new methodology to build multi-key homomorphic signatures from single-key ones (published in the Theoretical Computer Science journal).

Avances que van más allá del estado de la técnica e impacto potencial esperado (incluida la repercusión socioeconómica y las implicaciones sociales más amplias del proyecto hasta la fecha)

All the project's results that we mentioned above have advanced significantly the state of the art; this is corroborated by the fact that they have been accepted for publication at top-tier venues in the fields of cryptography and security.

The results achieved so far constitute first steps in the plans of our project. Significant work remains to be done to achieve the main objectives.

In the near future, we will improve our solutions for integrity and authenticity of computation, taking advantage from our recent results. On this front, we believe that the work "Chainable Functional Commitments for Unbounded-Depth Circuits" is particularly promising for inspiring future improvements of both functional commitments and homomorphic signatures.

In the longer term, we will address the problem of designing cryptographic protocols for privacy and integrity of computation. To this end, we expect to take advantage from the techniques that we developed in the context of efficient zkSNARKs.

We will also tackle the problem of designing solutions for secure computation over data streams. Our next steps in this direction include extending our recent results on homomorphic signatures.

picocrypt-logo.png

Última actualización: 17 Septiembre 2024

Permalink: https://cordis.europa.eu/project/id/101001283/reporting/es