PHYLAWS

PROJECT SYNTHESIS REPORT

(Deliverable D1.5)

Grant Agreement number:	**317562**
Project acronym:	**PHYLAWS**
Project title:	**PHYsical LAyer Wireless Security**
Funding Scheme:	**FP7/STREP**
Period:	**from November 1st, 2012 to October 31th, 2016**

Name, title and organisation of the scientific representative of the project's coordinator:

François Delaveau, Thales Communications & Security, France

Tel: + 33 (0)1 46 13 31 32

Fax: + 33 (0)1 41 30 33 08

E-mail: francois.delaveau@thalesgroup.com

Project website address: http://www.phylaws-ict.org/

Version: 1.2

Submission date: 03/03/2016

Table of Content

Table of Figures

List of the Partners of the Phylaws Consortium

TCS:	**Thales Communications and Security SAS (France)**
TPT:	**Institut Mines Telecom – Telecom ParisTech (France)**
ICL:	**Imperial College London (United Kingdom)**
VTT:	**Teknologian Tutkimuskeskus VTT Oy (Finland)**
CEL:	**Celeno Communications Ltd (Israel)**

History of the document – evolution of its content

Redactor	Contributors Reviewers	Version	Date	Comment
François Delaveau	Renaud Molière Christiane Kameni + partners TPT CEL VTT ICL	D1.5 V1.0	20 January 2017	Synthesis Report of the Phylaws project
François Delaveau	Renaud Molière	D1.5 V1.1	21 February 2017	Size reduce according to reviewers' recommendations, better pagination and typo corrections
François Delaveau	Renaud Molière	D1.5 V1.2	2 March 2017	Slight corrections relevant to R&D and dissemination activities into § 2 and 3.

Added notes about the synthesis report

- The present synthesis report deals with overall outputs, achievements and impacts of the Phylaws project over its 4 year duration.
- The publication occurs after the final review meeting of the project held on the 21st of December 2016 in Brussels (Belgium). It completes the periodic reports of the project [PHYLAWS_D.1.2], [PHYLAWS_D.1.3] [PHYLAWS_D.1.3_PPR3], [PHYLAWS_D.1.4] by extracting the essential realizations and impacts of the Phylaws project.

1- Introduction – project objectives - project organization

1.1- Introduction to the document

This document is the Synthesis Report of the Phylaws project (numbered D1.5, as specified in the updated DoW of the project [PHYLAWS_GA-DOW2]). It deals with overall results, management and cost issues of the PHYLAWS project during its whole 48 months duration (2012-11-1, 2016-10-31).

This 62 pages synthesis report includes 27 pages of core content and 35 pages of annex organized in the following manner:

- Section 1 recalls the context, the objectives, the contributors and the overall organization of the project.
- Section 2 first deals with the major scientific and technical results of the project and then focuses on the achieved feasibility proofs, relevant academic and industrial perspectives for the future of the Physec technologies into radio-communication networks.
- Section 3 deals with the major impact of the project: large scale dissemination and added value contributions to standardization.
- Section 4 deals with risk management.
- Section 5 deals with ethical and lawful issues.
- Section 6 concludes the synthesis report.

In addition, several annexes provide useful information on complete results and gather coordination information from the numerous deliverables of the Phylaws project (which can be downloaded on the project Website):

- Annex 1 includes the glossary of the main acronyms used in the technical and coordination tasks of the Phylaws project.
- Annex 2 provides the complete reference list of the Phylaws project relevant to administrative documents, coordination deliverables and technical deliverables.
- Annex 3 provides for each work package and task the list of the relevant deliverables with and a short summary of their content.
- Annex 4 illustrates the feasibility proof of the SKG scheme with Wifi experiments and LTE simulations.
- Annex 5 illustrates the feasibility proof of the SC scheme with Wifi experiments and LTE simulations.
- Annex 6 provides a synthesis of the core content of the standardization proposals during the Phylaws project.
- Annex 7 recalls the main items of the threat models considered in the project.
- Annex 8 recalls the main theoretical notions and principles of Physical Layer Security.

Finally, the reader is kindly reminded that:

- The complete versions of dissemination deliverables, standardization deliverables, advisory board deliverables and technical deliverables are available on the project web site at the following address: http://www.phylaws-ict.org/?page_id=48.
- The complete versions of publications and thesis sustained of produced by the Phylaws project are also available on the project web site at the following addresses: http://www.phylaws-ict.org/?page_id=92 and http://www.phylaws-ict.org/?page_id=457.

1.2- Project context, objectives, contributors and achievements

1.2-1. Context

Wireless communication is becoming a universal way to access information for nearly every human around the world and also presents major risks to society, owing to the widely recognized leaks and unsafe technologies in the current wireless public networks. Basically, security protocols relying only on bit level cryptographic techniques may exhibit severe drawbacks into mass market worldwide radio networks and can be insufficiently secure in practice.

Phylaws considers new approaches investigated recently in order to exploit security opportunities offered by signal processing operated at the physical layer level with respect to the fundamental notion of security in the context of information theory. The project focused on practical applications of Physical Layer Security (Physec) into public wireless radio networks in order to enhance the security of wireless communications in an affordable, flexible and efficient manner.

1.2-2. Objectives

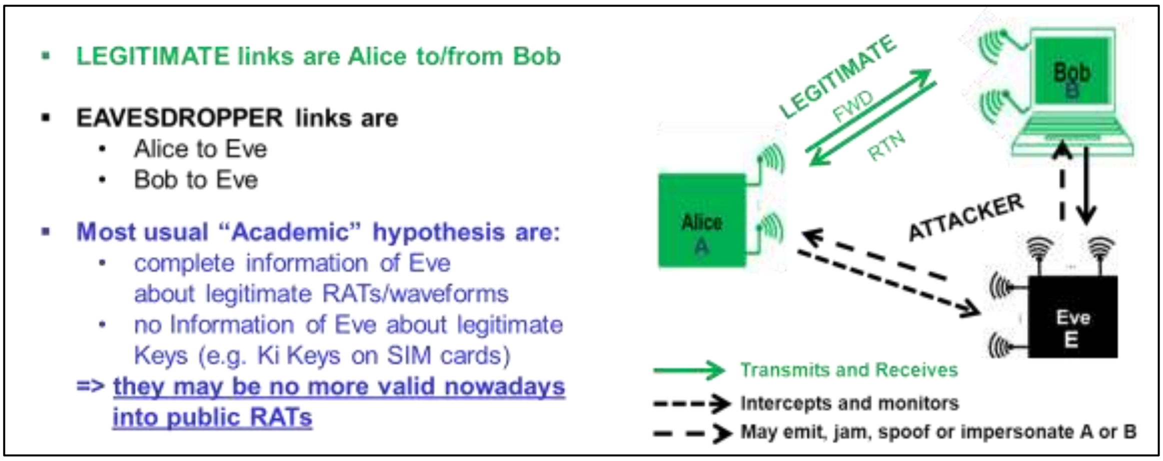
Our main goal was to propose and prove feasibility of key-free secure schemes

- easy to develop and to validate
- convenient to embed necessitating low energy and computing resources,
- applicable to a large variety of existing and future standards for a wide set of communication services.

In a more concrete manner, Phylaws intended

- to design, simulate and experiment new key free privacy and confidentiality schemes for subscriber signalling and user data messages, that exploit the randomness of radio-propagation and apply very early into the radio access protocol of wireless networks.
- to evaluate and optimize their performance in real-field radio environments (processing embedded in real communication devices, applying to real-field radio signals into realistic network topologies).
- to impact both existing and future Radio Access Technologies (existing 2G/3G/4G/WLAN, future 5G)

Figure 1 illustrates the basic study configuration which involves a legitimate transmitter Alice, a legitimate receiver Bob and an attacker Eve. It is noticeable that Eve is not only a passive eavesdropper but may also have protocol aware jamming and spoofing capabilities, especially to disturb or impersonate Alice and Bob at the beginning of the legitimate communication (negotiation phases). Annex 7 provides more details about Eve models considered in Phylaws, while annex 8 recalls the theoretical principles of Physical Layer Security



- LEGITIMATE links are Alice to/from Bob
- EAVESDROPPER links are
  - Alice to Eve
  - Bob to Eve
- Most usual "Academic" hypothesis are:
  - complete information of Eve about legitimate RATs/waveforms
  - no Information of Eve about legitimate Keys (e.g. Ki Keys on SIM cards)

  => they may be no more valid nowadays into public RATs

Figure 1: security issues studied by Phylaws - Illustration of the wiretap channel and several kinds of threats

1.2-3. Partners

For reaching these objectives, the Phylaws' project was built on a suitably sized consortium combining:

- an excellent academic expertise (Telecom Paris Tech and Imperial College of London) in order to address information theory fundamentals, to design optimal codes, to design furtive signal waveforms and versatile radio access protocols
- a major research center (Teknologian Tutkimuskeskus VTT Oy) for the development and test of several competing techniques;
- a SME commitment perfectly aligned with the application targets (Celeno Communication LdT)
- a strong industrial commitment highly motivated by security in wireless networks as a manufacturer, as an end-user and as a provider of wireless communication services (Thales Communications and Security).

All partners involved in the project were chosen for their high values skills and complementary competences. The complementarity of partners inside the consortium ensured both innovation and impact towards industrial applications, and assessed validation of the commercial goals and validation of the society use relevance.

Moreover, the project took many benefits from the recommendations and advice of an international Advisory Board (AB), constituted by very high level personalities from governmental bodies, standardization bodies or academia. This AB was one of the cornerstones of the project, contributed to elaborate the excellent technical developments and demonstrations and their wide spreading, and shared a proper vision for optimized project impact at standardization bodies and major stakeholders.

1.2-4. State of the art, academic studies and development

For an efficient leadership of developments and evaluations of the secure schemes in the project, the Phylaws team performed:

- Intensive investigations on the state of the art of security protocols for radio networks that revealed their drawbacks and failures when applied to public mass marked worldwide wireless networks.
- Deep academic researches about the radio-channel, Secret Key Generation and Secrecy Coding. This led to the completion of two PhD thesis, two workshops dedicated on physical layer security, numerous publications and three patents during of the project.
- Industrial development of the three patented key-free secure schemes and relevant metrics.

1.2-5. Test bed and simulator development

For achieving convincing feasibility proof of the secure schemes developed by the project, the Phylaws team developed

- A test bed in the perspectives of propagation studies and experimental feasibility proof for Wifi. This test bed is able:
    - To record signals in real networks during considerable amount of time (several seconds).
    - To transmit, receive, record and process Wifi signal in the 2.4 GHz and 5 GHz band.
    - To implement and study performance of secure schemes into a real field wifi transmission processed into existing commercial embedded wifi chipsets.
- A LTE simulator in the perspectives feasibility proof into radio-cell networks. This LTE simulator is able:
    - To model realistic 4G links in realistic radio environments: transmission, radio propagation, receiving, processing and LTE protocol layer are all based on most advanced simulation components [QUADRIGA, VIENNA]).
    - To implement and study performance of the patented secure schemes into the simulated LTE transmission and processing with significant statistics over radio and network parameters.

1.3- Project organization

Figure 2 recalls the organization of the Phylaws project in 6 work packages (each including three or four tasks) over its 4 years duration. It also recalls the leadership distribution of work packages over partners.

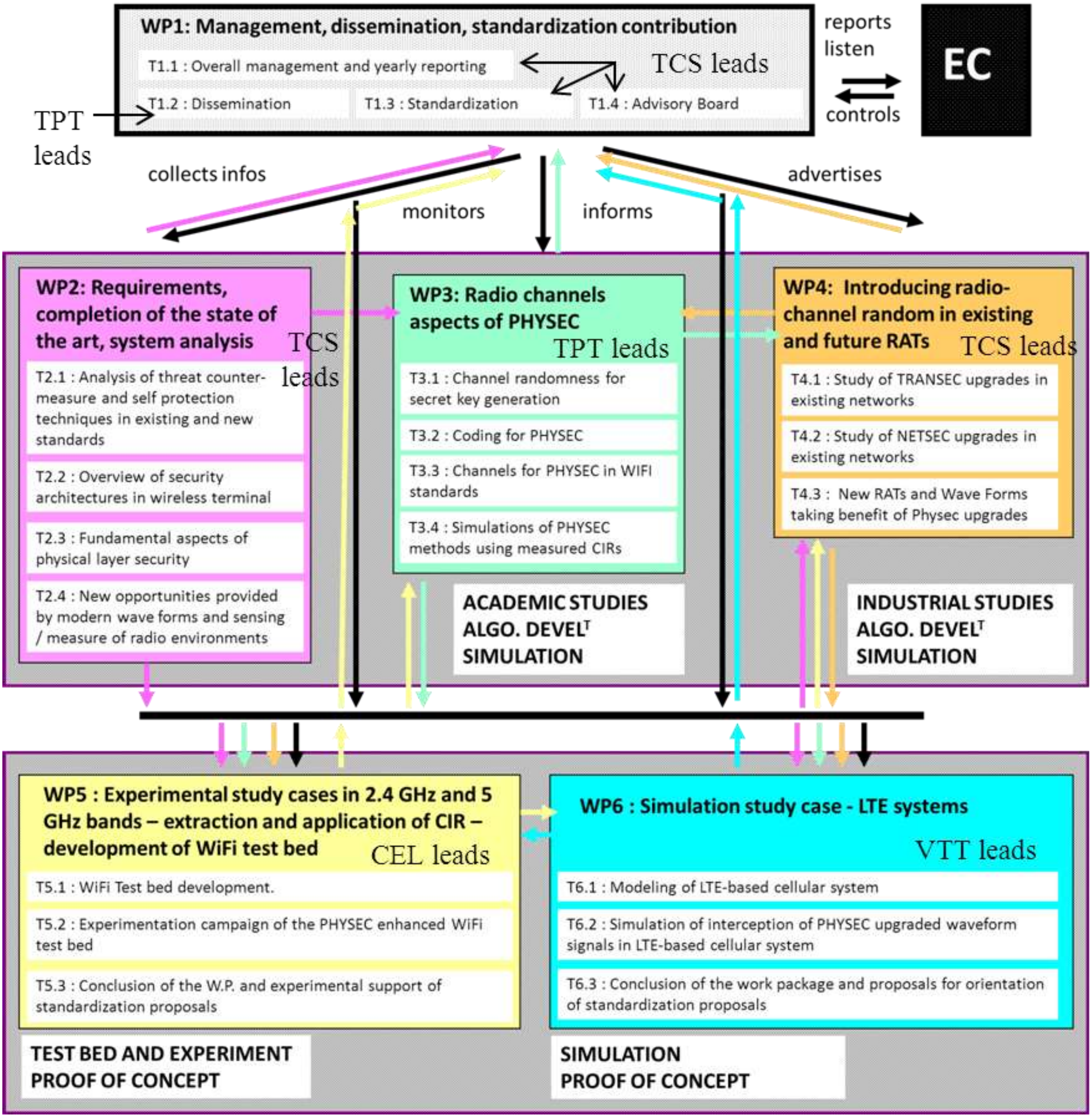

WP1: Management, dissemination, standardization contribution
T1.1 : Overall management and yearly reporting
TCS leads
T1.2 : Dissemination
T1.3 : Standardization
T1.4 : Advisory Board
TPT leads
reports
listen
controls
EC
collects infos
monitors
informs
advertises
WP2: Requirements, completion of the state of the art, system analysis
TCS leads
T2.1 : Analysis of threat counter-measure and self protection techniques in existing and new standards
T2.2 : Overview of security architectures in wireless terminal
T2.3 : Fundamental aspects of physical layer security
T2.4 : New opportunities provided by modern wave forms and sensing / measure of radio environments
WP3: Radio channels aspects of PHYSEC
TPT leads
T3.1 : Channel randomness for secret key generation
T3.2 : Coding for PHYSEC
T3.3 : Channels for PHYSEC in WIFI standards
T3.4 : Simulations of PHYSEC methods using measured CIRs
ACADEMIC STUDIES
ALGO. DEVELT
SIMULATION
WP4: Introducing radio-channel random in existing and future RATs
TCS leads
T4.1 : Study of TRANSEC upgrades in existing networks
T4.2 : Study of NETSEC upgrades in existing networks
T4.3 : New RATs and Wave Forms taking benefit of Physec upgrades
INDUSTRIAL STUDIES
ALGO. DEVELT
SIMULATION
WP5 : Experimental study cases in 2.4 GHz and 5 GHz bands – extraction and application of CIR – development of WiFi test bed
CEL leads
T5.1 : WiFi Test bed development.
T5.2 : Experimentation campaign of the PHYSEC enhanced WiFi test bed
T5.3 : Conclusion of the W.P. and experimental support of standardization proposals
TEST BED AND EXPERIMENT
PROOF OF CONCEPT
WP6 : Simulation study case - LTE systems
VTT leads
T6.1 : Modeling of LTE-based cellular system
T6.2 : Simulation of interception of PHYSEC upgraded waveform signals in LTE-based cellular system
T6.3 : Conclusion of the work package and proposals for orientation of standardization proposals
SIMULATION
PROOF OF CONCEPT

Figure 2: Phylaws project organisation

2- Major scientific and technical outputs of the Phylaws project – academic and industrial perspectives

2.1- General introduction to the main outputs of the Phylaws project

During the project, the Phylaws' team investigated the security weaknesses and constraints of radio network standards, studied the radio propagation channel as a random source, and developed and experimented 3 key-free secure schemes, with several variants and optimization procedures.

- The first scheme realizes the Secure Pairing (SP) of communication nodes and terminals at the early stages of the radio access, by using a dedicated key-free radio protocol named Interrogation and Acknowledgement Sequences (IAS), supported by specific designed signals called Tag Signals (TS), which design is made dependant on the on-going channel measurements by radio-communications nodes and terminals.
- The second scheme, called Secret Key Generation (SKG), generates secret shared keys from the randomness extracted at the physical interface by radio-communications nodes and terminals inside their synchronization and equalization processing.
- The third scheme, called Secrecy Coding (SC) provides a radio advantage to legitimate transmitters and receivers when they face any kind of threats (eavesdropper, protocol aware jammer, spoofing systems) and applies secret codes to ensure information theoretic secrecy of legitimate transmitted data (which is equivalent to the semantic secrecy which is usually targeted by crypto schemes).

In each case, the ultimate goal is to achieve optimized protection in the radio access protocol (transec) to enhance privacy of subscribers (netsec), and confidentiality of user communication into on-going traffic messages (comsec), especially when no protection can be set because of a lack of classical cryptographic key.

A synthesis of the relevant developments, academic and industrial results is given in the following of this section 2.

While achieving studies, experiments, feasibility proof and optimization of the secure schemes above, the Phylaws team performed a large dissemination in the scientific community and an intensive activity at standardization bodies.

A synthesis of the relevant strategies, achievements and impacts is given section 3.

2.2- Secured schemes developed into the Phylaws project

2.2-1. Secure Pairing (SP)

The key-free secure pairing scheme invented by the Phylaws team is dedicated to the earliest stages of the radio access of nodes and terminal when facing any kind of threats at the radio layer. It prevents any monitoring and any intrusion by a third party during this crucial period. As a consequence it can support the implementation of further Physec protections (such as SKG and SC) thanks to reliably authenticated radio-channel measurements. Moreover it can also support terminal/node authentication and identification into the further stages of the radio access protocols to network.

The SP scheme is based on dual sense Interrogation and Acknowledgement sequences supported by low power forward (FWD) and return (RTN) Tags Signals (TS) emitted under beacon signals:

- TS are designed with pseudo noise spread sequences of high Spreading Factor (SF) to allow efficient Matched Filtering (MF) procedures and accurate estimations of the Channel Impulse Response (CIR) by legitimate nodes and terminals (see Figure 3 - B part), while any third party losing the building of the TS can no more achieve neither detection nor synchronization of the TS.
- The design of TS at each new IAS is made dependent on the on-going radio-channels measurements on the previous IAS - see Figure 3 - A part. The choice of thee TS sequence from the channel measurement uses a simplified quantization algorithm without any public exchange (see next paragraph for more information).

- The relevant power ratio, called Tag to Signal Ratio (TSR) ensures the protection of the TS when facing Eves receiving and processing.
- To achieve ultimate resilience when facing most advanced threats, several other protections can be added in the building and processing of tag signals such as
  - Uncoordinated Spread Spectrum and Time Jitter.
  - Full arbitrary building of sets of tags signals.

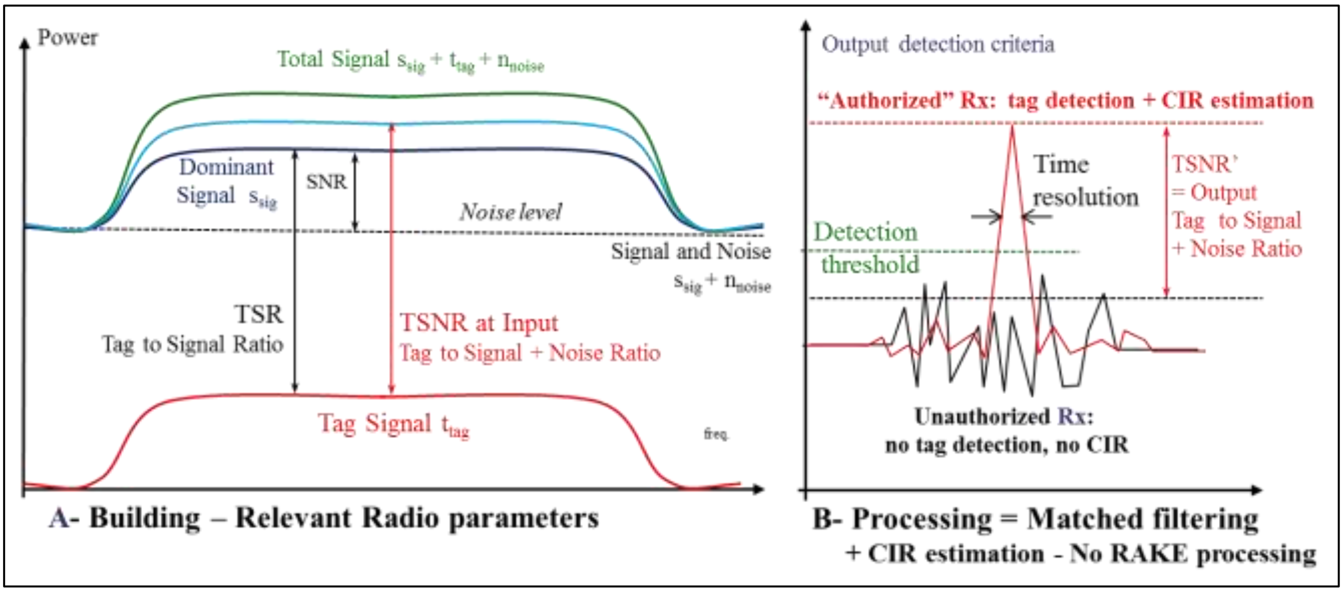
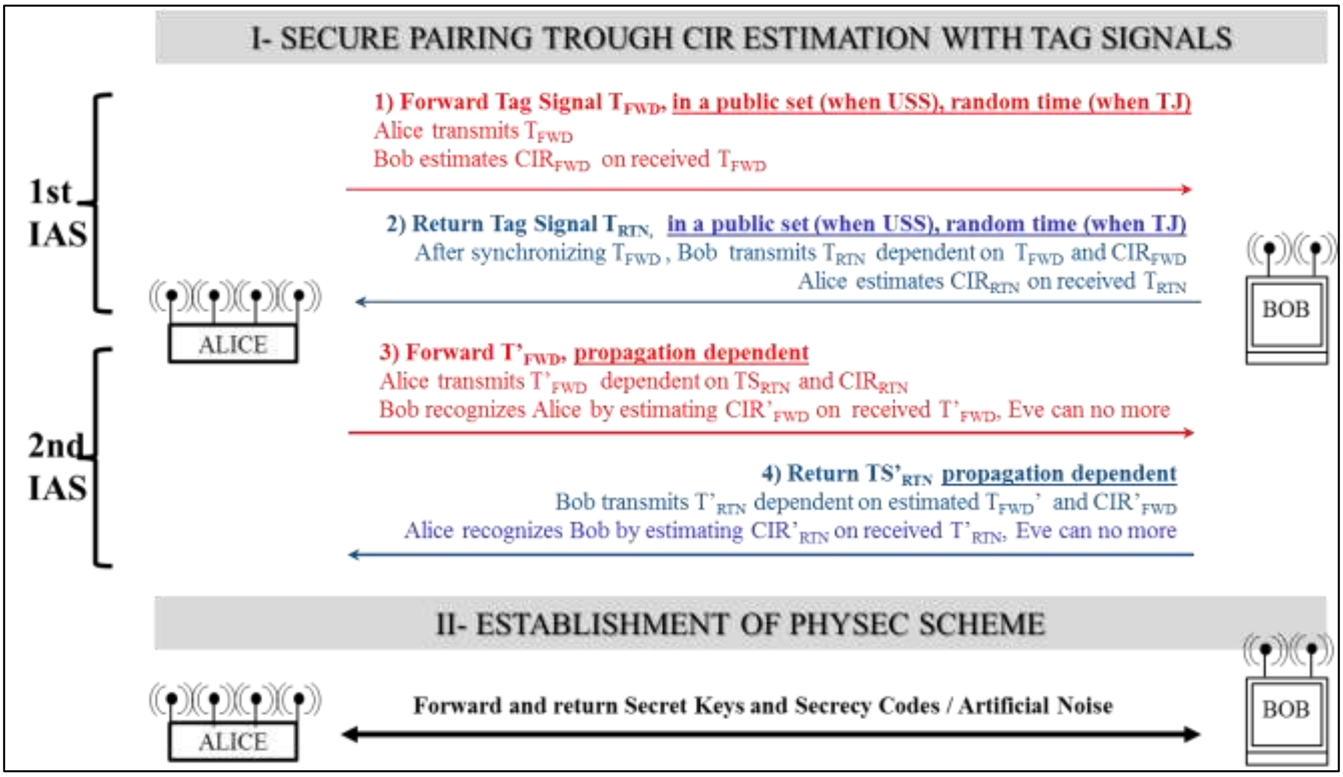

Power
Total Signal $s_{sig} + t_{tag} + n_{noise}$
Dominant Signal s_{sig}
SNR
Noise level
Signal and Noise
$s_{sig} + n_{noise}$
TSR
Tag to Signal Ratio
TSNR at Input
Tag to Signal + Noise Ratio
Tag Signal t_{tag}
freq.
A- Building – Relevant Radio parameters
Output detection criteria
"Authorized" Rx: tag detection + CIR estimation
Time resolution
TSNR'
= Output
Tag to Signal
+ Noise Ratio
Detection threshold
Unauthorized Rx:
no tag detection, no CIR
B- Processing = Matched filtering
+ CIR estimation - No RAKE processing

Figure 3: tag signals - configuration of transmission, reception and processing



1) Forward Tag Signal T_{FWD}, in a public set (when USS), random time (when TJ)
Alice transmits T_{FWD}
Bob estimates CIR_{FWD} on received T_{FWD}

2) Return Tag Signal T_{RTN}, in a public set (when USS), random time (when TJ)
After synchronizing T_{FWD} , Bob transmits T_{RTN} dependent on T_{FWD} and CIR_{FWD}
Alice estimates CIR_{RTN} on received T_{RTN}

3) Forward T'_{FWD}, propagation dependent
Alice transmits T'_{FWD} dependent on TS_{RTN} and CIR_{RTN}
Bob recognizes Alice by estimating CIR'_{FWD} on received T'_{FWD}, Eve can no more

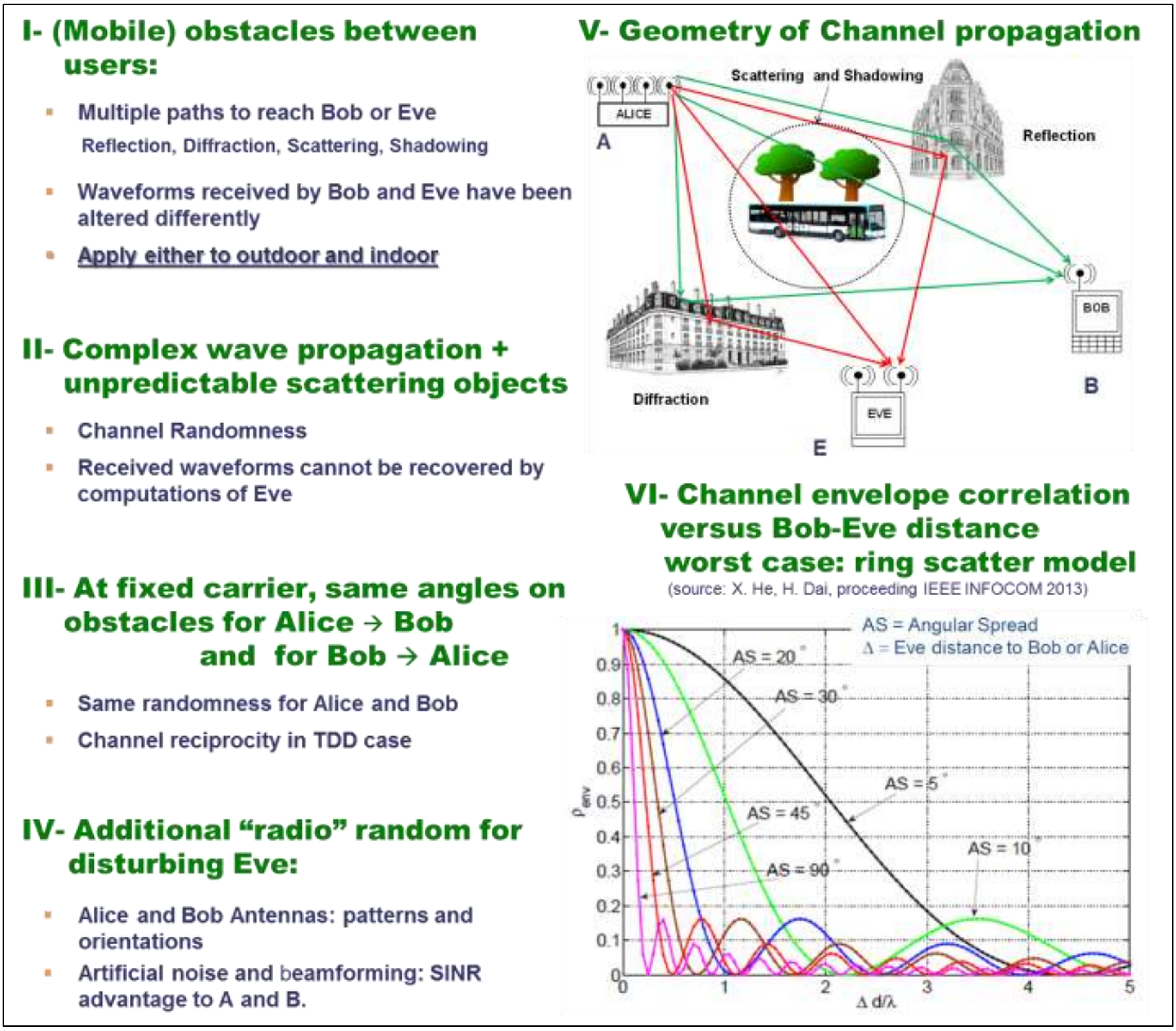
4) Return TS'_{RTN} propagation dependent
Bob transmits T'_{RTN} dependent on estimated T_{FWD}' and CIR'_{FWD}
Alice recognizes Bob by estimating CIR'_{RTN} on received T'_{RTN}, Eve can no more

Forward and return Secret Keys and Secrecy Codes / Artificial Noise

Figure 4: synthesis of the IAS protocol supported by Tag Signals (TS)

2.2-2. Secret Key generation (SKG)

The Secret Key Generation scheme computes shared keys at legitimate nodes and terminals from the randomness extracted from the radio propagation channel (see Figure 5 below). The channel reciprocity ensures the ability for the legitimate node and terminal to compute a very similar key, while the channel diversity ensures the privacy of the computed keys when facing any third party.



I- (Mobile) obstacles between users:

- Multiple paths to reach Bob or Eve
  Reflection, Diffraction, Scattering, Shadowing
- Waveforms received by Bob and Eve have been altered differently
- Apply either to outdoor and indoor

II- Complex wave propagation + unpredictable scattering objects

- Channel Randomness
- Received waveforms cannot be recovered by computations of Eve

III- At fixed carrier, same angles on obstacles for Alice → Bob and for Bob → Alice

- Same randomness for Alice and Bob
- Channel reciprocity in TDD case

IV- Additional “radio” random for disturbing Eve:

- Alice and Bob Antennas: patterns and orientations
- Artificial noise and beamforming: SINR advantage to A and B.

V- Geometry of Channel propagation

VI- Channel envelope correlation versus Bob-Eve distance worst case: ring scatter model

(source: X. He, H. Dai, proceeding IEEE INFOCOM 2013)

Figure 5: physical foundations of the usage of the radio propagation channel as a private source of randomness

This key-free secure scheme is very useful to enhance the protection of clear text signaling and access messages that include sensitive data in most of public radio-networks.

While theoretical foundations of SKG are well described in the literature (see for example [BLOCH]), we developed during the Phylaws project a complete embeddable SKG scheme with the following key enhancements (see Figure 6):

- Accurate channel estimation algorithms (on real field radio signals) that extract the complete radio propagation richness (in terms of randomness) and output the Channel State Information (CSI), including amplitude and phase information, as illustrated Figure 7.

- Efficient channel de-correlation pre-processing prior to SKG computation in order or enhance the key privacy in very stationary radio-environments.
- Optimized variant of the Channel Quantization Algorithm introduced by Wallace [WALLACE]
- Optimized tuning of the key reconciliation and key privacy amplification in order to achieve both reciprocity restoration and key bit correction while enhancing key randomness and privacy.
- Study and development of suitable security metrics to be embedded in the SKG schemes.

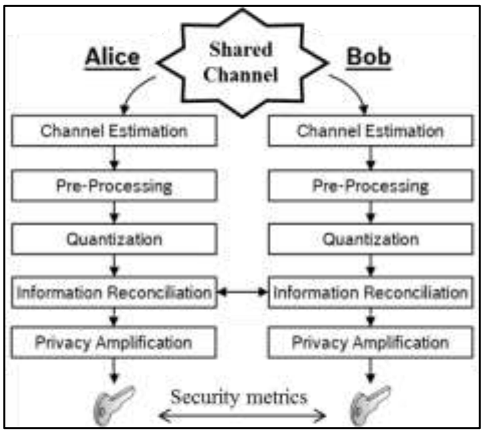


Figure 6: illustration of the SKG algorithm blocks developed and experimented into the Phylaws project

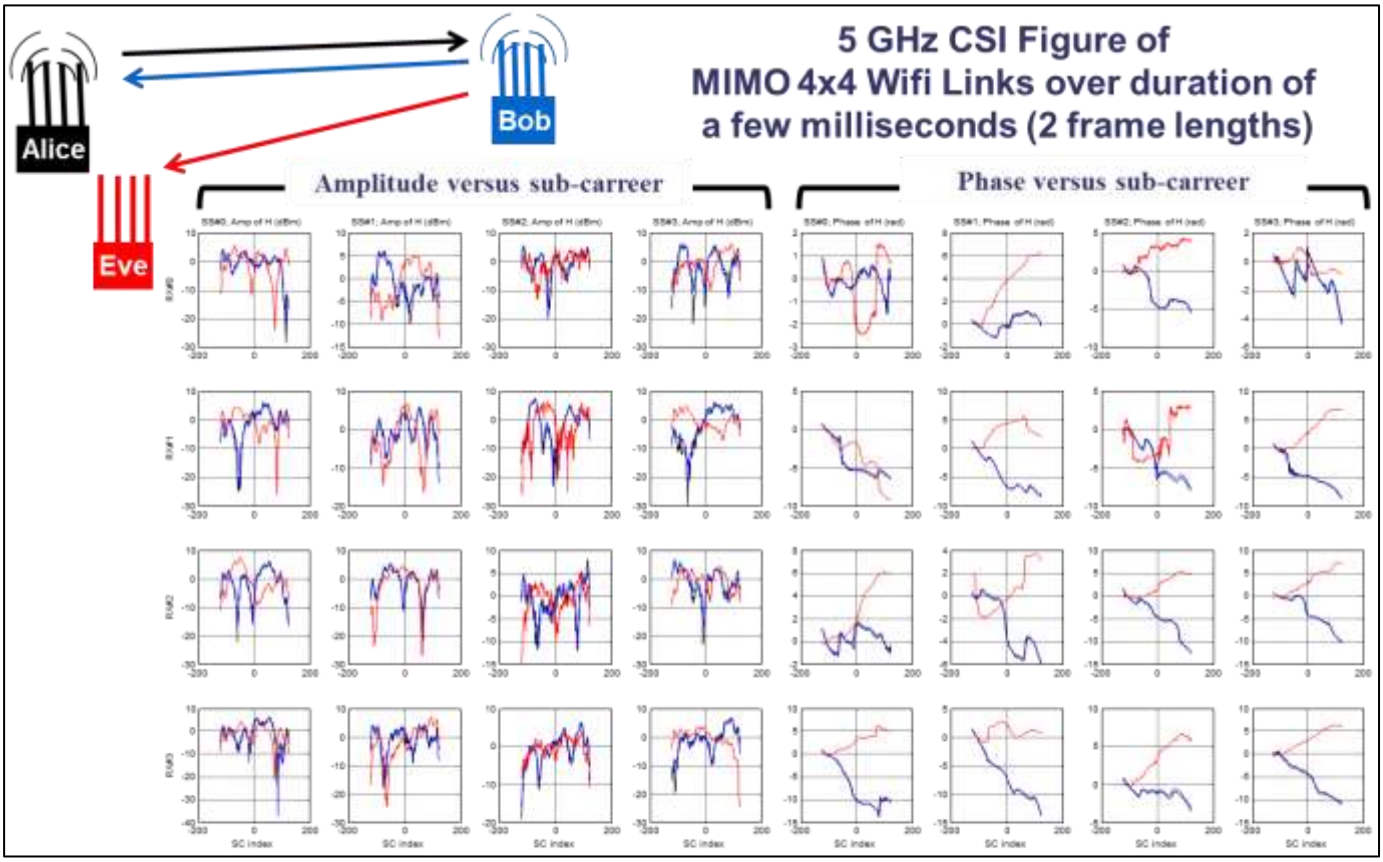
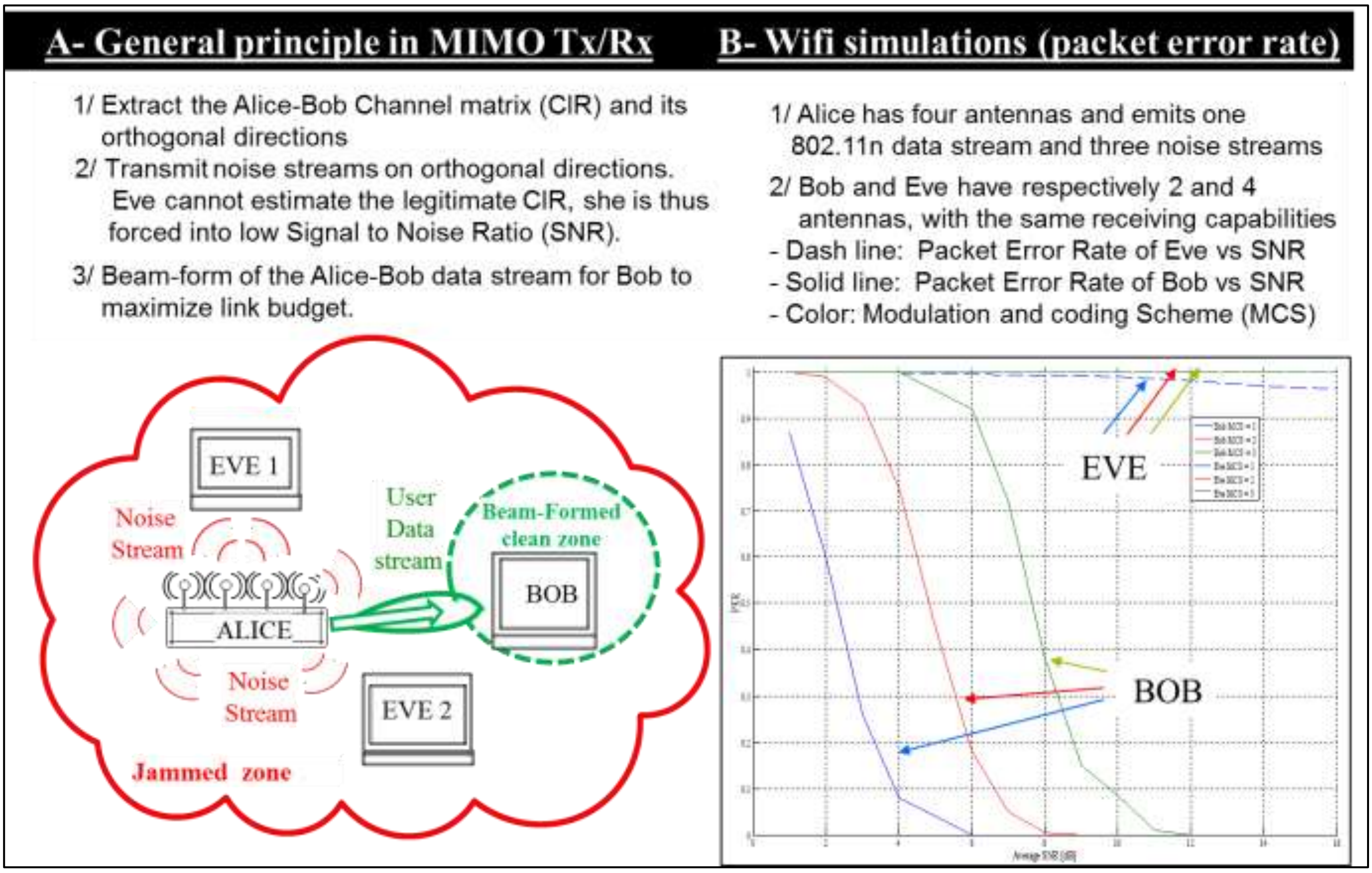


Figure 7: illustration of CSI reciprocity and diversity at the 5 GHz Wi-Fi band: case of CSI in indoor environment. 4x4 MIMO transmitter receiver and eavesdropper over short term duration (a few milliseconds) – Eve-Alice distance is about ten wavelengths (60 cm) - slight mobility of scatterers

2.2-3. Secrecy Coding (SC) under established Radio Advantage (RA) with Artificial Noise (AN) and Beam Forming (BF)

The Secrecy Coding scheme aims at designing public codes that achieves both reliable decoding of errors and semantic-level secrecy of the user data up to the secrecy capacity, less or equal to the Shannon capacity. Achieving a positive secrecy capacity requires a Radio Advantage (RA) of the legitimated received to the attacker receiver (meaning a Shannon capacity of the legitimate channel greater to the Shannon capacity of the attacker channel - [BLOCH]).

Such a radio advantage can be achieved with several means (directive antenna, short range communication, intentional jamming, etc.). The Phylaws team developed and experimentally proved a scheme based on a MIMO transmitting and receiving architecture with Artificial Noise (AN) and Beam Forming (BF) such as illustrated in Figure 8.



A- General principle in MIMO Tx/Rx

1/ Extract the Alice-Bob Channel matrix (CIR) and its orthogonal directions
2/ Transmit noise streams on orthogonal directions. Eve cannot estimate the legitimate CIR, she is thus forced into low Signal to Noise Ratio (SNR).
3/ Beam-form of the Alice-Bob data stream for Bob to maximize link budget.

B- Wifi simulations (packet error rate)

1/ Alice has four antennas and emits one 802.11n data stream and three noise streams
2/ Bob and Eve have respectively 2 and 4 antennas, with the same receiving capabilities
- Dash line: Packet Error Rate of Eve vs SNR
- Solid line: Packet Error Rate of Bob vs SNR
- Color: Modulation and coding Scheme (MCS)

Figure 8: creating a radio advantage with Artificial Noise and Beam-Forming

Once the radio advantage is set, the formulation of the secrecy capacity is established and the existence of optimal secrecy codes is proven in any case (see for example [BLOCH]). Nevertheless their general determination for continuous radio channels is not established and the practical design of optimal secrecy codes in realistic radio-environments is challenging.

Inspired by academic results on polar codes that have been proven to provide strong security for discrete channels [ARIKAN, MAHDAVIFAR], the Phylaws team invented slightly sub-optimal secrecy coding schemes that concatenate nested polar codes or Reed Muller (RM) Codes (which generator matrices are close to the ones of polar codes) to capacity approaching code (LDPC, turbo, others) that are usually used into wireless standards (see Figure 9 - A).

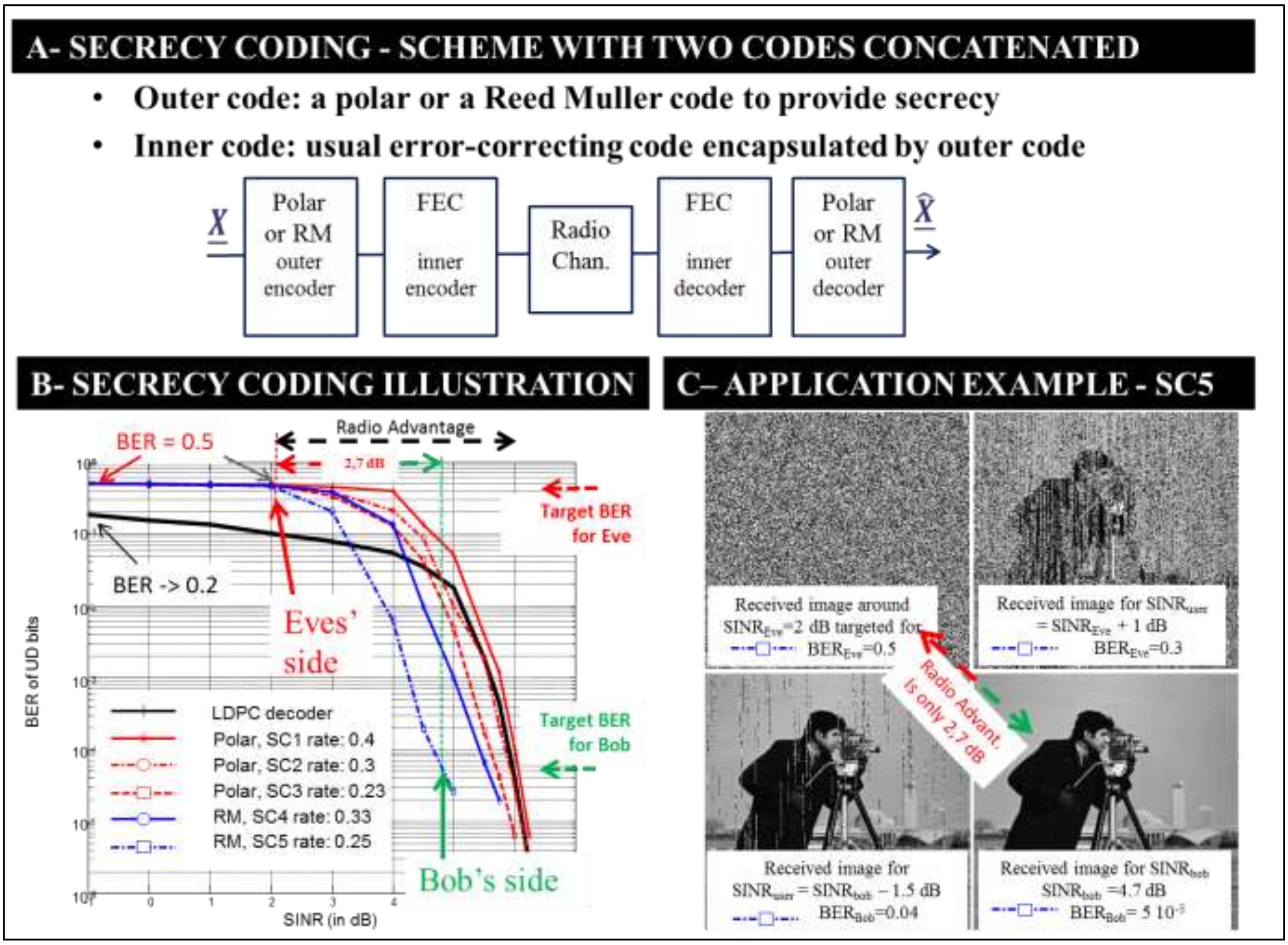
In our secrecy coding schemes, the continuous channel processed by the inner code is viewed as a discrete Binary Symmetric Channel (BSC) by the outer decoder, what is a suitable condition for exploiting polar codes and RM codes [MAHDAVIFAR].

As shown in Figure 9 – B:

- the secrecy effect of the outer codes achieves perfect secrecy at attacker's side who is disadvantaged by lower Signal to Interference + Noise Ratio (SINR). For example, when the attacker's SNIR is 0 as in Figure 9 – B, the BER at the output of the outer decoder is 0.5 instead of 0.1 to 0.3 at the output of the classical inner decoder. This leads to non-intelligible user data as shown in Figure 9 – C).

- legitimate users manage to correct errors up to the decoding capacity of the secrecy code since they have few decibels of Signal to Interference + Noise ratio (SINR): for example, when the legitimate SINR is 4.7 dB as in Figure 9 – B, the BER at the output of the outer decoder is $5*10^{-5}$, what leads to perfectly decoded user data as shown Figure 9 – C bottom right part).

To the best of our knowledge, this invention of the Phylaws project is the first practical implementation of a secrecy coding scheme. In addition, our studies proved that the performance of the schemes is very close to optimal performance. In Gaussian channels, the schemes reach from 50 to 70% of the secrecy capacity.



A- SECRECY CODING - SCHEME WITH TWO CODES CONCATENATED

- Outer code: a polar or a Reed Muller code to provide secrecy
- Inner code: usual error-correcting code encapsulated by outer code

B- SECRECY CODING ILLUSTRATION

C– APPLICATION EXAMPLE - SC5

Figure 9: design of the secrecy coding schemes invented by the Phylaws project

2.3- Feasibility proof and resilience analysis of the secured schemes into the Phylaws project

2.3-1. Feasibility proof and resilience analysis of Secure Pairing in simplified laboratory environment

Phylaws achieved the feasibility proof of the major key items of the SP scheme by combining laboratory tests and simulation inputs from real field records from the Wifi test bed. We established the following proofs:

- Capability of defining sets of arbitrary random Tag Signals of significant number and correlation quality.
- Capability to achieve protection level (TSR of -10 to -20 dB) with Tag Signals which period and spreading factor match the frame length of radio standards (typical time duration in LTE and Wifi is 10 ms).
- Capability to provide accurate synchronization and estimations of Channel Impulse Response (CIR) at legitimate receivers.
- Capability to generate or select new Tag Signals from the previous CIR estimations shared by legitimate nodes and terminals (thanks to channel reciprocity) for following interrogations.

Thus, after inventing and patenting the SP scheme [PHYLAWS_Patent1], Phylaws opened the road toward its complete feasibility proof. At the end of the project, the remaining step is the achievement of Self Interference Mitigation into the legitimate receiver, similar as Full Duplex technologies which feasibility was proven by other EC-ICT granted project [DUPLO], and that are intensively studied for spectrum efficiency enhancements [FUDU].

In addition, the resilience and security analyses performed into the project showed very good performance of the SP schemes when facing passive attacker (security in this case is extremely high) and also when facing advanced active and man in the middle attackers.

2.3-2. Complete feasibility proof and security analysis of Secret Key Generation in real environments

Phylaws achieved the complete feasibility proof of the SKG scheme by experiments on several radio carriers, with a special focus on Wifi links recorded in real indoor environment (Figure 10) and simulations of LTE links.

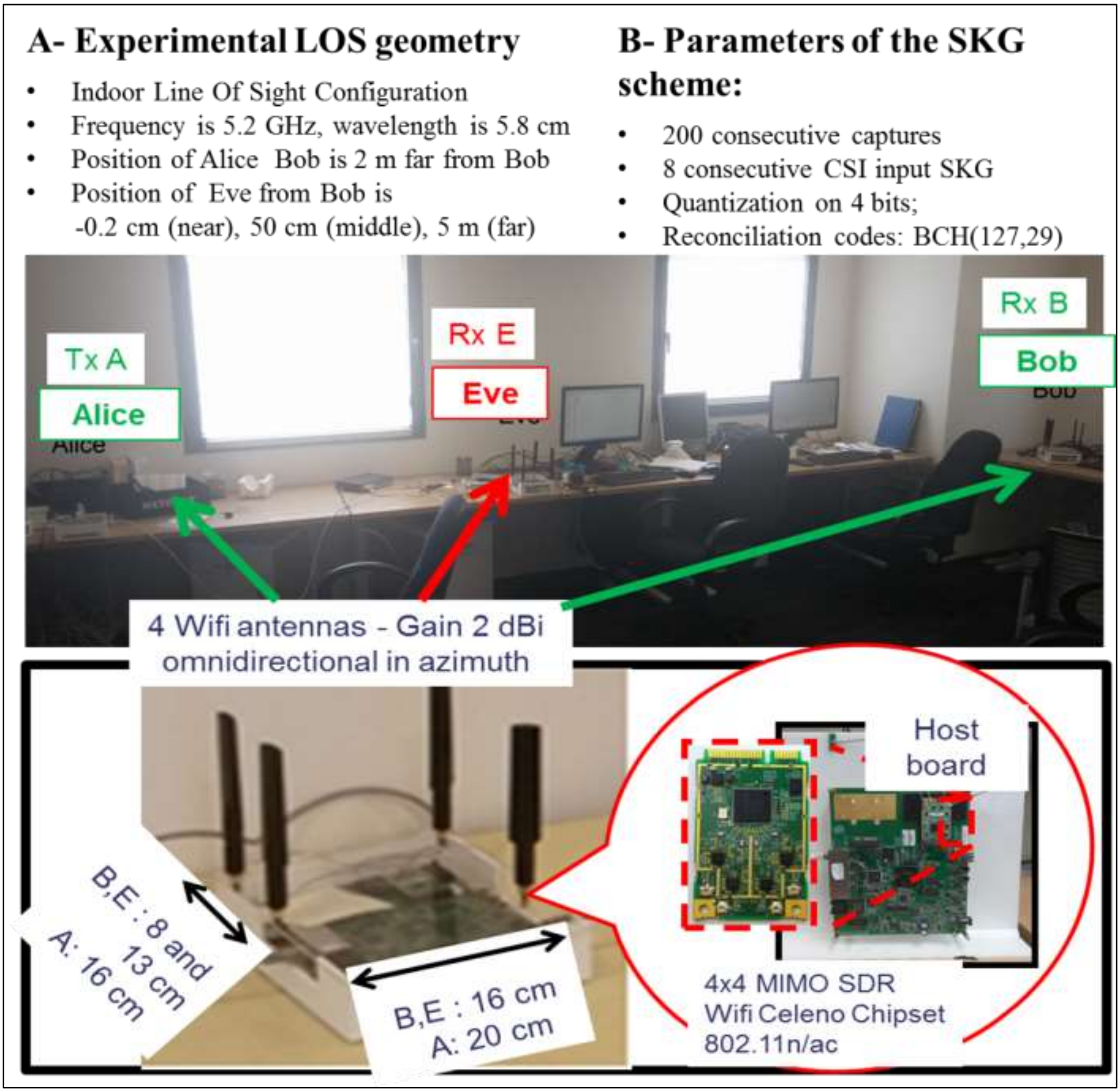
We established the following proofs:

- The channel reciprocity and the diversity of radio propagation that allow the design of keys of significant number, length and privacy. All our experiments confirmed these major properties of the radio channel in various environments and pedestrian geometries.
- Even in most stationary environment, a significant randomness quality of the key can be achieved with de-correlation pre-processing of the radio channel.
- The spatial diversity of the radio channel is effective in all measured environments and the estimations of mutual entropy and information ensure good rate and privacy properties of the generated keys bits.
- The parameters of the SKG processing can be tuned as a function of the mutual entropy estimates by legitimates nodes and terminals through their radio channels measurements.
- Embeddable security metrics such as Inter Heath Check [IHC] apply very well at the end of the SKG processing.

Thus, after patenting the invented SKG scheme [PHYLAWS_Patent2], Phylaws proved its feasibility and achieved its performance study.

Moreover, the resilience and security analyses performed into the project:

- Showed that very good performance of the SKG schemes based on Channel State Information can be achieved in most of realistic radio-environments, especially pedestrian rural and urban, but also indoor fixed and empty geometries.
- Identified numerous application cases of SKG into Time Division Duplex radio networks, either standardized or private.



A- Experimental LOS geometry

- Indoor Line Of Sight Configuration
- Frequency is 5.2 GHz, wavelength is 5.8 cm
- Position of Alice Bob is 2 m far from Bob
- Position of Eve from Bob is -0.2 cm (near), 50 cm (middle), 5 m (far)

B- Parameters of the SKG scheme:

- 200 consecutive captures
- 8 consecutive CSI input SKG
- Quantization on 4 bits;
- Reconciliation codes: BCH(127,29)

Figure 10: example of geometry for the SKG experiments

Finally, we can consider that:

- the feasibility proof of the Secret Key Generation is achieved
- the metrics and performance of the SKG schemes are established for realistic radio environments
- the SKC schemes developed and patented by the Phylaws consortium are experimentally proven for pedestrian and indoor geometries
- these SKG schemes are mature for standardization and industrial implementation

Considering the Line of Sight geometry described Figure 10, Figure 11 illustrates some of the experimental results of our SKG schemes.

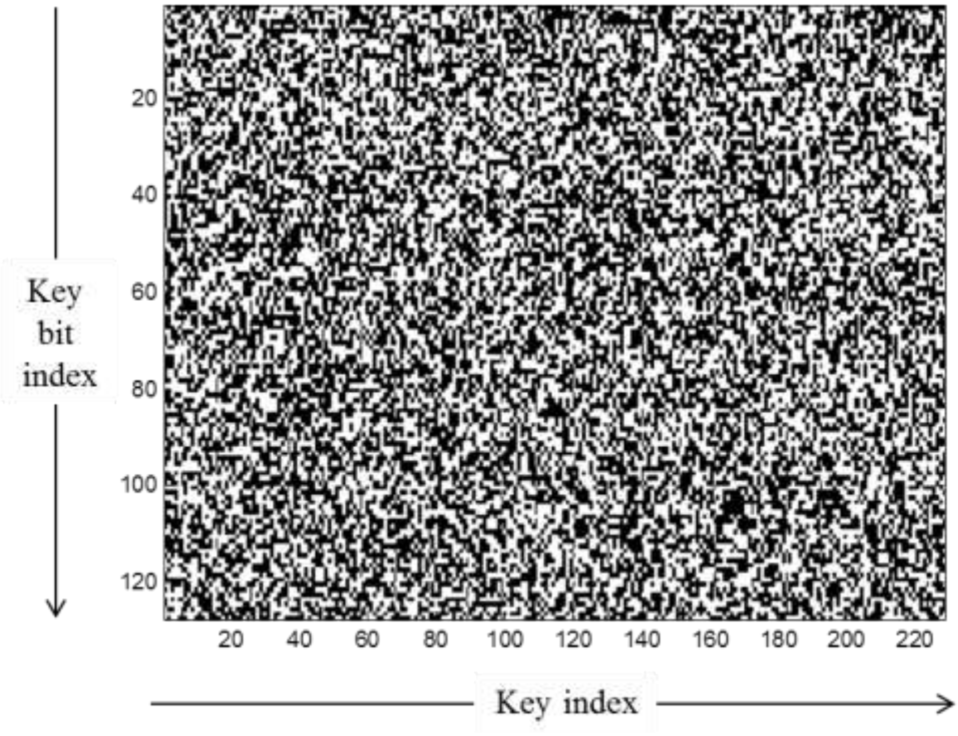


Figure 11: illustration of keys randomness output by the SKG schemes (228 Keys of 127 bits each)

Complete illustration about the steps and the performance of the SKG scheme over experimental and simulation results can be found in annex 4.

2.3-3. Complete feasibility proof and security analysis of Secrecy Coding in real environments

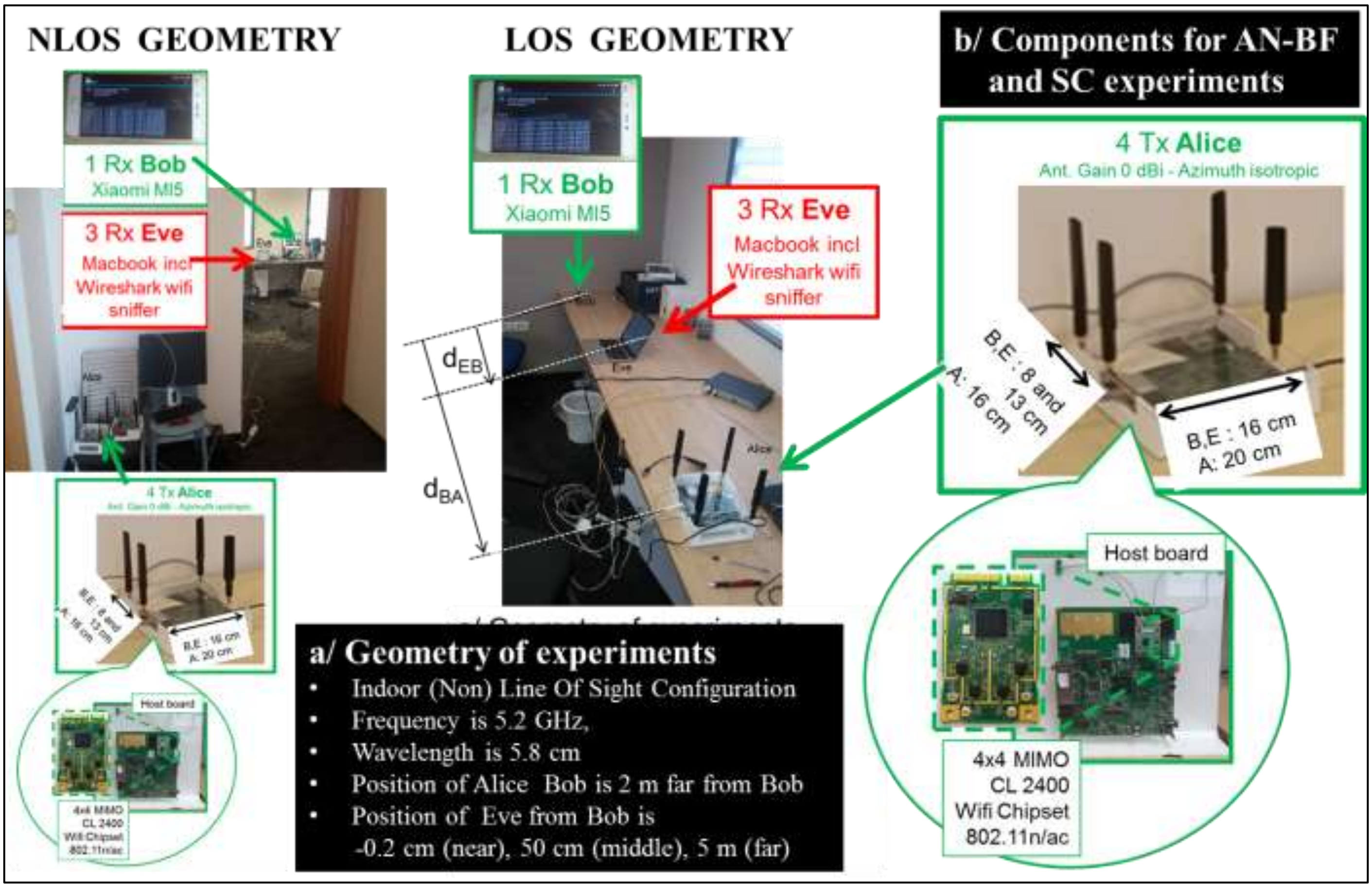
Phylaws has achieved the complete feasibility proof of the SC scheme by experiments on several radio carriers, with a special focus on Wifi links recorded in real indoor environment (Figure 12) and simulations of LTE links.

We established the following proofs:

- The capability of enabling and control significant radio advantages in MIMO RAT, with only a negligible or slight decrease of user data rates, thanks to the Artificial Noise and Beam-Forming processing.
- The capability to tune the parameters of the secrecy codes as a function of the established and controlled radio advantage.
- The “quasi-perfect” reliability and confidentiality of secret coded user data.

Thus, after patenting the invented SC scheme [PHYLAWS_Patent3], Phylaws proved its feasibility and achieved its performance study. Moreover, the resilience and security analyses performed into the project:

- Showed "quasi-perfect" reliability of secret coded user data at legitimate receiver.
- Confirmed the "quasi-perfect" performance of the SC schemes regarding confidentiality of the user data at any third party's receiver, whatever is its decoding performance.
- Investigated added key-free crypto mechanisms to add authentication and integrity control user data based on self-synchronized chaining protocols and hash functions extending the Carter and Wegman scheme [CARTER]).
- Identified numerous application cases in both Time Division Duplex and Frequency Division Duplex radio networks, either standardized or private for ground, airborne or satellite applications.



a/ Geometry of experiments

- Indoor (Non) Line Of Sight Configuration
- Frequency is 5.2 GHz,
- Wavelength is 5.8 cm
- Position of Alice Bob is 2 m far from Bob
- Position of Eve from Bob is -0.2 cm (near), 50 cm (middle), 5 m (far)

Figure 12: example of experimental configuration of AN-BF and SC on Wi-Fi 2.4 and 5 GHz links

Finally, we can consider that:

- the feasibility proof of the Secrecy Coding is achieved.
- the metrics and performance of the SC schemes are established for realistic radio environments and networks.
- the SC schemes developed and patented by the Phylaws consortium are experimentally proven for pedestrian and indoor geometries.
- these SC schemes are mature for standardization and industrial implementation.

Considering the Non Line of Sight geometry described Figure 12, Figure 13 illustrates some of the experimental results of our SC scheme (built in this case with outer nested polar codes).

Complete illustration about the steps and the performance of the SC scheme over experimental and simulation results can be found in annex 5.

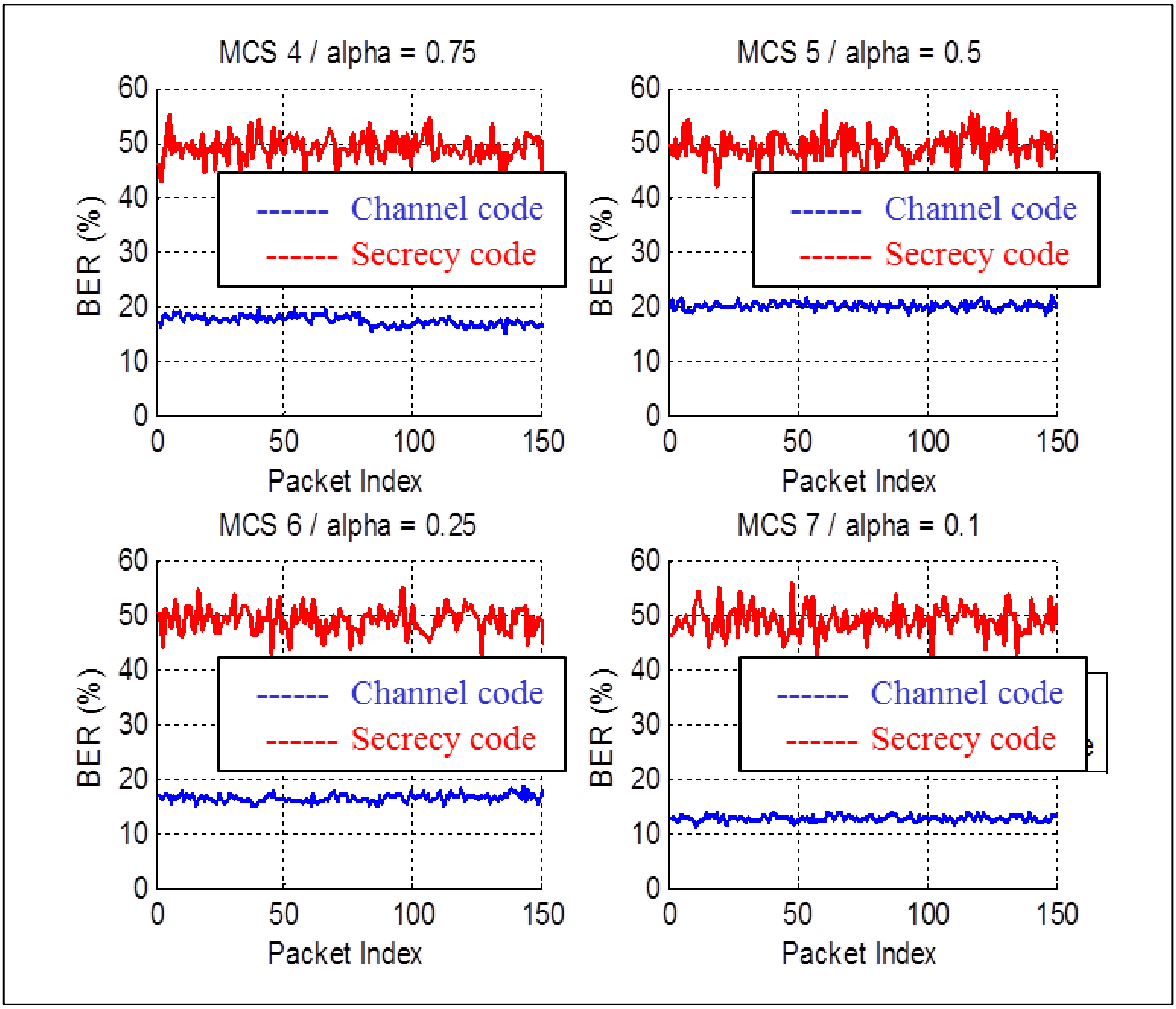
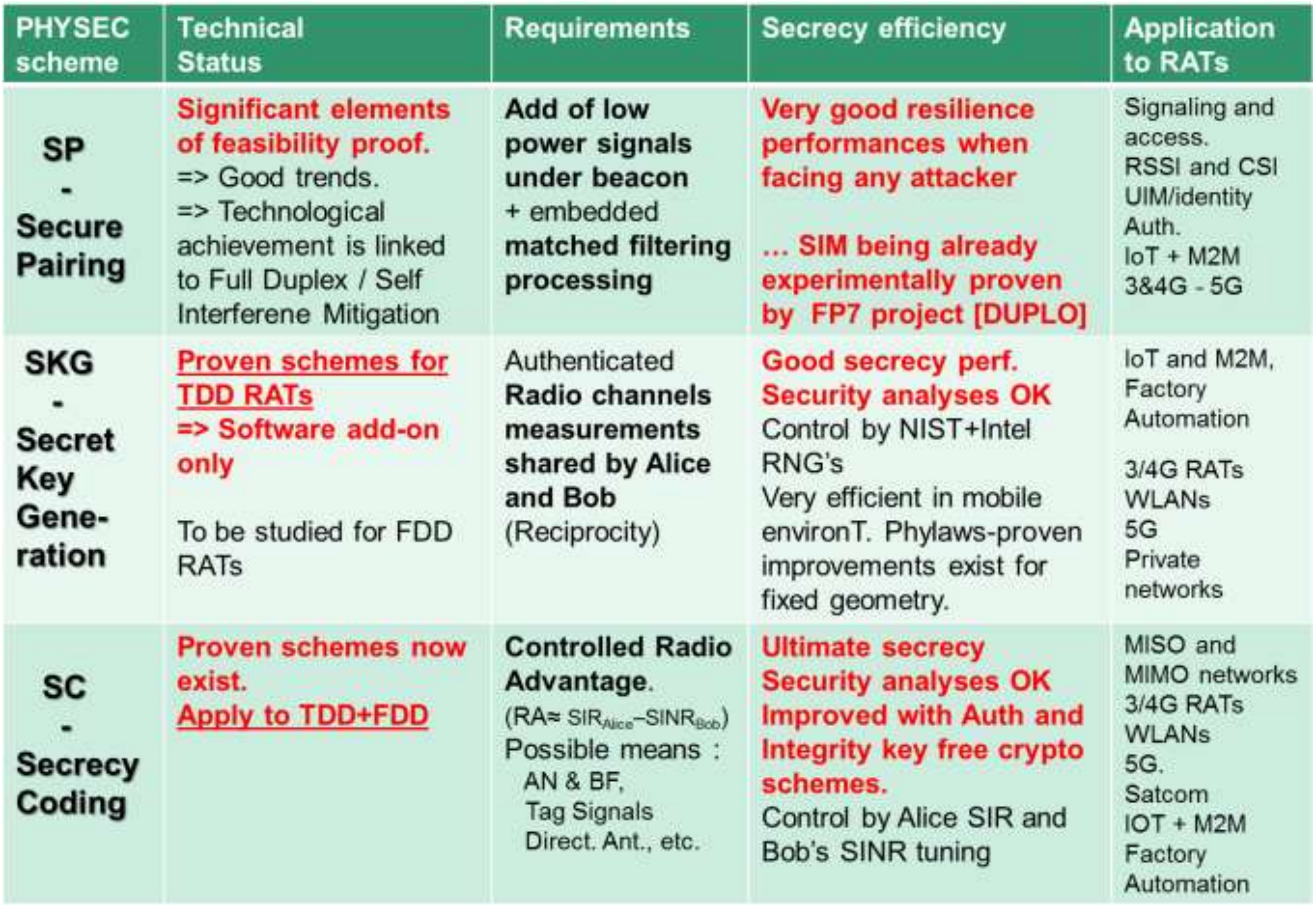


Figure 13: example of experimental BER of channel codes and secrecy codes built with outer nested polar codes applied with AN-BF Wi-Fi 5 GHz links, where Eve is close to Bob and Alice in Non Light of Sight geometry

3- Major impacts of the Phylaws project

3.1- Synthesis of the major scientific and industrial impacts of the Phylaws project

Figure 14 hereafter synthetizes the major scientific and technical achievements of the project relevant to the three patented secured schemes described and illustrated in section 2.



PHYSEC scheme	Technical Status	Requirements	Secrecy efficiency	Application to RATs
SP - Secure Pairing	**Significant elements of feasibility proof.** => Good trends. => Technological achievement is linked to Full Duplex / Self Interferene Mitigation	**Add of low power signals under beacon** + embedded **matched filtering processing**	**Very good resilience performances when facing any attacker** **... SIM being already experimentally proven by FP7 project [DUPLO]**	Signaling and access. RSSI and CSI UIM/identity Auth. IoT + M2M 3&4G - 5G
SKG - Secret Key Gene-ration	**Proven schemes for TDD RATs** **=> Software add-on only** To be studied for FDD RATs	Authenticated **Radio channels measurements shared by Alice and Bob** (Reciprocity)	**Good secrecy perf.** **Security analyses OK** Control by NIST+Intel RNG's Very efficient in mobile environT. Phylaws-proven improvements exist for fixed geometry.	IoT and M2M, Factory Automation 3/4G RATs WLANs 5G Private networks
SC - Secrecy Coding	**Proven schemes now exist.** **Apply to TDD+FDD**	**Controlled Radio Advantage.** (RA≈ SIR_{Alice}–$SINR_{Bob}$) Possible means : AN & BF, Tag Signals Direct. Ant., etc.	**Ultimate secrecy** **Security analyses OK** **Improved with Auth and Integrity key free crypto schemes.** Control by Alice SIR and Bob's SINR tuning	MISO and MIMO networks 3/4G RATs WLANs 5G. Satcom IOT + M2M Factory Automation

Figure 14: synthesis of the major scientific and technical achievements of the Phylaws project

3.2- Significant results of dissemination activities – Web site

Dissemination efforts were very intensive and fruitful during the complete project duration. They were initiated by an initial workshop focusing on academic state of the art of the physical security, hosted by PIMRC 2013, London. They were concluded with a very successful workshop hosted by PIMRC'2016 Valencia Spain, 4th of September 2016, which performed demonstration of the test bed enabling SKG and SC schemes over established Wifi links.

Moreover, dissemination activities produced numerous presentations for conferences, standardization bodies and stakeholders, and also several academic articles and journal papers (especially in the course of the two PhD Thesis supported by the project). Besides, at the end of the project, two journal papers and two book chapters on Phylaws results were submitted and agreed by reviewing committees, which publication will occur during year 2017. Some dissemination efforts will continue after the end of the project and the relevant outputs are/will be available on the project web sites.

The numerous papers and presentations of the Phylaws team that occurred during the project are detailed in the final dissemination report published by the project [PHYLAWS_D1.8].

The public site of the project is reachable at the following URL: http://www.phylaws-ict.org. The publications are available at URL http://www.phylaws-ict.org/?page_id=58.

The partners's dedicated site is reachable at the following URL (identification and password requested) https://e-ecm.online.corp.thales/livelink/livelink.exe/open/tcsehatphylaws/?name=_TCS__e_HAT_Phylaws.

The EC's dedicated site site of the project is reachable at the following URL (identification and password requested):https://e-ecm.online.corp.thales/livelink/livelink.exe?func=ll&objId=1184473&objAction=browse&sort=name.

3.3- Significant results of standardization activities

Strongly supported by dissemination, standardization efforts were very intensive and fruitful during the Phylaws project.

Numerous participations and contributions of the Phylaws team occurred at the 3rd Generation Project Partnership (3GPP):

- Participation to 6 meeting of the security Group (SA3).
- Redaction of 11 contributions proposals for 5G standardization.
- Acceptance of 3 contributions related to Physec based solutions for 5G.

Numerous participations and contributions of the Phylaws team also occurred at International Telecommunication Union (ITU-R), under the authority of the French Frequency Agency:

- Participation to 6 working parties of the 5D group.
- Redaction of at least 6 contributions proposals for further technical reports and recommendation projects.
- Acceptance of at least two contributions, etc.

Besides, several communication initiatives were led towards IEEE, European Defense Agency, Frequency administrations of France, Finland, Germany and towards other regulators.

It is noticeable that the advice and the support of our Advisory Board were very fruitful for the Phylaws project, not only on standardization activities but also on technical development and dissemination strategy.

Finally, despite the inherent politically/diplomatically difficulties of standardization actions, our deep knowledge of security lacks into public Radio Access Technologies and our intensive promotion of Physec-based solutions for enhancing wireless security were successful at the end of the project:

- Phylaws deeply disseminated over stakeholders and regulators (first about security threats, second about advantages, feasibility proof and performance of Physec solutions).
- Several of our contribution proposals were accepted at 3GPP SA3 and ITU WP 5G.
- The Phylaws' approach of the wireless security had finally a significant impact on stakeholders and regulators.

The numerous standardization initiatives of the Phylaws team that occurred during the project are detailed in the final standardization report published by the project [PHYLAWS_D1.11]. The publications relevant to standardization initiatives are available at the URL http://www.phylaws-ict.org/?page_id=58, while annex 6 details the core content of the Phylaws' standardization proposals.

Some standardization effort will continue after the end of the project to ensure the durability of our proposals and the relevant outputs will be uploaded on the project web site.

3.4- Networking – Collaboration with other projects

During the Phylaws project, several contacts with projects such as Duplo [DUPLO], Prophylaxe [PROPHYLAXE] and 5G-Ensure [5G-ENSURE] were very useful. They concerned:

- Technical achievements and orientation of our study and development tasks. For example:
  - Duplo's feasibility proof of Full Duplex radio with self-interference mitigation capabilities directly impacted our design of Tag Signal and Interrogation and Acknowledgement Sequence in the studies and tests of our Secure Paring scheme.
  - Prophylaxe's experimental feasibility proof and test bed about Secret Key Generation with Radio Signal Strength Information (RSSI) directly impacted the design of our SKG scheme based on Channel State Information (CSI) and channel de-correlation pre-processing.

- Synergies and mutual support at standardization bodies (especially at ETSI, at 3GPP and at ITU-R 5G). For example:
  - Phylaws and Prophylaxe performed several common publication (ETSI, EUCNC 2016), organized or contributed to common workshops (panel at the Physec workshop at ICC London 2015, final Phylaws workshop at PIMRC 2016). Phylaws and Prophylaxe also achieved common effort and mutual support at standardization bodies (ITU-R) with the support of their respective national administrations.
  - Phylaws participated to the security workshop organized by 5G-Ensure, provided input data on threats occurring at physical layer and capabilities of Physec to enhance the global security of wireless networks. Both Phylaws and 5G-Ensure supported the standardization effort of the Thales teams at 3GPP, by taken the benefit of the presence of Thales representatives at the numerous meetings organized by 3GPP working groups all over the world.

In the near future:

- it is expected that 5G-Ensure will continue to provide economic scenarios about 5G Security, and long term perspectives for the "carrier" continuation of Phylaws' solutions into 5G standards, as part of a global security solution for 5G networks.
- Share of standardization issues teams towards 3GPP and ITU will continue between 5G-Ensure and Phylaws.

3.5- Patent and IPR strategy of the project

Three patents were written in French (submitted to the French patent office at the end of 2015, examined during year 2016):

- The first one focuses on Secure Pairing [PHYLAWS_Patent1].
- The second one focuses on Secret Key Generation [PHYLAWS_Patent2].
- The third one focuses on Secrecy Coding under radio advantage of Bob to Eve [PHYLAWS_Patent3].

The current status of these three patents is the following:

- Publicity was authorized from March 2016.
- Agreement by the French patent office was achieved end 2016. The official granting should occur at the end of 2017.
- International extensions and IPR issues are under examination by the legal entities of each partner, from an initial IPR repartition and cost evaluation submitted by TCS.

Note: The descriptions of the patents are available on the private part of the Phylaws website. They will be published on the public part (in French) after the official authorisation of the French patent office.

4- Ethical and Lawful issues

4.1- Brief summary of the background

Privacy and citizen right issues are usually associated to projects dealing with communication privacy, because of policies requirements and needs, and because of security items. With regard to the legal security awareness systems and actions (such as prevention of terrorist attacks), four European norms should be considered that comprise two international treaties between the Member States of the Council of Europe and two supranational rules of the European Union and its Member States:

- European Human Rights Convention: Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe of 4 November 1950 (ETS. No.5)
- European Convention on the Automated Processing of Personal Data: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe of 28 January 1981 (ETS No.108)
- European Data Protection Directive: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and the free Movement of such Data
- Charter of Fundamental Rights of the European Union proclaimed by the European Council in Nice on 7 December 2000

European policies direct the adoption of privacy by technical standardisation, market intervention and legal norms. In particular, Article 8 of the European Human Rights Convention, the European Convention on the Automated Processing of Personal Data of the Council of Europe and the Data Protection Directive (95/46/EC) of the European Union all have an impact on polices, legal actions, and security awareness actions by private bodies. For public bodies, although prevention of terrorist attacks security awareness actions need a legal basis of need according to the Human Rights Convention, it is not affected by the European data protection provisions since its regulation remains the realm of national member legislation.

Same considerations apply for awareness of privately operated systems without data storage capabilities (e.g. communication signal recording).

4.2- Practical consequences for the PHYLAWS project – corrective actions

The wide variety of privacy and data-protection legislation across Europe could have impacts on the PHYLAWS project and the future exploitation of its innovative technological outputs.

To avoid any risk regarding privacy issues, the PHYLAWS project and especially its experimental tasks were organized in such a manner that:

- No privacy leakages risks should occur for users of radio-communications networks
- No hard interaction constraints of Phylaws' security solutions with lawful and network engineering considerations should reduce the benefit of the project's outputs for the EC.

Then, at the end of the project and during standardization actions, the Phylaws consortium oriented the developments innovations and standardization proposals to keep as neutral as possible to network engineering of upper protocol layers, to lawful interception systems, to governmental policies and intelligence actions. In practice, the consortium identified three types of ethical considerations related to the project experiments and to the future usages of the innovation created into the project.

We answered to these considerations in the following manner described below.

4.2-1. Privacy and disturbance cautions relevant to experiments

No collection of real subscriber data occurred during the experiments of the project. The data collected were only:

- Broadcasted signalling channels in the 2G/3G/4G/Wifi real field networks, without any subscriber sensitive data. Functionally speaking, what we performed on the radio links is similar to the sensing and measurement stages implemented into terminals themselves.
- Artificial Wifi user signals were simulated and transmitted and recorded over the air: No real Wifi subscriber's signals (neither signalling nor data) have been intercepted. During experiments, the dual sense signals transmission and record were performed by the test bed itself, without any interaction with other Wifi terminal or access point.
- Moreover, in order to avoid confusions risks with real communication in progress in neighbour networks, the transmitted artificial signal were fully identified and controlled by carrier, signal and spectrum shape, modulations characteristics, and finally an artificial message content which included a prior known pattern.

4.2-2. Neutrality of the Physec-based security improvements with respect to lawful interception, policies, legal and intelligence governmental organizations

Our studies and standardization proposal (see D1.11 and a synthesis of the relevant technical arguments in annex 6) highlight that every Physec-based protection proposed by the Phylaws project, has no significant impact on lawful interception at the core network:

- The intrinsic Physec-based protections end as soon as messages are decoded in the node. They thus do not modify higher protocol layer.
- Even at the radio link when needed and relevant, the Physec-based protections can easily be shortcut:
    - with "generated keys" forced to values '0…0' or to values known by policies and intelligence organizations
    - with "generated keys" forced to restricted lengths
    - with "secret codes" limited to inner codes (e.g. existing correction codes without secrecy capabilities).

Note that these important results were expected by the Phylaws team till the start of the project. Indeed, limiting the impact at the physical protocol layer, not to neither lawful interception nor governmental policies nor intelligence actions are requirements more or less necessary for standardization issues.

4.2-3. Innocuousness of the project outputs to legal issues

Ethical and legislative issues concerned by the future use of the PHYLAWS outputs have been explored at the end of the project, in a way that PHYLAWS is expected to strongly upgrade protection of wireless transmission for the citizen at the radio interface. As noted above, our innovations avoid the main "collision risk" with governmental actions on public networks because:

- Our protections operate a the physical layer only risk, and can be easily shortcut if required
- When lawful communication interceptions are needed and relevant, polices, judiciary and intelligence administrations operate mainly at core network.

Finally, PHYLAWS (and future researches relevant to Physec) should not impact legislation, while the secrecy extracted at the physical layer is not propagated into higher level protocol layers

5- Conclusion of the Phylaws project

Coming back to the preliminary studies (WP2), academic works (WP3), developments (WP4) and considering the outputs of experiments (WP5) and simulation (WP6), it appears that Phylaws achieved the major results listed below.

5.1- Scientific achievements

- Phylaws studied the randomness properties of the radio channel and experimentally proved its richness, reliability and reciprocity. In addition, the radio channel randomness showed good privacy properties thanks to the spatial and frequency diversity of the propagation over the air. Even in very stationary environments (indoor, empty, fixed Line of Sight geometry), the channel randomness richness is enough to provide instances with sufficient entropy and spatial de-correlation.
- Phylaws explored several implantations of Physec-based security concepts and proved with suitable metrics that these schemes were valid and efficient for enhancing the citizen privacy and confidentiality in slight-mobility radio environments. In addition, it appears that Physec solutions are compatible:
  - With added key-free crypto schemes that enhance authentication and integrity control.
  - With the usage of conventional crypto schemes (with prior key share/computation) that enhance confidentiality, when needed by the communication service.
- Phylaws proved the feasibility of the SKG and SC schemes in 4G radio-environments (simulation of realistic LTE links) and in WLAN radio-environments (experiments with Wifi established links with processing embedded into commercial devices). In addition the security analysis was performed with real field records and assessed the performance with suitable metrics based on mutual entropies and mutual information estimators applied to massively recorded data.

5.2- Implementation perspectives in future radio networks

- Phylaws patented three secure schemes based on Physec: one dedicated to Secure Pairing, one dedicated to Secret Key Generation and one dedicated to Secrecy Coding.
- Through suitable metrics and thanks to numerous experiments and simulations, Phylaws proved that the privacy and secrecy provided by the patented Physec schemes above are very significant in real wireless public networks, with real environment constraints (outdoor and indoor, pedestrian mobile or fixed geometry, crowed of empty, Line Of Sight and Non Line of Sight, etc.), and when facing any kind of attacker operating at the physical layer.
- Phylaws proved that the implementations of the Physec schemes developed during the project are quite easy and very efficient in existing radio devices, with a very limited processing complexity.
- Finally, Phylaws highlighted that Physec-based protections, being dedicated to the radio interface, will have a limited impact on standardization effort and no significant impact neither on lawful interception at the core network.

5.3- Benefits to future radio networks and European citizen

- Phylaws has largely disseminated towards the scientific community, the stakeholders and the administrations dealing with radio communications. The project has also significantly contributed to future 5G standards thanks to several 3GPP-agreed and ITU-agreed contributions.
- Ultimately, Phylaws has strongly contributed to the future penetration of wireless technologies in the personal and professional sphere, by providing the means for a safer access to the digital world. The achievements of the project should thus impact the evolution of standardization and contribute to trustworthy ICT in the following years.

Annex 1 - Glossary

Term	Definition
2/3/4/5G	Second/Third/Fourth/Fifth Generation (of radio networks)
3GPP	Third Generation Partnership Project (main instance for 2/3/4/5 G network standardization)
AN-BF	Artificial Noise – Beam Forming
AP	Access Point
CFR	Channel Frequency Response (of the radio-propagation filter). CFR = FFT(CIR).
CIR	Channel Impulse Response (of the radio-propagation filter). CIR = FFT^{-1}(CFR) – provided by single sense radio channel estimation
COMSEC	Communication Security: is relevant to the protection of the content of user messages (voice, data). COMSEC applies either at the radio interface or at upper layer. COMSEC techniques involve ciphering, authentication and integrity control of signalling and user data at several protocol layers and interfaces (examples are point to point ciphering of each data flux, ciphering of IP packets, ciphering of artery, etc.).
CSI	Channel State Information – provided by dual sense radio channel estimation magnitude and phase and channel restoration capabilities (with calibration, post computing etc.) when needed.
FDD	Frequency Division Duplexing (communicating devices operate in different carrier frequencies)
FFT FFT^{-1}	Fast Fourier Transform Inverse of the Fast Fourier Transform
IAS	Interrogation and Acknowledgment Sequences: radio protocol derived from concepts of Identification Friend or Foe Radio systems. IAS are performed by exchanging Tag Signals between legitimate transmitters and receivers, and achieve security pairing and secured estimation of radio channels.
IJ	Intelligent Jammer: Eavesdropping and jamming (protocol aware) system that jams dedicated part of the legitimate radio protocol (such as channel probes used for CSI for example).
ITU	International telecommunication Union (Main standardization body for radio spectrum regulation and usage).
LOS, NLOS	Line Of Sight Non Line Of Sight
MIMO	Multiple Input Multiple Output.
MITM	Man-in-the-Middle: Eavesdropping and spoofing system that intercepts and modifies messages within the legitimate protocol in real time.
NETSEC	Network Transmission Security: NETSEC is relevant to the protection of the signalling of the network. NETSEC applies mainly at the radio interface and at the medium access protocol layer, with request to upper protocol layers. NETSEC techniques involve mainly transmitter authentication protocols, integrity control and ciphering of signalling data.
PHYLAWS	Acronym of the ICT-FP7 Granted project whose complete name is PHYsical LAyer Wireless Security Grant Agreement number: 317562
PHYSEC	Physical Layer Security is a generic term that will be used in this project to design all kind of protection techniques that are based on the use of the physical layer sensing and/or measurement.
RA	Radio Advantage (of legitimate receiver versus attacker receiver)
RAT	Radio Access Technology (e.g. FDMA, TDMA, CDMA, CSMA, OFDM, Full Duplex, SISO, SIMO, MISO, MIMO, etc.)
RSSI	Radio Signal Strength Information – provided by dual sense radio channel magnitude estimation and channel restoration capabilities (with calibration, post computing etc.) when needed.
SC	Secrecy Coding: coding schemes ensuring low or null information leakages towards any eavesdropper location while enabling a controlled BER data transmission towards legitimate receiver. Subject of a patent deposit during the Phylaws project [PHYLAWS_patent3]
SINR	Signal to Interference + Noise Ratio

SKG	Secret Key Generation: quantification, reconciliation and amplification schemes generating secret keys from shared radio channel estimations. Subject of a patent deposit during the Phylaws project [PHYLAWS_patent2]
SNR	Signal to Noise Ratio
SP	Secure pairing: secured association of legitimate Nodes and terminal with Tag Signals into Interrogation and Acknowledgement Sequences, build from on-going shared radio channel estimations in the same manner of a key-free Identification Friend of Foe system. Subject of a patent deposit during the Phylaws project [PHYLAWS_patent1]
TDD	Time Division Duplexing
TRANSEC	Transmission Security: TRANSEC is relevant to the protection of the waveform face to interception/direction finding of the transmitted radio signal, to jamming of the user receiver, and to intrusion attempts into the radio-communication access protocol. It applies mainly at the radio interface.
TS	Tag Signal: Low power signal, which can be transmitted in a self-interfered scheme, at the same time (same frame or slot) and at the same carrier than the user signal (such as in Full Duplex RATs). They are used in IAS to securely pair transmitter and receiver and support accurate and authenticated channel estimations.
TSR	Tag Signal Ratio: Level of intentional Self-Interference applied to the Tag Signals (level of radio protection of the Tag Signal).
Tx Rx	Transmitter Receiver.
WLAN	Wireless Local Access Network (includes Wifi Standards)

Annex 2 - References list of the Phylaws project

A2.1- Web Site

[PHYLAWS_WS] Phylaws Web site: www.phylaws-ict.org

A2.2- PhD Thesis

[PHYLAWS_PhDTM] PhD dissertation of Mrs Taghrid Mazloum held in Telecom Paris Tech, Paris 12 February 2016.

[PHYLAWS_PhDHM] PhD dissertation of Mr Hamed Mirghasemi held in Telecom Paris Tech, Paris 10 October 2014.

A2.3- Patents

[PHYLAWS_Patent1] Patent submitted to French office « Procédé d'association univalente et univoque entre émetteurs et récepteurs de transmission a partir du canal de propagation», Thales, Teknologian Tutkimuskeskus VTT, Date 29/12/2015, Number 1502713. The official references of the existing deposit (French patent bureau for now) are the following:

Deposit number	1502713
Date of deposit	29 décembre 2015
Official title (French)	PROCEDE D'ASSOCIATION UNIVALENTE ET UNIVOQUE ENTRE EMETTEURS ET RECEPTEURS DE TRANSMISSION A PARTIR DU CANAL DE PROPAGATION
Inventors	François DELAVEAU, Renaud MOLIERE, Christiane KAMENI NGASSA, Claude LEMENAGER, Adrian KOTELBA, Jani SUOMALAINEN
Companies	THALES, TEKNOLOGIAN TUTKIMUSKESKUS VTT

[PHYLAWS_Patent2] Patent submitted to French office « Procédé d'extraction univalente et univoque de clés a partir du canal de propagation », Thales, Telecom ParisTech, Celeno Communication Ltd, Date 29/12/2015, Number 1502712. The official references of the existing deposit (French patent bureau for now) are the following:

Deposit number	1502712
Date of deposit	29 décembre 2015
Official title (French)	PROCEDE D'EXTRACTION UNIVALENTE ET UNIVOQUE DE CLES A PARTIR DU CANAL DE PROPAGATION
Inventors	Renaud MOLIERE, Christiane KAMENI NGASSA, François DELAVEAU, Claude LEMENAGER, Alain SIBILLE, Taghrid MAZLOUM, Nir SHAPIRA
Companies	THALES, TELECOM ParisTech, CELENO COMMUNICATION LTD

[PHYLAWS_Patent3] Patent submitted to French office « Procédé de codage univoque et secret de transmission sur un canal de propagation à avantage de capacité», Thales, Telecom ParisTech, Imperial College Of Science, Technology And Medicine, Date 29/12/2015, Number 1502710. The official references of the existing deposit (French patent bureau for now) are the following:

Deposit number	1502710
Date of deposit	29 décembre 2015
Official title (French)	PROCEDE DE CODAGE UNIVOQUE ET SECRET DE TRANSMISSION SUR UN CANAL DE PROPAGATION A AVANTAGE DE CAPACITE
Inventors	Christiane KAMENI NGASSA, François DELAVEAU, Jean-Claude BELFIORE, Cong LING
Companies	THALES, TELECOM PARIS TECH, IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

A2.4- Dissemination, Standardization and Advisory Board

[PHYLAWS_D.1.5] Project synthesis report – version V1.0 date 2017-1-30 – present document.

[PHYLAWS_D.1.6] PHYLAWS Dissemination plan Report – version V1 date 2013-01-31.

[PHYLAWS_D.1.7] PHYLAWS Dissemination intermediate Report – version V1 date 2015-05-12

[PHYLAWS_D1.8] PHYLAWS Dissemination final report – version 1.0 date 2016-10-31.

[PHYLAWS_D.1.9] PHYLAWS Standardization plan Report – version V1 date 2013-01-31.

[PHYLAWS_D.1.10] PHYLAWS Standardization intermediate Report – version V1 date 2015-05-30

[PHYLAWS_D.1.11] PHYLAWS Standardization final report – version 1 date 2016-10-31.

[PHYLAWS_D.1.12_AB] PHYLAWS Advisory Board Meeting report – version V1 date 2013-11-08.

[PHYLAWS_D.1.13_AB] PHYLAWS Advisory Board Meeting report – version V1 date 2016-02-14.

[PHYLAWS_D1.14] PHYLAWS Advisory Board final report – version date 2016-10-31.

A2.5- Technical deliverables

[PHYLAWS_D.2.1] PHYLAWS Study report "*Privacy threats for the radio interface of public wireless networks*"– revised version 2.0 date 2015-12-28.

[PHYLAWS_D.2.2] PHYLAWS Study report "*Secure architectures and protocols for privacy enhancement of radio terminals*" – version V1.0 date 2013-09-23.

[PHYLAWS_D.2.3] PHYLAWS Study report "*State of the art of physical layer security*" – version V1.1 date 2013-11-14.

[PHYLAWS_D.2.4] PHYLAWS Study report "*New opportunities provided by modern wave forms new security protocols and sensing of radio environments*" – revised version V3.0 date 2015-11-30.

[PHYLAWS_D.3.1] PHYLAWS Study report "*Channel based random generators – interm. report*" – version V1.0 date 2014-03-10.

[PHYLAWS_D.3.2] PHYLAWS Study report “*Channel based random generators – final report*” – version V2.1 date 2015-11-30.

[PHYLAWS_D.3.3] PHYLAWS Study report “*Coding techniques and algorithms for secrecy coding and secret key generation*” – version V2.0 date 2015-11-05.

[PHYLAWS_D3.4] PHYLAWS Study report “*CIR measurements and modeling in ISM 2,4 GHz band & 5 GHz band*” – version V1.0 date 2016-03-30 - version V2.0 date 2016-11-21.

[PHYLAWS_D3.5] PHYLAWS Study report “*Simulations report of PHYSEC methods using measured CIR*” – version V1.0 date 2016-12-04.

[PHYLAWS_D.4.1] PHYLAWS Study report “*TRANSEC upgrades of existing RATs - study report*” – revised version V2.0 date 2015-12-30.

[PHYLAWS_D.4.2] PHYLAWS Study report *“TRANSEC upgrades of existing RATs - simulation and analyses complements”* – version V1.0 date 2015-11-30.

[PHYLAWS_D.4.3] PHYLAWS Study report “*NETSEC upgrades of existing RATs - study report*” – version V1.0 date 2015-11-30.

[PHYLAWS_D4.4] PHYLAWS Study report “*NETSEC upgrades of existing RATs - simulation analyses complements*” – version V1.0 date 2016-08-30.

[PHYLAWS_D.4.5] PHYLAWS Study report “*New RATs and waveforms taking benefit of Physec upgrades – interim report*” – version V1.0 date 2016-10-17.

[PHYLAWS_D.4.6] PHYLAWS Study report “*New RATs and waveforms taking benefit of Physec upgrades – Final report*” – version V1.1 date 2016-11-18.

[PHYLAWS_D.5.1] PHYLAWS Study report “WiFi test bed setup development report” – version V1.0 - date 2016-03-20, version V1.1 - date 2016-04-22

[PHYLAWS_D.5.2] PHYLAWS Study report “Experiment campaign plan” – draft version V1.α - date 2016-03-24” – final version V1.0 - date 2016-04-22.

[PHYLAWS_D.5.3] PHYLAWS Study report “Intermediate Report on WiFi interceptor experiments with the test bed” – draft version V1.α – 29 / 03 / 2016 - final version V1.0 - date 2016-12-10.

[PHYLAWS_D.5.4] PHYLAWS Study *"WiFi Testbed - Final Report on WiFi Interceptor Experiments with the Testbed”* – version V1.0 - to be published

[PHYLAWS_D.5.5] PHYLAWS Study report *"Concluding report on experimental support for standardization proposals for WiFi PHYSEC upgrades”* – version V1.0 - to be published

[PHYLAWS_D.6.1] PHYLAWS Study report “*Modelling of LTE-based cellular system*” – revised version V2 date 2016-02-26.

[PHYLAWS_D.6.2] PHYLAWS Study report “Simulation of interception of waveform signals in LTE-based cellular system” – version V1 Version date 2016-05-12.

[PHYLAWS_D6.3] PHYLAWS Study report "LTE-based cellular system simulations - Concluding report including simulation results and proposals for standardization”, version V1.0 date 2016-09-30.

A2.6- Extra references

[BLOCH]: M. Bloch and J. Barros, Physical-Layer Security, Cambridge University Press, 2011.

[WALLACE]: J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO Wireless channels: measurement and analysis," IEEE Transactions on information forensics and security, vol. 5, no. 3, pp. 381-392, September 2010.

[ARIKAN]: E. Arikan, «Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels,» Information Theory, IEEE Transactions on , vol. 55, n° %17, pp. 3051-3073, 2009.

[MAHDAVIFAR]: H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," IEEE Transactions on Information Theory, vol. 57, no. 10, pp. 6428-6443, 2011.

[3GPP1]: 3GPP, Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation, 2015.

[3GPP2]: 3GPP, «3G Security: Security Architecture - release 8 ; System architecture evolution - release 8,» n° %13GPP TS 33.102 V8.0.0 ; 3GPP TS 33.401 V8.1.1, June 2008 ; October 2008.

[FUDU] : Z. Zhang, K. Long et L. Hanzo, «Full-Duplex wireless communications: Challenges, solutions and future research directions,» Proceedings of the IEEE, to appear.

[INTEL]: M. Hamburg, P. Kocher and M. E. Marson, "Analysis of Intel's Ivy Bridge Digital Random Number Generator," 2012.

[NIST] National Institute of Standards and Technology, «Recommendation for the Entropy Sources Used forRandom Bit Generation,» 2016.

[QUADRIGA] S. Jaeckel, L. Raschkowski, K. Brner et a. L. Thiele, «Quadriga: A 3-d multicell channel model with time evolution for enabling virtual field trials,» IEEE Trans. Antennas Propag, vol. 62, p. 3242–3256, 2014.

[VIENNA] C. Mehlfuehrer, J. C. Ikuno, M. Simko, S. S, M. Wrulich et a. M. Rupp, «The vienna lte simulators - enabling reproducibility in wireless communications research,» EURASIP Journal on Advances in Signal Processing, vol. 21, 2011.
[TALVARDY]: Tal et A. Vardy, «List Decoding of Polar Codes,» Information Theory, IEEE Transactions on, vol. 61, n° %15, pp. 2213-2226, 2015.

[BALATSOUKAS]: A. Balatsoukas-Stimming, M. B. Pariz et A. Burg, «LLR-Based Successive Cancellation List Decoding of Polar Codes,» IEEE Transactions on Signal Processing, vol. 63, n° %119, pp. 5165-5179, 2015.

[DUPLO]: "Full-Duplex Radios For Local Access" Grant number CNECT-ICT-316369 http://www.fp7-duplo.eu/

[PROPHYLAXE]: "Providing Physical Layer Security for the Internet of Things", funded by BMBF GN 16KIS0005K, http://www.ict-prophylaxe.de

[5G-ENSURE]: "5g enablers for network and system security and resilience", funded H2020 under grant agreement No 671562, http://www.5gensure.eu/

[ZOU] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, « Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends », Proceedings of the IEEE, Vol. 104, No. 9, September 2016.

[CARTER]: Carter, J. L., Wegman, M. N. (1979). Universal classes of hash functions. Journal of Computer and System Sciences, 143-154.

Annex 3 - Synthetic description of the deliverables

A3.1- Introduction

The table below give the list and a short description of the content of the deliverables written in the Phylaws project. All these deliverables are reachable at the project 's Web site http://www.phylaws-ict.org/?page_id=48.

A3.2- Management work package 1 – Task T1.2 – Dissemination

Delive rable	Date	*"Title"* Summary of the content
D1.6	Period 1 V1 2013-01-31	"PHYLAWS Dissemination Plan". D1.6 includes the planned dissemination actions over the complete project duration
D1.7	Period 2 V1 2015-05-12	"PHYLAWS Dissemination intermediate Report" D1.8 reviews all dissemination actions of periods 1 and 2 of the project. Updates the planned dissemination actions over the end of period 2 and over period 3, especially linked to standardization actions
D1.8	Period 3 V1: 2016-10-31	*"PHYLAWS Dissemination final report"* D1.8 reviews all dissemination actions of periods 1, 2 and 3 of the project, with a special focus on the final WS hosted by PIMRC'2016 held in Valencia Spain 4 September 2016 and provides explanations about the overall significant impact of this (very) successful task of the PHYLAWS project.

A3.3- Management work package 1 – Task T1.3 - Standardization

Delive rable	Date	*"Title"* Summary of the content
D1.9	Period 1 V1 2013-01-31	"PHYLAWS Standardization Plan". D1.9 includes the possible standardization actions considered during the complete project duration
D1.10	Period 2 V1 2015-05-30	"PHYLAWS Standardization intermediate Report" D1.10 reviews the first standardization initiatives held at the end of the period 2 of the project (when first experimental results and elements of feasibility were available) Updates the pertinent standardization actions (by following advices of our advisory board) ant he best standardization bodies to be targeted during period 3.
D1.11	Period 3 V1 2016-10-31.	"PHYLAWS Standardization final report" D1.11 reviews the all standardization initiatives and results held during period 2 and 3 of the project and provide explanations about the overall significant impact of this successful task of the PHYLAWS project.

A3.4- Management work package 1 – Task T1.4 - Advisory board

Deliverable	Date	*"Title"* Summary of the content
D1.12	Period 1 V1 2013-11-08	"PHYLAWS Advisory Board Meeting report". D1.12 includes the minutes of the first AB Meeting and details how the Phylaws consortium intend to exploit and apply the advices and recommendation of AB members
D1.13	Period 3 V1 2016-02-14.	"PHYLAWS Advisory Board Meeting Report" D1.13 includes the minutes of the second AB Meeting and details how the Phylaws consortium intend to exploit and apply the advices and recommendation of AB members
D1.14	Period 3 V1 2016-10-31.	"PHYLAWS Advisory Board final report" D1.14 syntheses the outputs of the two AB Meetings and details how the Phylaws consortium has exploited and applied the advices and recommendations of AB members

A3.5- Technical work package 2 – State of The Art

Deliverable	Date	"Title" Summary of the content
D2.1	Period 1 -> 3 V2: 2015-12-30	"Privacy threats for the radio interface of public wireless networks". This report surveys security threats occurring to the physical layer of wireless standards and existing solutions for enhancing security (authentication, subscriber privacy and data confidentiality).
D2.2	Period 1 V1: 2013-09-23	"Secure architectures and protocols for privacy enhancement of radio terminals" This report surveys security architectures of radio devices and systems in the scope of existing and emerging public wireless standards. It achieves a wide overview of security solutions and the relevant hardware and software architectures, as well as on the possibilities of embedding physical security concepts (Physec) in terminals and in communications nodes.
D2.3	Period 1 V1: 2013-11-14	"State of the art of physical layer security" This report surveys advances in physical security and relevant application perspectives in public wireless networks. It introduces several notions related to information theory, points out the main Physec concepts, discusses their theoretic advantages and the current development. Finally, it highlights practical implementation perspectives of Physec in existing and future public radio-networks, as stand-alone added modules operating or as added algorithm combined with classical solutions in order to upgrade and/or to simplify existing security procedures.
D2.4	Period 2 -> 3	"New opportunities provided by modern waveforms, new security protocols and sensing of radio environments"

	V3: 2015-11-30	This report surveys opportunities for Physec-based security improvements in wireless standards by exploiting, in the scope of existing and emerging public wireless standards: • versatile radio access protocols including Uncoordinated Spread Spectrum (USS) schemes for the first access stages, • cognitive and opportunist RATs, such as RATs dedicated to spectrum white space, that includes advanced processes such as Self-Network Organization and advanced front end processing such as spectrum sensing, CIR measurement, adaptive equalization. • antenna processing, MISO and MIMO RATs, relevant modulations and space time coding schemes, • PCMA and Full Duplex technologies, including self-interference mitigation techniques, • advanced RATs of Identification of Friend or Foe, Starting from the key items (previously identified in D2.2 and D2.3) the report deepens: • How to provide a radio advantage to the legitimate links when facing eavesdropper threats, and especially during the earliest negotiations phase (recalling that in most situations, a radio advantage is a necessary condition for applying Physec-based security solutions)? • Considering that the radio advantage is established for legitimate users, how to consolidate it for a better security of the RATs, firstly during the negotiation protocol (security pairing, authentication, etc.), then in the messages exchanges, when facing passive, IJ and MITM threats This report finally highlights and studies key items that will be developed in WP3 WP4 experiments, in WP5 and simulated in WP6 such as Artificial Noise (AN), Tag Signals (TS) and Interrogation and Acknowledgement Sequences (IAS).

A3.6- Technical Work Package 3 - Radio-channel aspects of Physical layer Security

Deliverable	Date	"Title" Summary of the content
D3.1	V1: 2014-03-10	"Channel based random generators: interim report" This report studies the fundamental role of noisy fading radio channels in security. It analyzes how much secrecy we can extract from channel randomness in the form of a secret key. Specifically, it assumes that the legitimate parties and the eavesdropper observe the realizations of correlated random variables and that the legitimate parties attempt to agree on a secret-key unknown to the eavesdropper. Thus, the relevant metric in SKG involves the number of secret-key bits distilled per observation of the correlated random variables and the quality of the keys (NIST criteria for example). In SC, the natural metric is the number of message bits that could be transmitted securely and reliably per channel use, what is included in the flatness factor. First, standard models are introduced for secret-key agreement. Second, their fundamental limits are discussed. Then, specific types of key generation methods based on wiretap codes are studied in detail: Wyner-Ziv codes, lattices and sequential key distillation strategies. Also, the report highlights practical Implementation perspectives of the key-agreement schemes in existing and future public radio-networks, as stand-alone added modules operating at the physical player, or as added algorithm combined with classical solutions in order to upgrade and/or to simplify existing security procedures. The following of the document concentrates on SKG from channel randomness: • State of the art and analysis • Investigation of a preliminary channel model about the meaning of secrecy in this context and about the effectiveness of obtaining "good quality" keys with enough secure bits, depending on the nature of the environment and the distance between Bob and Eve Methodology to perform channel measurements or channel simulations in Phylaws: The last part is a first attempt into this direction, by starting from the well-known "Clarke" multipath discrete channel model for spatially stationary channels with a goal to generalize it towards the case of moderate non-stationary.

D3.2	V1: 2015-11-30	“Channel based random generators: final report”. This deliverable concludes task T3.1 on channels and SKG, with outputs intended to impact downstream work in work packages WP4, WP5 and WP6. It deals with • Evaluation of the performance of the SKG schemes, with a specific focus on the description of suitable metrics. • Modeling of non-stationary statistical channel with random distribution of scatterers, by introducing time varying shadow fading effects, then focusing on the improved performance of SKG schemes in this more realistic propagation. • Physical interpretation of performance of extracted secret keys, from a simplified variant of dispersive channel model. • Radio channel modeling by ray-tracing, carried out in a few environments inside and close to Paris city (France). Radio channel measurements performed through several indoor and outdoor/indoor campaigns and on their first exploitation as input to SKG schemes.
D3.3	V1: 2015-11-05	“Coding techniques and algorithms for secrecy coding and secret key generation”. This deliverable first introduces several notions relevant to information theory and the main principle that are relevant to wiretap coding at the physical layer. From a state of the current researches, several wiretap coding solutions are highlighted, especially • the wiretap coding scheme for discrete channels, based on the famous LDPC codes and the recently proposed polar codes. • extension of the coset wiretap coding scheme to continuous Gaussian channels, by constructing polar lattices Secondly, The deliverable deals with practical implantation perspectives of secret key generation in existing and future radio-networks (secret key generation from Gaussian source, using the lattice hashing technique), as stand-alone added modules operating at the physical player, or as added algorithm combined with classical solutions such as TRANSEC, NETSEC and COMSEC protections. It highlights the major channel issues regarding SKG and routes towards the development of channel models and the way to conduct channel measurements or channel simulations suited to the PHYLAWS needs for SKG.
D3.4	Partial version V1: 2016-03-30 V2 2016-11-21	“CIR measurements and modeling in ISM 2,4 GHz band & 5 GHz band”. The final version of deliverable D3.4 provides • completed details about material and processing into the Wifi measurement campaign at 2.4 and 5 GHz, including calibration issues encountered and partially solved by partner CEL • completed measurement results for dual sense CSI under 5GHz and 2.4 GHz wifi carriers • completed analyses of wifi radio channels issues for an usage in Physec-based secure schemes • numerous illustrations of calibration issues • numerous illustrations of CSI measurements
D3.5	V1.0 2016-11-30	“Simulations report of PHYSEC methods using measured CIR”” Deliverable D3.5 performs • massive usage of CSI measurements provided by D3.4 for SKG processing, for join entropy estimations, for mutual information estimations • numerous illustrations of SKG results. • complete analyses of the channel randomness properties and their usage for SKG • few exploitations and analyses of the measurements in simplified simulations of Secure Pairing with Tag Signals (modeling and simulation of a complete Interrogation and Acknowledgement Sequence).

A3.7- Technical Work Package 4 - Introducing radio-channel randomness into existing and future RATs

Deliverable	Date	"Title" Summary of the content
D4.1	V1: 2015-06-12 V2: 2015-12-30	"TRANSEC upgrades of existing RATs – study report". This report first provides attacker models for many kind of threats including passive eavesdropper, Intelligent Jammer and Man in the Middle, and surveys then opportunities for Transec (Transmission Security) improvements in existing public wireless standards by exploiting channel randomness when facing such threats. D4.1. focusses on the combination of several radio technologies such as: • Spread Spectrum modulated radio signals (and especially Direct Spread Spectrum Sequences) • Uncoordinated Spread Spectrum and Time Jitter schemes • Concepts derived from radio systems designed for Identification Friend or Foe (IFF) • Full-Duplex technologies and self-interference mitigation techniques • Artificial Noise Starting from the work performed over WP2, looking into works performed in the FP7 projects (such as Duplo for example) and in numerous references, it deeply studies the new radio protocol proposed in D2.4 for early secure pairing of radio devices at the earliest stages of the RATs. This new radio protocol is RAT independent. It is based on self-interfered furtive and adaptive radio signals, called Tag Signals (TS), which support dedicated Interrogation and Acknowledgement Sequences (IAS). These TS and IAS provide a controlled radio advantage for Alice and Bob, enabling simultaneously secure pairing and authenticated estimation of CIR. The reports details why this early secure pairing of Alice and Bob based on TS and IAS is expected to be resilient against any kind of threats (passive, Intelligent Jammer and Man-In-The-Middle). In addition to the authenticated estimation of CIR, it should enable secured Channel State Information (CSI) and the enabling of several further Physec-based protections from CIR and CSI, such as Establishment of Artificial Noise, Secret Key Generation, and even computation of Secrecy Codes, thanks to the radio advantage provided by TS. Precise application cases are deepened for WiFi links, a precise description of the complete IAS protocol is given, an accurate study of the radio constraints is performed and the report provides a deep analysis of CIR estimation based on TS under WiFi carriers. This report is completed by the deliverable D4.2 with extra simulations and analyses.
D4.2	V1: 2015-11-30	"TRANSEC upgrades of existing RATs –analyses and simulation complements". Completing deliverable D4.1, the results of this deliverable strengthen the proof of concept of Tag Signals and Interrogation and Acknowledgement Sequences with additional simulations and experiments. In addition, we propose a schemes for building large sets of Tags Signals, we complete the analyses of resilience of the scheme and we definitely conclude on the "tremendous" perspectives of the proposed TS and IAS schemes concerning: • Enhanced Secure Pairing of devices and most accurate CSI measurements for initiating artificial noise, beam forming, SKG and SC. • SINR measurement for controlling the radio advantage directly provided by Tag Signals or by other methods (such as Artificial Noise and Beam Forming) and support further users' attach, identity authentication, cipher key negotiation.
D4.3	V1: 2015-11-30	"NETSEC upgrades of existing RATs – Study report". This deliverable surveys opportunities for Netsec (Network Security) improvements in existing public wireless standards by exploiting channel randomness. It focuses mainly on the following items: • New developments relevant to the complete "pre-industrial" implementation of the patented Secret Key Generation scheme (SKG) based on full CSI.

		• An innovative implantation scheme of Secrecy Coding (SC), invented and studied and patented by the Phylaws team. Even if it may be suboptimal regarding the secrecy capacity, this new scheme allows a practical implementation within node and terminal by using well-known coding components of limited complexity. • Advanced attackers capabilities (wormhole attacks), on authentication issues, as well as cellular network (LTE) security architectures. • First analyses of radio resilience capabilities provided by SKG and SC when facing such attacks. • Possible interaction of SKG and SC and classical asymmetric and symmetric ciphering schemes (e.g. how physical-layer security approaches and classical crypto-based security mechanisms can complement each other).
D4.4	V1: 2016-08-30	“NETSEC upgrades of existing RATs - simulation analyses complements”. This deliverable completes D4.3 with the latest results and optimization issues of our patented Physec-based secure schemes (SKG and SC). After introducing the context, recalling terminology and main notions and concepts relevant to Physec, then recalling the attacker models the complete implementation of a Secret Key Generation scheme (SKG) based on full Channel State Information (CSI), the deliverable provides • entropy analysis of the communication channel, • new randomness test to evaluate the quality of secret keys, • new simulation results for LTE signals and CSIs • new experimental results from dual sense measured WiFi CSI. This deliverable also provides first analyses of the security upgrades provided by SKG schemes to future generation Radio Access Technologies, in a standardization perspective. Then this deliverable • recalls the secrecy coding scheme developed by the Phylaws team • proposes a new decoding algorithm issued from PPR3 discussion with reviewers) which leads to better performance • designs also new Secrecy Codes • provides new results from LTE simulated signals and from measures under WiFi carriers. This deliverable also provides first analyses of the security upgrades provided by SC schemes to future generation Radio Access Technologies, still in a standardization perspective.
D4.5	V2: 2016-10-17	“New RATs and waveforms taking benefit of Physec upgrades – interim report”. This deliverable includes the resilience analyses and the security analyses of our patented physec-based secure schemes when facing nominal threats. After recalling some basics for a better understanding of the content of our innovative security schemes plus the available elements of feasibility proof, it defines nominal threats (both passive and active). Then it presents the results of the resilience analyses of the security schemes, including • Radio considerations; resilience analysis, proposals for optimized implementation of the SKG SC and SP schemes into existing and future RATs. • Security analyses; crypto analyses, elements towards a security proof of the SKG and SC schemes. Enhancement proposals of the SC scheme are proposed in order to provide authentication and integrity control in addition to secrecy of messages.
D4.6	V2: 2016-11-18	“New RATs and waveforms taking benefit of Physec upgrades – Final report”. This deliverable completes D4.5 in two senses: D4.6 performs the resilience analyses and the security analyses of our patented Physec-based secure schemes when facing ultimate threats. After defining ultimate threats (both passive Huygens Fresnel Green Attack and active light–speed WormHole Attack), it presents the limits of the security schemes based on Physec, and several tracks to recover some resilience with the help of crypto techniques. • D4.6 synthetizes the resilience analyses led over WP4 when facing both nominal and ultimate attackers, proposes and analyses optimal combinations of secure schemes that were highlighted during WP4 studies. Finally, D4.6 concludes WP4 by providing a synthesis of the technical content of our standardization proposals.

A3.8- Technical Work Package 5 – Experimental study cases in 2.4 and 5 GHz Band – Extraction and application of CIRs – Development of the WiFi test bed.

Deliverable	Date	“Title” Summary of the content
D5.1	Initial V1.0: 2016-03-20 Released V1.1 2016-04-22	“WiFi test bed setup development report”. This deliverable describes the WiFi Tesbed setup that will be used for all WP5 experiments. This document provides all information about the initial architecture of the test bed: • Legitimate part built, with the Wifi chipsets of Celeno, by partner Celeno. • Interceptor/Attacker part built with Ettus URSP devices by partner TCS. Moreover, D5.1 explicates how the test bed can be used for extracting dual sense CSIs in Wifi bands, modeling several legitimate and attacker configurations and test countermeasures and security schemes such as: • Artificial Noise and Beam-Forming • Secret Key Generation • Secrecy coding under radio advantage
D5.2	V1: 2016-03-20 V2: 2016-04-22	“Experiment campaign plan”. This deliverable includes all information about the initial experimental plan of the test bed and demonstrates the capabilities of the WiFi test bed before experimentations.
D5.3	Draft V1: 2016-03-20 Completed V2: 2016-12-10	“Intermediate Report on WiFi interceptor experiments with the test bed”. The draft deliverable included the first description items of experiments and storage of records performed during the experiment campaign, and it highlighted the outputs of the test beds. The completed version includes the complete description of experiments and results dedicated to Secret Key Generation under Wifi links.
D5.4	Completed V1: Published 14 December 2016	“Final Report on WiFi interceptor experiments with the test bed”. The completed version includes the complete description of experiments and results dedicated to Artificial Noise and Secrecy Coding under Wifi links.
D5.5	Completed V1: To be published December 2016	“Concluding report on experimental support for standardization proposals for WiFi PHYSEC upgrades”. The completed version will be described here after its publication (In the V2 version of the present deliverable D1.5).

A3.9- Technical Work Package 6 – Simulation study case – LTE Systems

Deliverable	Date	"Title" Summary of the content
D6.1	Initial (end of period 2) V1: 2015-06-30 Rev. (period 3) V2: 2016-02-20	"Modelling of LTE-based cellular system". This report describes in details the model and simulation of an LTE-based cellular system which will be later used to simulate realistic transmissions in LTE of legitimate users and signal interception by unauthorized users. The simulation focusses on the strengthening of transmission security (TRANSEC) and network security (NETSEC) of public LTE wireless systems and networks. The key objective of the simulation is to demonstrate the usefulness of the physical-layer-based security extensions by assessing their performance in a simulated LTE-based cellular environment. • After some overall presentation of LTE networks and waveforms, a presentation is given about the overall structure and capabilities of the open-source LTE link simulator developed by the Technical University of Vienna, which will be used to perform all simulations in WP 6. • Discussion of possible limitations of the link simulator and extensions to be introduced to make the link-level simulator a suitable tool for simulations of physical-layer security extensions (to be implemented in Task 6.2). • Discussion about the problem of radio channel modelling for correlated propagation channels between transmitter and legitimate receiver as well as transmitter and eavesdropper in various interception configurations: advantages and drawbacks of two different multi-antenna channel models: Winner II channel model and QuaDRiGa channel model. • First simulation results obtained for simple test cases The new version V2 details • the motivation for radio-channel models (QuaDRiGa versus Winer II) • simulation plan for SKG • Simulation plan for SC Simulation plans are provided for simulations to be performed in Task 6.2.
D6.2	V1: 2016-05-12	"Simulation of interception of waveform signals in LTE-based cellular system" This deliverable includes • A recall of the most important parts of the LTE link level simulators. • A complete description of the algorithms, simulator block diagrams and parameters, figures-of-merit, scenarios and test cases for the LTE link level performance of the LTE waveform signals with and without underlying Tag Signals. Complete results and detailed analyses are also provided. • A complete description of the algorithms, simulator block diagrams and parameters, figures-of-merit and first scenarios and test cases for the LTE link level performance of the LTE waveform signals enabling Secret Key Generation. First results and analyses are also provided. • A complete description of the algorithms, simulator's block diagrams and parameters, figures-of-merit and first scenarios and test cases for the LTE link level performance of the LTE waveform signals enabling AN-BF and Secrecy Coding. First results and analyses are also provided.
D6.3	V1: 2016-09-30	"LTE-based cellular system simulations - Concluding report including simulation results and proposals for standardization" Focusing on LTE-based cellular networks, this deliverable describes all implementations, test, performance simulations of the proposed physical-layer security schemes (Secure Pairing with Tag Signals, Secret Key Generation, Secrecy Coding), compared to the performance of a conventional transmission • Recall and complements on the algorithms, simulator block diagram and parameters, scenarios and test cases, figures-of-merit and results for the Tag Signals PHYSEC technique.

		• Recall of the algorithms, simulator block diagram and parameters, scenarios and test cases, figures-of-merit of the Secret Key Generation PHYSEC technique. Complete results and detailed analyses. • Recall of the algorithms, simulator block diagram and parameters, scenarios and test cases, figures-of-merit of the Artificial Noise Beam Forming and Secrecy Coding PHYSEC techniques. Complete results and detailed analyses. • Conclusions of the simulations results and proposal for standardization.

Annex 4 - Illustration of the feasibility proof of SKG schemes with Wifi experiments and LTE simulations

A4.1- Introduction

This section describes the steps and the performance of the SKG processing developed during the Phylaws project.

We recall below the main steps of the SKG scheme.

- **Channel Estimation**: where the radio channel is estimated and CSI are computed.
- **Channel Coefficient de-correlation**: in this pre-processing step, an algorithm is introduced to select channel coefficients with low cross correlation properties in order to increase the randomness of the quantized keys.
- **Quantization**: this step uses the Channel Quantization Alternate (CQA) algorithm introduced by Wallace to quantize the selected channel coefficients. The CQA minimizes key mismatch between Alice and Bob.
- **Information Reconciliation**: this step corrects the remaining mismatch between Alice and Bob keys. Secure sketches and error correcting codes are employed to correct Bob's errors on Alice's key.
- **Privacy Amplification**: this step improves the randomness of the secret key and removes the redundant information that could be used by Eve. To do so, hash functions are used and, when necessary, the final key length is reduced. This final step guarantees that the generated secret key is fully de-correlated from the key computed by the eavesdropper.

During the SKG scheme, the performance is evaluated by estimating both key agreement and key privacy:

- **Evaluation of key agreement:** We compute the **mismatch between Alice and Bob** key bits which represents the amount of errors made by Bob on Alice's keys. The mismatch should be null in order to ensure that Alice and Bob agree on the same keys.
- **Evaluation of key privacy:** We compute the **Bit Error Rate (BER) between Bob and Eve** keys which represents the amount of errors made by Eve on Bob's keys. For the best confidentiality, this BER should be as close as possible to value 0.5 that ensures that Eve has no information on the secret key.

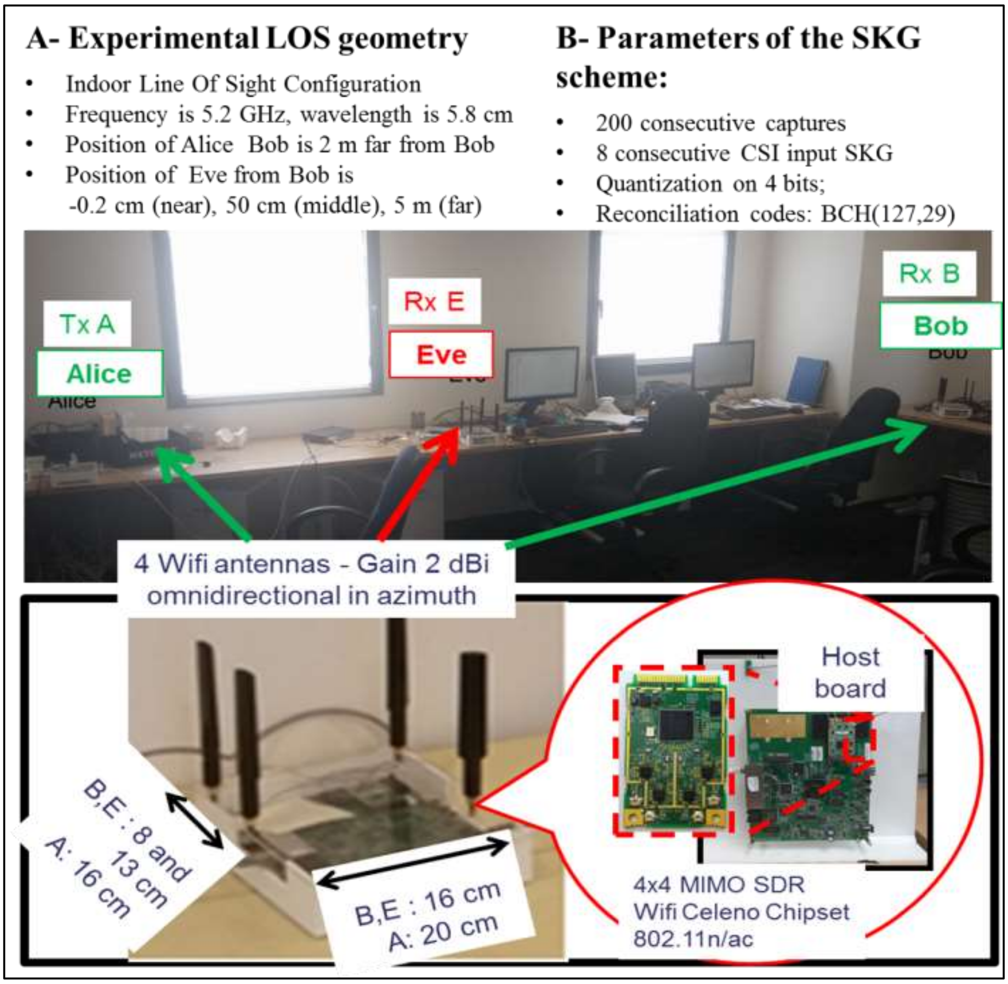
A4.2- Examples of SKG experimental results on Wifi links.

First, Figure 15 below illustrates one of the experimental geometry (Line of Sight configuration).

Then, Figure 16 provides entropy and information estimates computed in the geometry of Figure 15 (Eve location is "near case" e.g. 20 cm to Bob). The results of this figure show that, for every test, the dependency between Alice and Bob is higher than between Alice and Eve or Bob and Eve. This means that Alice and Bob share more information together than with Eve. Moreover, according to the most common value estimate test, the dependency between Alice and Bob is three times higher than the dependency of Alice and Bob with Eve. Finally these results confirm that:

- The channel estimates of Alice and Bob are highly correlated, what highlights the channel reciprocity of the radio channel and the capability of sharing keys.
- The channel estimates of Eve are much less correlated, what highlights the channel spatial diversity of the radio channel and the confidentiality of the keys.

Therefore, the amount of information shared by Alice and Bob is significant and not accessible to Eve. The channel information can thus be quantized to generate keys that will be shared by legitimates and that will be secret for a third party.



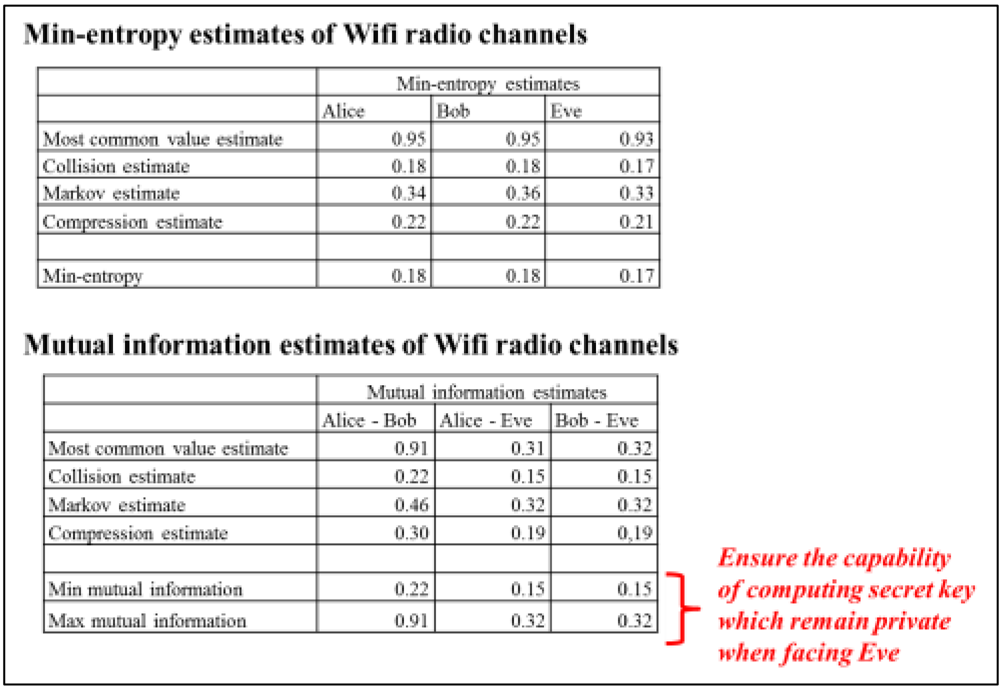
A- Experimental LOS geometry

- Indoor Line Of Sight Configuration
- Frequency is 5.2 GHz, wavelength is 5.8 cm
- Position of Alice Bob is 2 m far from Bob
- Position of Eve from Bob is -0.2 cm (near), 50 cm (middle), 5 m (far)

B- Parameters of the SKG scheme:

- 200 consecutive captures
- 8 consecutive CSI input SKG
- Quantization on 4 bits;
- Reconciliation codes: BCH(127,29)

Figure 15: example of geometry for the SKG experiments



Min-entropy estimates of Wifi radio channels

	Min-entropy estimates		
	Alice	Bob	Eve
Most common value estimate	0.95	0.95	0.93
Collision estimate	0.18	0.18	0.17
Markov estimate	0.34	0.36	0.33
Compression estimate	0.22	0.22	0.21
Min-entropy	0.18	0.18	0.17

Mutual information estimates of Wifi radio channels

	Mutual information estimates		
	Alice - Bob	Alice - Eve	Bob - Eve
Most common value estimate	0.91	0.31	0.32
Collision estimate	0.22	0.15	0.15
Markov estimate	0.46	0.32	0.32
Compression estimate	0.30	0.19	0,19
Min mutual information	0.22	0.15	0.15
Max mutual information	0.91	0.32	0.32

Ensure the capability of computing secret key which remain private when facing Eve

Figure 16: estimates of min-joint entropy and mutual information

Over a total of 228 generated keys of 127 bits each, Figure 17 provides:

- The mismatch between the keys computed by Alice and Bob. For each key, the mismatch was less that 10% after quantization and the reconciliation step managed to correct all errors allowing Bob to always retrieve Alice's key.

- The Binary Error Rate between keys computed by Bob and Eve. While after quantization, the average BER is close to 0.3, what is not enough to ensure perfect privacy of the keys, the privacy amplification raises this BER value up to 0.5 meaning that Eve has no more information on the secret keys.

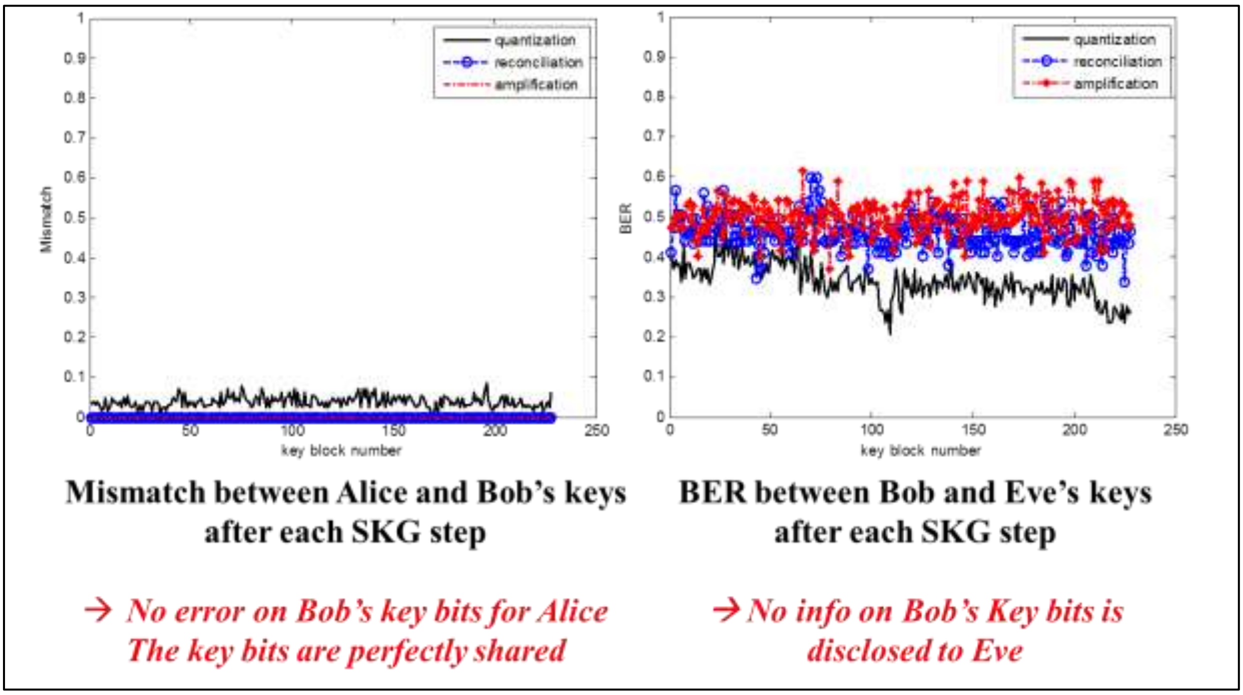


Figure 17: mismatch between Alice and Bob's keys and Binary Error Rate between Bob and Eve's keys after each step of the SKG processing.

Figure 18 shows the overall randomness of key bits output by SKG. Even if most of the keys already look random after the quantization step, some remaining stationary components into the LOS near range propagation due to time-correlated channel coefficients cause some deterministic patterns between key 100 and key 200. As expected, privacy amplification mitigates the remaining determinism and every key become completely random.

Finally, Figure 19 shows:

- The number of 127-bits keys that passed the NIST frequency mono-bit test (top left) and the NIST Runs test (top right): The results show that many keys pass the test after quantization (blue bars) and that almost all keys pass the test after amplification (green bars).
- The number of 256-bits keys that passed the Intel Health Check (bottom left): The results show that all keys passed the test after quantization (blue bars) and also after privacy amplification (green bars), except one key.
- The number 256-bits keys recovered by Bob (bottom right - blue bars) and Eve (bottom right - green bars). The results show, as expected, that the key sharing between legitimates is perfect (Bob computes exactly the same secret keys as Alice without any error) and also that the privacy of generated keys is perfect (Eve can recover none of secret keys).

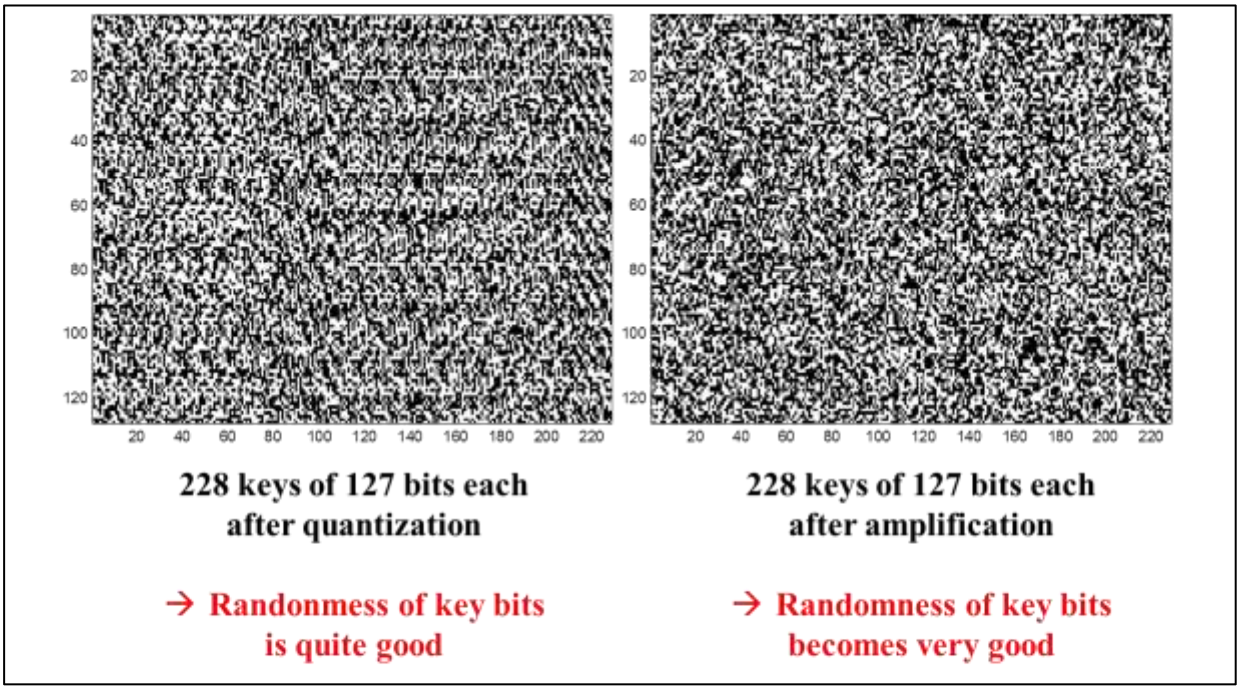


Figure 18: keys randomness after quantization and after privacy amplification

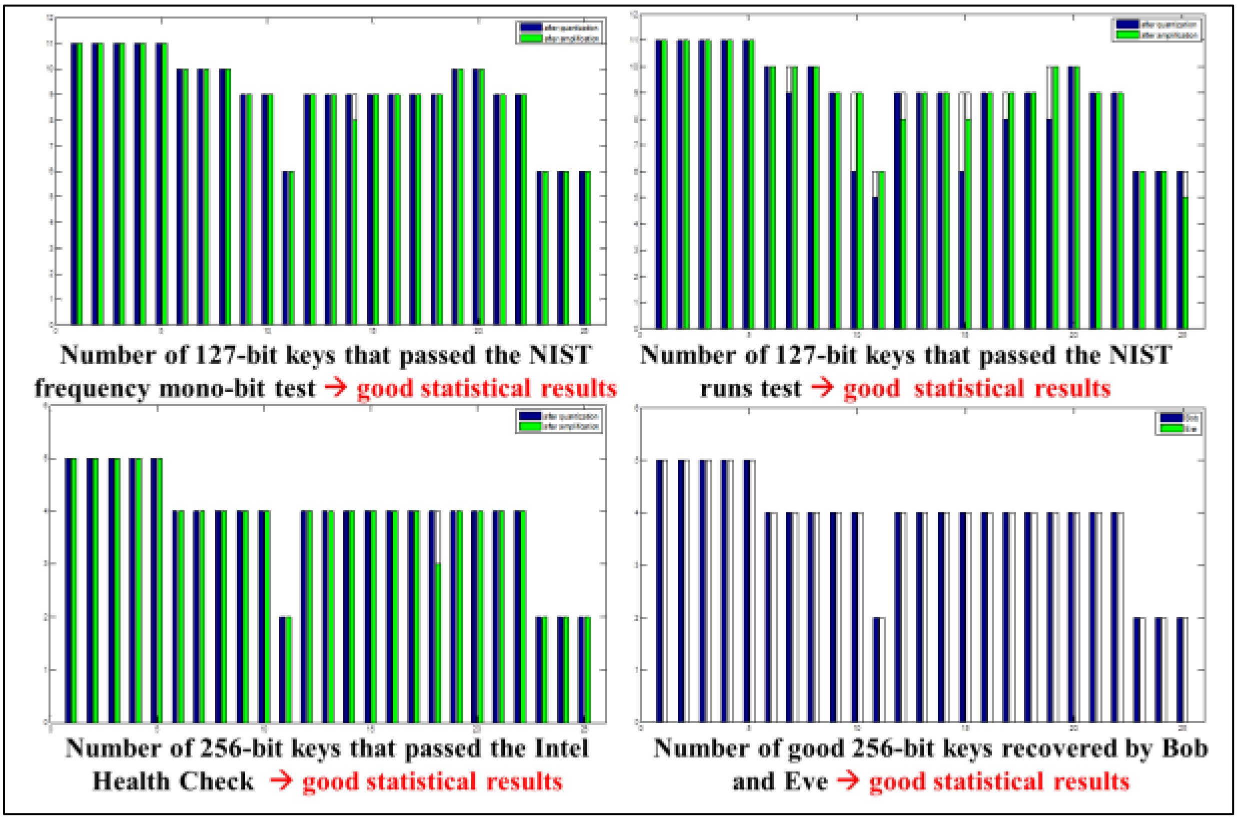


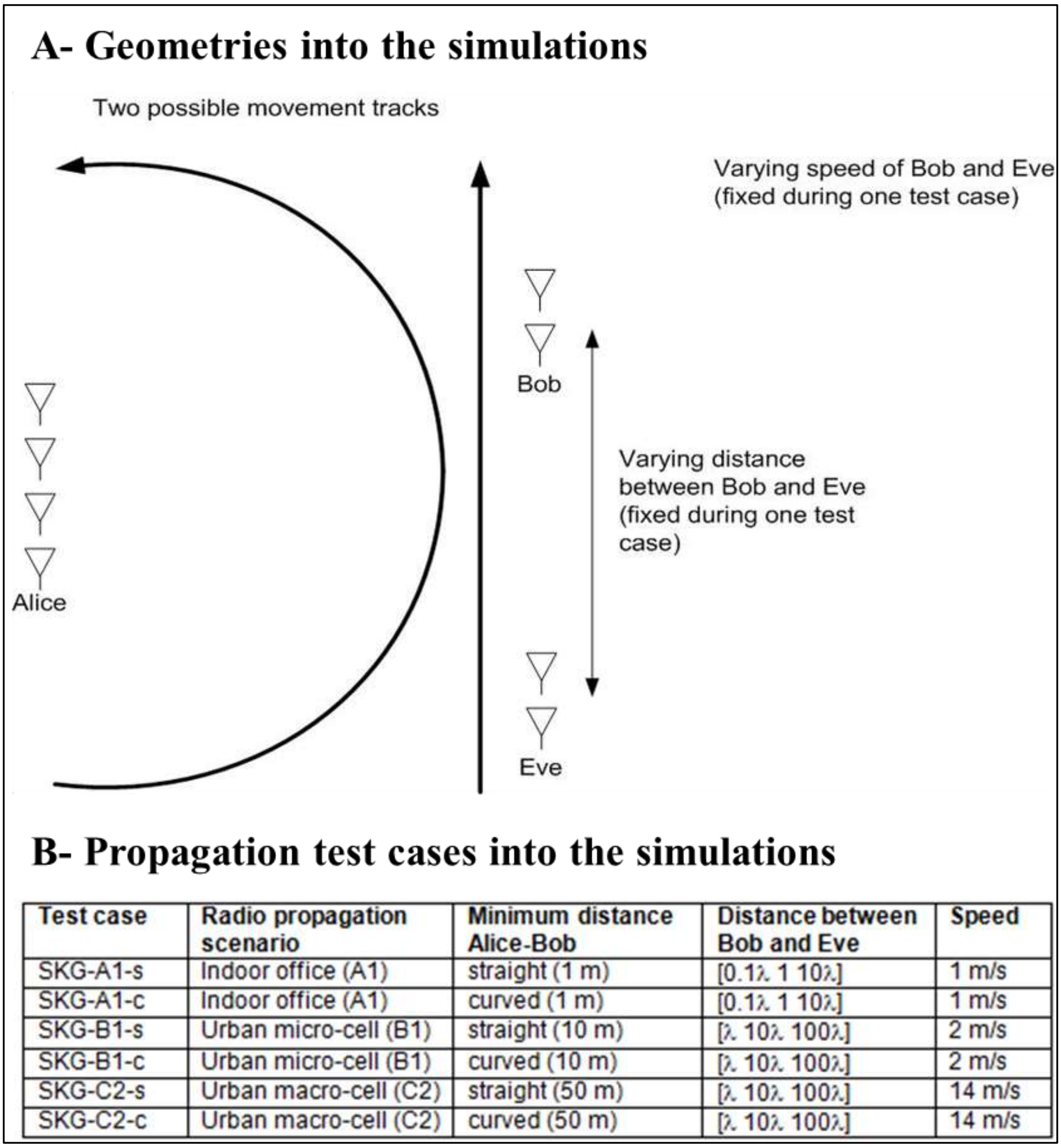
Figure 19: statistical results of NIST and Intel health test applied to the key bits output by the SKG scheme

A4.3- Examples of outputs of SKG simulations on LTE links

Massive simulations of the SKG scheme at LTE links extended the performance evaluation and provided statistical indicators about the overall efficiency regarding both:

- Key agreement between legitimates nodes and terminals
- Key confidentiality when facing third party.

Relevant to the geometries illustrated in Figure 21 illustrates the statistical performance of the SKG scheme over realistic LTE radio environments at frequency 2.6 GHz.


A- Geometries into the simulations
Two possible movement tracks
Varying speed of Bob and Eve (fixed during one test case)
Bob
Varying distance between Bob and Eve (fixed during one test case)
Alice
Eve
B- Propagation test cases into the simulations

Test case	Radio propagation scenario	Minimum distance Alice-Bob	Distance between Bob and Eve	Speed
SKG-A1-s	Indoor office (A1)	straight (1 m)	[0.1λ 1 10λ]	1 m/s
SKG-A1-c	Indoor office (A1)	curved (1 m)	[0.1λ 1 10λ]	1 m/s
SKG-B1-s	Urban micro-cell (B1)	straight (10 m)	[λ 10λ 100λ]	2 m/s
SKG-B1-c	Urban micro-cell (B1)	curved (10 m)	[λ 10λ 100λ]	2 m/s
SKG-C2-s	Urban macro-cell (C2)	straight (50 m)	[λ 10λ 100λ]	14 m/s
SKG-C2-c	Urban macro-cell (C2)	curved (50 m)	[λ 10λ 100λ]	14 m/s

Figure 20: configuration of the SKG simulation under LTE links

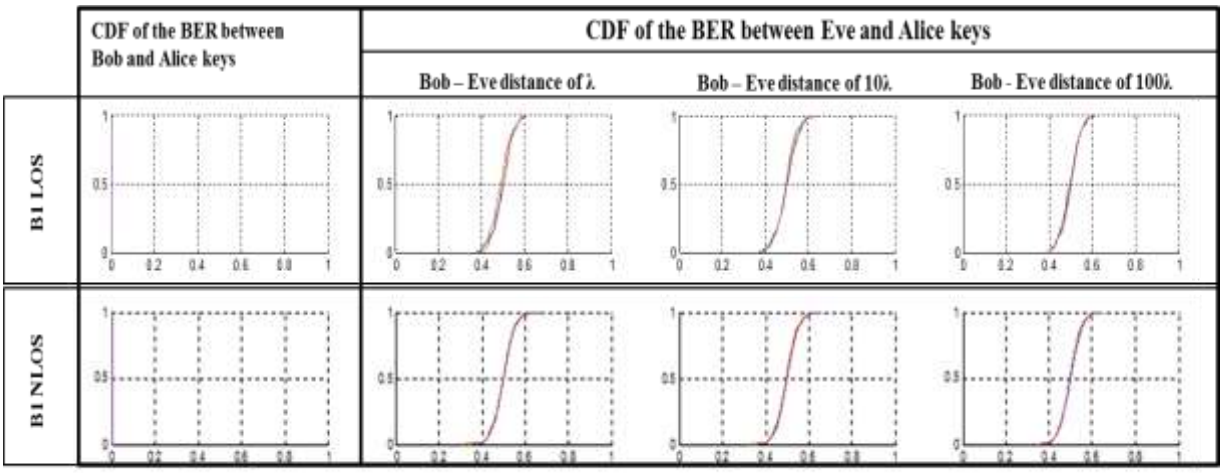


Figure 21: statistical results of the Binary Error Rate between the keys computed by Bob and Alice and between Bob and Eve for the SKG-B1 LOS and NLOS environment, straight movement propagation mode and various distances of Eve to Bob

The two preceding figures confirm the good performance of the SKG scheme and they extend the previous experimental results over LTE networks with various geometries and propagation environments:

- at the first column of Figure 21, key agreement is statistically good between Alice and Bob, what means that channel reciprocity applies and that reconciliation is efficient in the SKG scheme. This is proven by the null value of the Cumulative Density Function of the Binary Error rate relevant to Bob's decoded key bits.
- at the second to fourth columns of Figure 21, key privacy computed by Alice and Bob is statistically good, what mean that channel spatial diversity applies and ensures significant de-correlation of legitimate and attacker channels which is well exploited into the SKG scheme. This is proven by the 0.5 main value of the Cumulative Density Function of the Binary Error rate relevant to Eve's decoded key bits, whatever is the distance of Eve to Bob.

Annex 5 - Illustration of the feasibility proof achieved of SC schemes with Wifi experiments and LTE simulations

A5.1- Introduction

This section illustrates the steps and the performance of the SC processing by experimental and simulation outputs of the Phylaws project.

We recall below the main step of the SC scheme.

- **Radio Advantage setting**: with a radio protocol involving Artificial Noise and explicit Beam Forming schemes.
- **Channel coding and decoding**: involving inner codes and decoder, as done in existing standards
- **Complete secrecy coding and decoding**: involving both inner and outer codes, as developed and patented in the Phylaws project.

During the SC scheme, the performance is evaluated by estimating both user data agreement and user data confidentiality:

- **Evaluation of user data agreement:** We compute the **Bit Error Rate (BER) between Alice and Bob** data bits, which represents the amount of errors made by Bob on Alice's transmitted data. This BER should be null or very low in order to ensure that the transmission from Alice to Bob is perfectly reliable.
- **Evaluation of user data confidentiality:** We compute the **Bit Error Rate (BER) between Alice and Eve** data bits, which represents the amount of errors made by Eve on Alice's transmit data. For optimal confidentiality, this BER value should be as close as possible to value 0.5 that ensures that Eve gets no information on the Alice's transmitted data.

A5.2- Examples of SC experimental results on Wifi links.

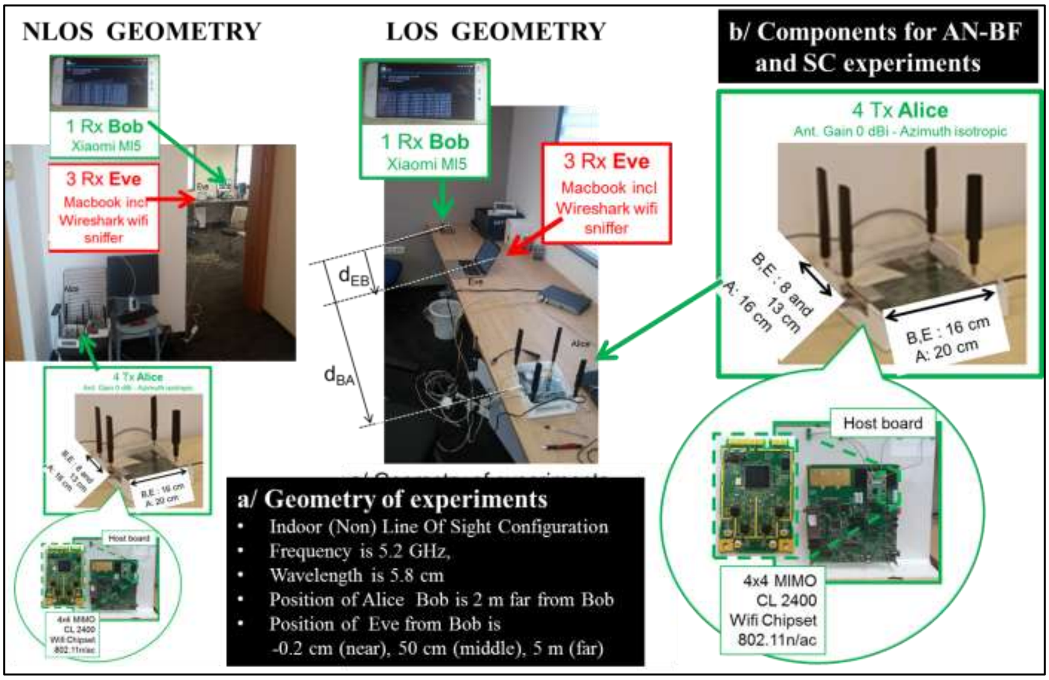
Figure 22 illustrates one of the experimental geometry (Line Of Sight and Non Line Of Sight).

Then, Figure 23 provides measured Signal to Interference + Noise ratios and relevant radio advantage of Bob compared to Eve on user data with Wifi frames in the geometry of Figure 10 (LOS Alice to Bob and Eve, middle Eve case, e.g. 50 cm from Bob) as a function of the mean power ratio value alpha of the Artificial Noise applied on the user data. The results of this figure show that while the receiver noise of Bob keeps low value with respect to the received signals at Bob's side (SNR of value 10 dB and more, as usually requested for conventional Wifi transmissions), the following security performance is achieved:

- very significant Radio Advantages to any third party can be reached quite easily thanks to the Artificial Noise (values of 10 dB and more for a mean power ratio value alpha=0.5, value of 14 dB and more for a mean power ratio value alpha=0.9),
- the relevant disturbance of Bob's receiver remain negligible thanks to the Beam Forming (Signal to Interference + Noise value at Bob's side keeps values greater than 5 dB for a high power ratio value alpha=0.9 and greater than 11 dB for a mean power ratio value alpha=0.5).

Figure 24 is relevant to numerous sequences of Wifi packets that are transmitted by Alice in NLOS geometry and that are perfectly decoded by Bob. It shows the Binary Error Rate that Eve can achieve with optimal decoding processing (List decoder [TALVARDY] and LLR-Base Successive Cancellation List decoder, [BALATSOUKAS]) under Artificial Noise as a function of the power ratio alpha, in several conditions:

- with channel coding only (blue plots)
- with secrecy-coding (red plots)



a/ Geometry of experiments

- Indoor (Non) Line Of Sight Configuration
- Frequency is 5.2 GHz,
- Wavelength is 5.8 cm
- Position of Alice Bob is 2 m far from Bob
- Position of Eve from Bob is -0.2 cm (near), 50 cm (middle), 5 m (far)

Figure 22: example of experimental configuration of AN-BF and SC on Wi-Fi 2.4 and 5 GHz links

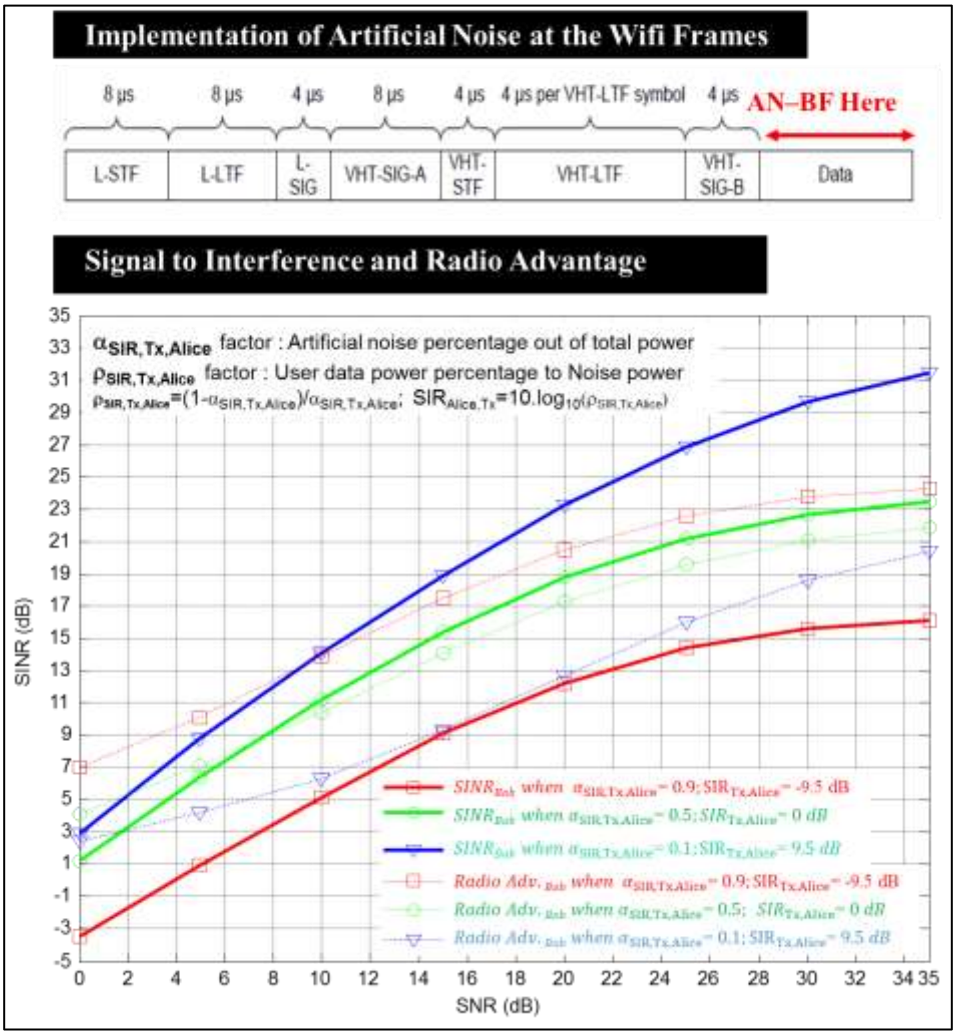


Figure 23: example of experimental results of AN-BF on Wi-Fi 5 GHz links, where Eve is in middle position

The statistical plots of Figure 24 show two performance of highest interest:

- The use of secrecy coding raises the BER from values included in the interval [0.1, 0.3] to value 0.5, which is consistent with the ultimate “semantic” security
- The variance of Eve disturbance over numerous decoding attempts of Wifi Packets remains very low, which ensures that the secrecy performance is constant and reliable over time.

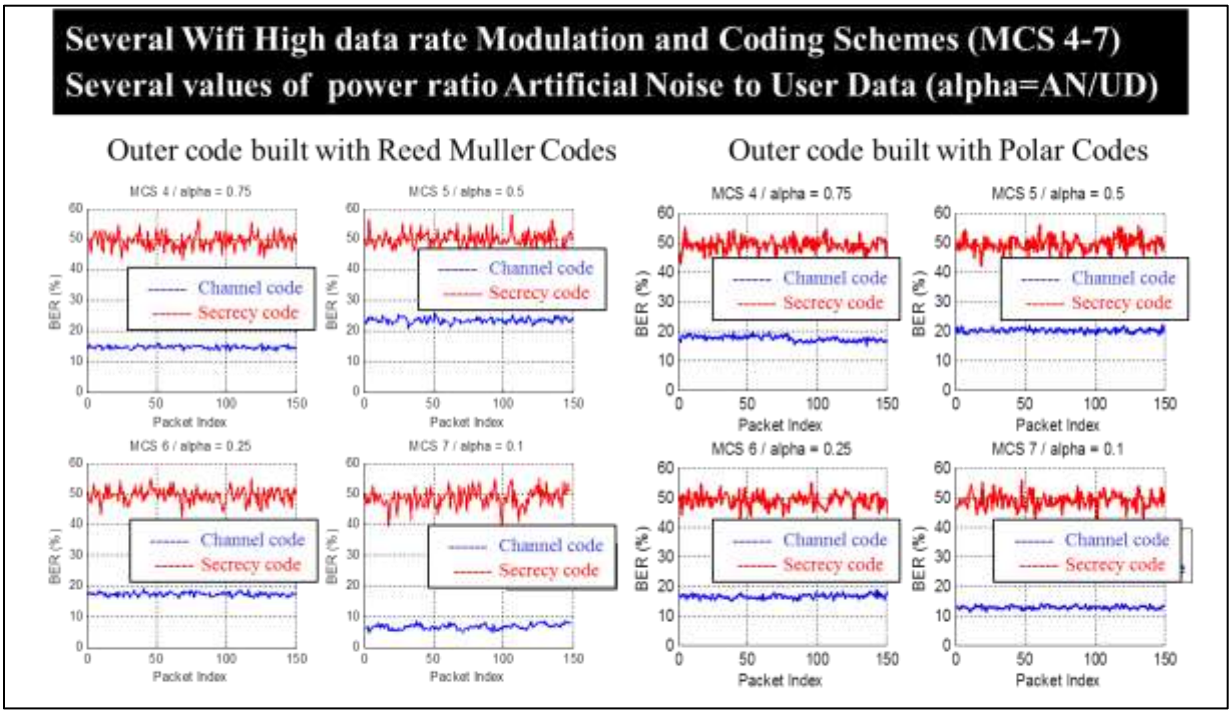


Figure 24: example of experimental BER of channel codes and secrecy codes applied with AN-BF Wi-Fi 5 GHz links, where Eve is 50 cm close to Bob and Alice is in Non Light of Sight geometry

A5.3- Examples of outputs of SC simulations on LTE links

Massive simulations of the AN-B + SC scheme at LTE links extended the performance evaluation and provided statistical indicators about the overall efficiency regarding both

- Data user agreement between legitimates nodes and terminals
- Data user confidentiality when facing third party.

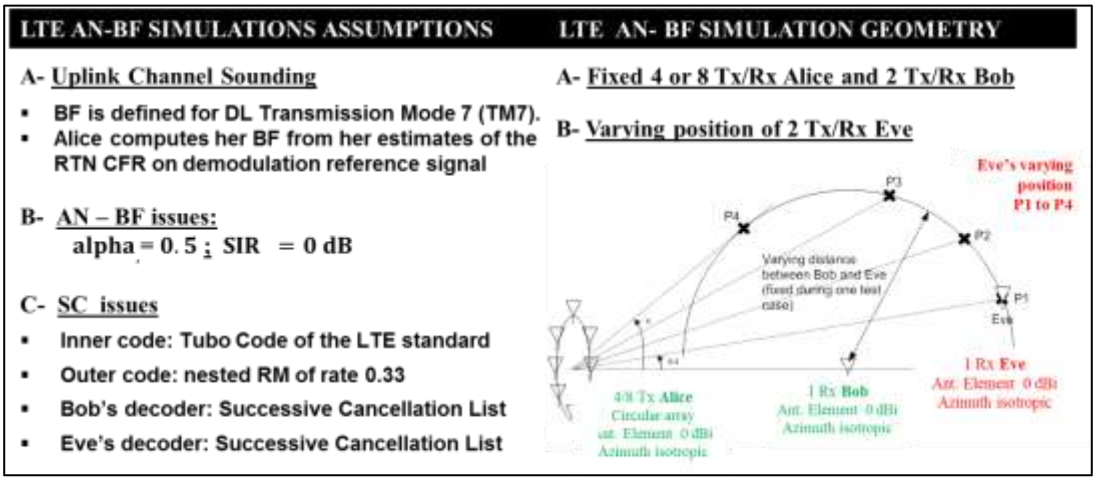
Relevant to the geometries and parameters given in Figure 25 below, Figure 26 shows the statistical performance of the AN-BF scheme over realistic LTE radio environments at a frequency of 2.6 GHz while Figure 27 shows the statistical performance of the secrecy coding applied on user data.

These two latter figures confirm the good confidentiality performance of the SC scheme and they extend the previous experimental results over LTE networks and various geometries and propagation environments:

- at the left and right parts of Figure 27, user data agreement is statistically good between Alice and Bob, what means that channel reciprocity applies and that reconciliation is efficient in the SKG scheme. This is proven by the null value of the Cumulative Density Function of the Binary Error rate relevant to Bob’s decoded key bits (blue plots).

- at the left hand part of Figure 27, user data confidentiality in presence of AN-BF without SC is statistically good for Radio Advantage values exceeding the threshold of 8 dB, which occurs more than 50% of simulated cases without disturbance of Bob’s decoding as shown by Figure 27 on the right column. Two other very significant performance are the fast raise of Eve's BER from low values to value 0.5 and the low variance of the BER in the vicinity of value 0.5 when confidentiality is achieved (SNR > 8 dB).

- Still at the right part of Figure 27, user data confidentiality in presence of AN-BF with SC is statistically good for Radio Advantage values exceeding only a threshold 4 dB, which occurs more than 90% of simulated cases at P1 P2 P3 positions of Eve and 50% of simulated cases at P4 positions of Eve without disturbance of Bob's decoding (see also Figure 26 right column). As above, two very significant performance are the fast raise of Eve's BER from low values to value 0.5 and the low variance of the BER in the vicinity of value 0.5 when confidentiality is achieved (SNR >4 dB).



LTE AN-BF SIMULATIONS ASSUMPTIONS

A- Uplink Channel Sounding

- BF is defined for DL Transmission Mode 7 (TM7).
- Alice computes her BF from her estimates of the RTN CFR on demodulation reference signal

B- AN – BF issues:

alpha = 0.5 ; SIR = 0 dB

C- SC issues

- Inner code: Tubo Code of the LTE standard
- Outer code: nested RM of rate 0.33
- Bob's decoder: Successive Cancellation List
- Eve's decoder: Successive Cancellation List

LTE AN- BF SIMULATION GEOMETRY

A- Fixed 4 or 8 Tx/Rx Alice and 2 Tx/Rx Bob

B- Varying position of 2 Tx/Rx Eve

Figure 25: simulation configuration of AN-BF + SC on LTE 2.6 GHz links

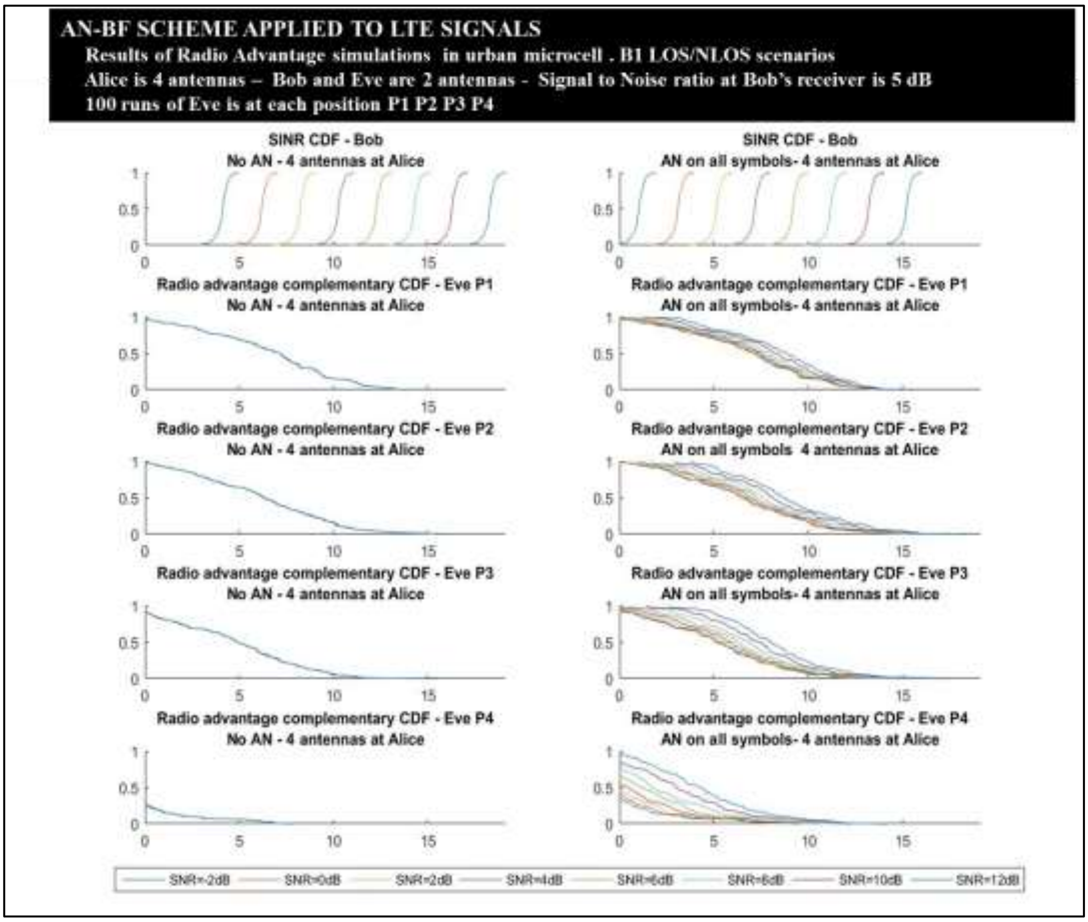
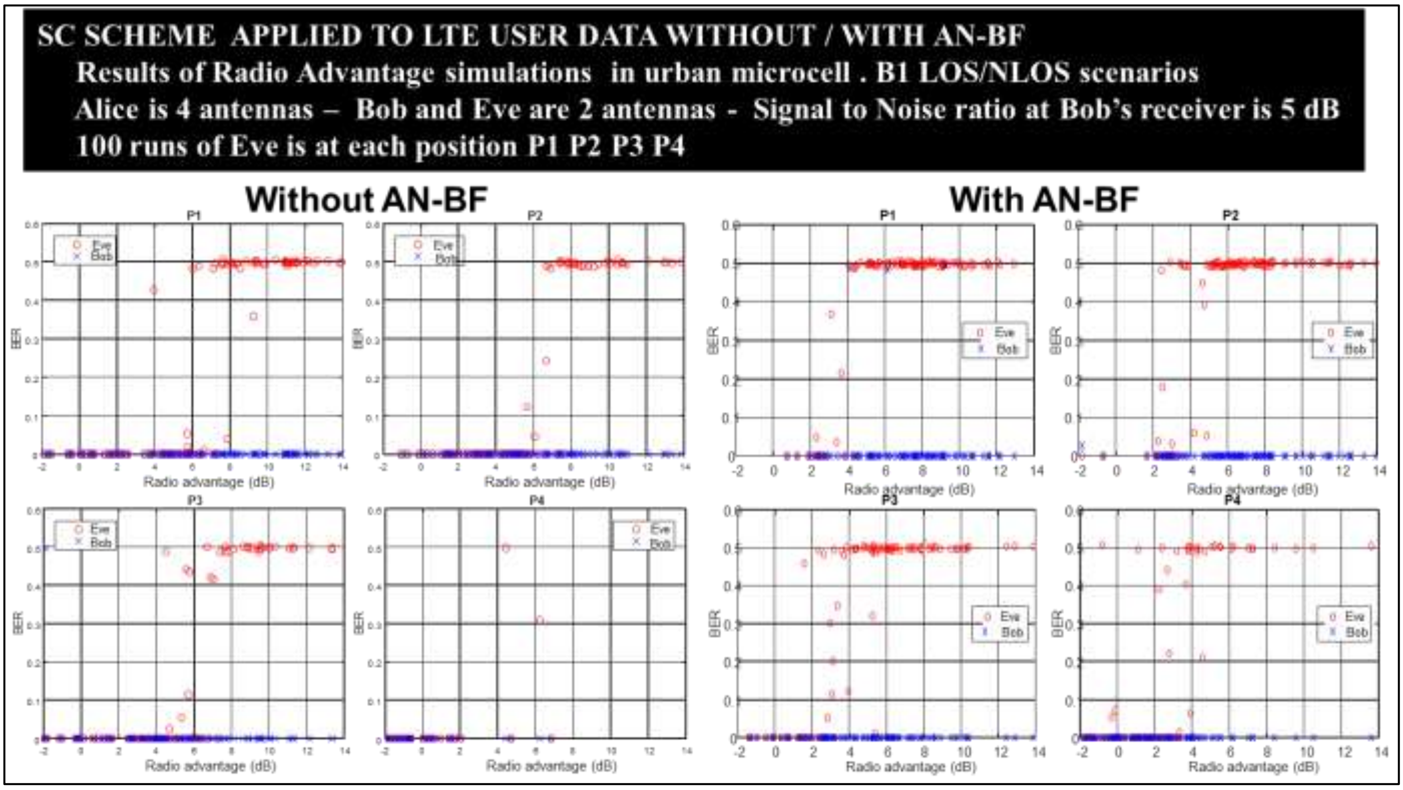


Figure 26: statistical (simulation) results of the Radio Advantage in the AN-BF configuration of Figure 26



SC SCHEME APPLIED TO LTE USER DATA WITHOUT / WITH AN-BF

Results of Radio Advantage simulations in urban microcell . B1 LOS/NLOS scenarios

Alice is 4 antennas – Bob and Eve are 2 antennas - Signal to Noise ratio at Bob's receiver is 5 dB

100 runs of Eve is at each position P1 P2 P3 P4

Figure 27: statistics of simulated BER at outputs of the Bob's decoder and Eve decoder for LTE TM7 links in the AN-BF configuration of Figure 27. Result comparison with AN-BF alone and with SC over AN-BF

Annex 6 - Core content of Phylaws' standardization proposals

A6.1- Basic ideas proposed to standardization bodies for Physec-based protections of existing RATs

1/ Re-use Channel estimates of the first synchronization and equalization procedures **for Channel State Information**

2/ Input Physec schemes with this Channel State Information (SP, SKG, AN-BF+SC)

3/ Protect the early transmitted messages in the existing/future RATs

- ❑ Identification request and acknowledgement messages ((T/I)MSI MAC address)
- ❑ Authentication request and acknowledgement messages
- ❑ Cipher establishment and response messages

=> Goals: Eve has no more decoding capability of authentication parameters

Eve has no more decoding capability of subscriber/terminal IDs

4/ Add PHY layer protections at on-going communication

- ❑ Input of cipher header with SKG
- ❑ Protection of MAC header, IP address, with SKG or SC
- ❑ Use SKG for location control, for messages integrity control (use the generated keys as "propagation stamps"),
- ❑ etc.

A6.2- Enhanced ideas for Physec-based protections of the PHY layer (future RATs)

Prior the preceding step 1:

01/ Establish Securely Paired (SP) channels between Alice and Bob

- ❑ Downlink and Uplink Tag signals (TSs), enhanced with Uncoordinated Spread Sequences (USS) and Time Jitter (TJ) schemes
- ❑ Interrogation and Acknowledgement Sequences (IASs)

02/ Negotiate the channel during SP and establish CSI by using TSs and IASs

- ❑ Channel State Information (CSI) are here authenticated
- ❑ Channel State Information has better accuracy
- ❑ During SP, TS can support protected Alice-Bob exchanges
  - o enhanced security during the SKG enabling, longer keys
  - o enhanced security during AN-BF and SC establishment
- ❑ In addition, TSs can take benefit of the SC (while TSs are self-interfered, they have a native radio advantage) to support protected Alice-Bob exchanges

During the preceding steps 1, 2, 3, 4:

Invert the order of Authentication and Identification (in radio-cellular networks)

- ❑ Pre-identification: only UE's HLR has to be transmitted
- ❑ Authenticate then: needs only HLR Id (and not (T/I)MSI)
- ❑ Only after Authentication, transmit UE's and Subscriber's IDs.
- ❑ Therefore, protected Authentication implies protected IMSI transmission

Superimpose underlying TSs and IASs in parallel to transmission of classical messages

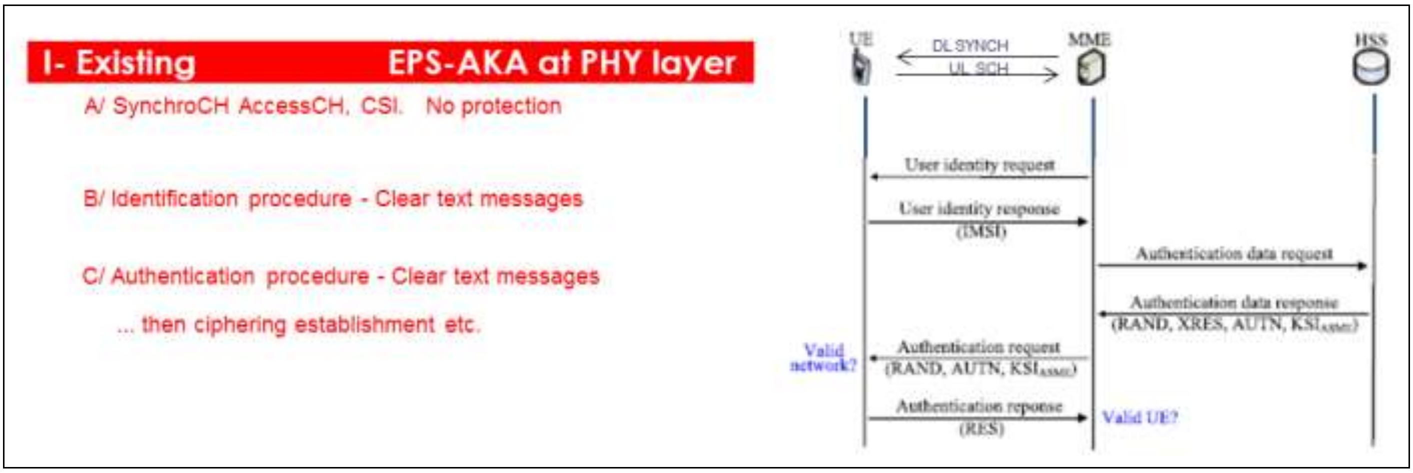
- ❑ Use TS for Integrity control of classical messages, etc.
- ❑ Use TS as a low data rate control channel with enhanced protection

Note that all these enhancements focus mainly on early access stages. This proposal strategy had two advantages:

- Our key-free secure schemes fulfil (dramatically wide) existing lacks, that are (now) well recognized by standardization bodies.
- Our schemes apply to a more secure enabling of existing authentication integrity control mechanism, and do not replace them.
- Regarding traffic of user data, there is no competition with cipher and integrity control schemes that are already standardized.

A6.3- Evolution proposals of the early radio access to network into 3GPP standards

The existing radio access protocol and our short-term and mid-term evolutions proposals are illustrated in the three figures below. These figures are completed after [ZOU].



I- Existing EPS-AKA at PHY layer

A/ SynchroCH AccessCH, CSI. No protection

B/ Identification procedure - Clear text messages

C/ Authentication procedure - Clear text messages

... then ciphering establishment etc.

Figure 28: existing radio access protocols of 3GPP

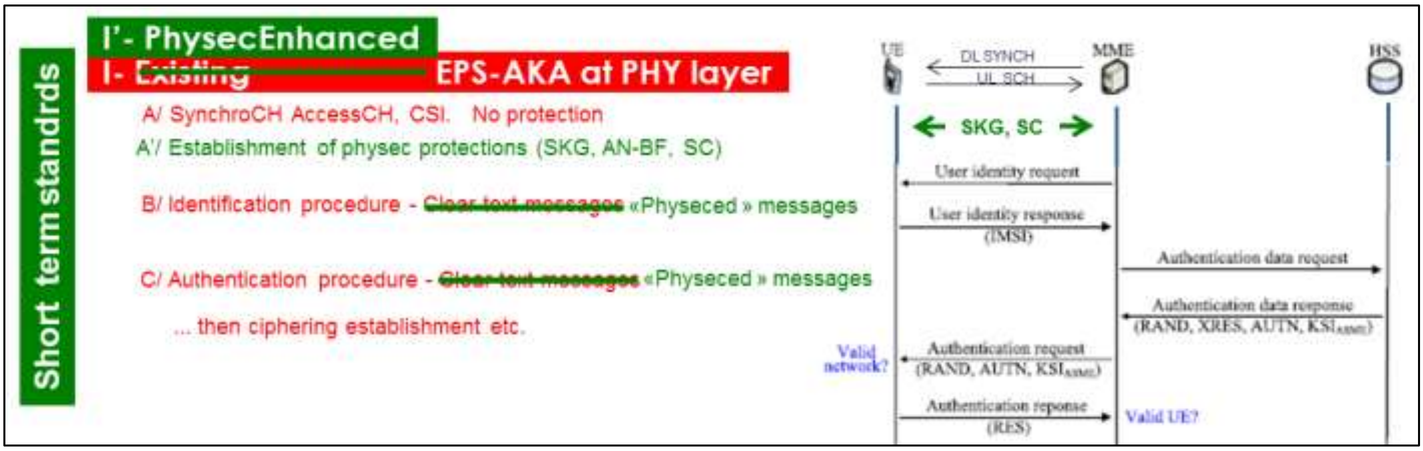

Short term standrds
I'- PhysecEnhanced
I- ~~Existing~~ EPS-AKA at PHY layer
A/ SynchroCH AccessCH, CSI. No protection
A'/ Establishment of physec protections (SKG, AN-BF, SC)
B/ Identification procedure - ~~Clear text messages~~ «Physeced » messages
C/ Authentication procedure - ~~Clear text messages~~ «Physeced » messages
... then ciphering establishment etc.
UE
DL SYNCH
UL SCH
MME
HSS
SKG, SC
User identity request
User identity response (IMSI)
Authentication data request
Authentication data response (RAND, XRES, AUTN, KSI_ASME)
Valid network?
Authentication request (RAND, AUTN, KSI_ASME)
Authentication reponse (RES)
Valid UE?

Figure 29: short-term evolution proposal of the radio access protocols of 3GPP including basic key-free Physec-based added protections

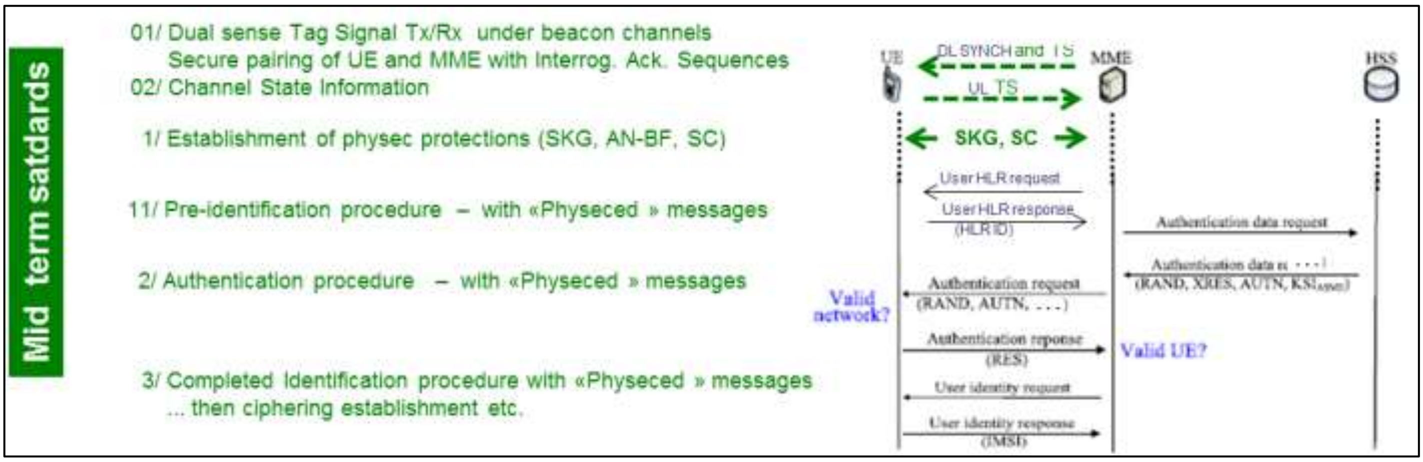
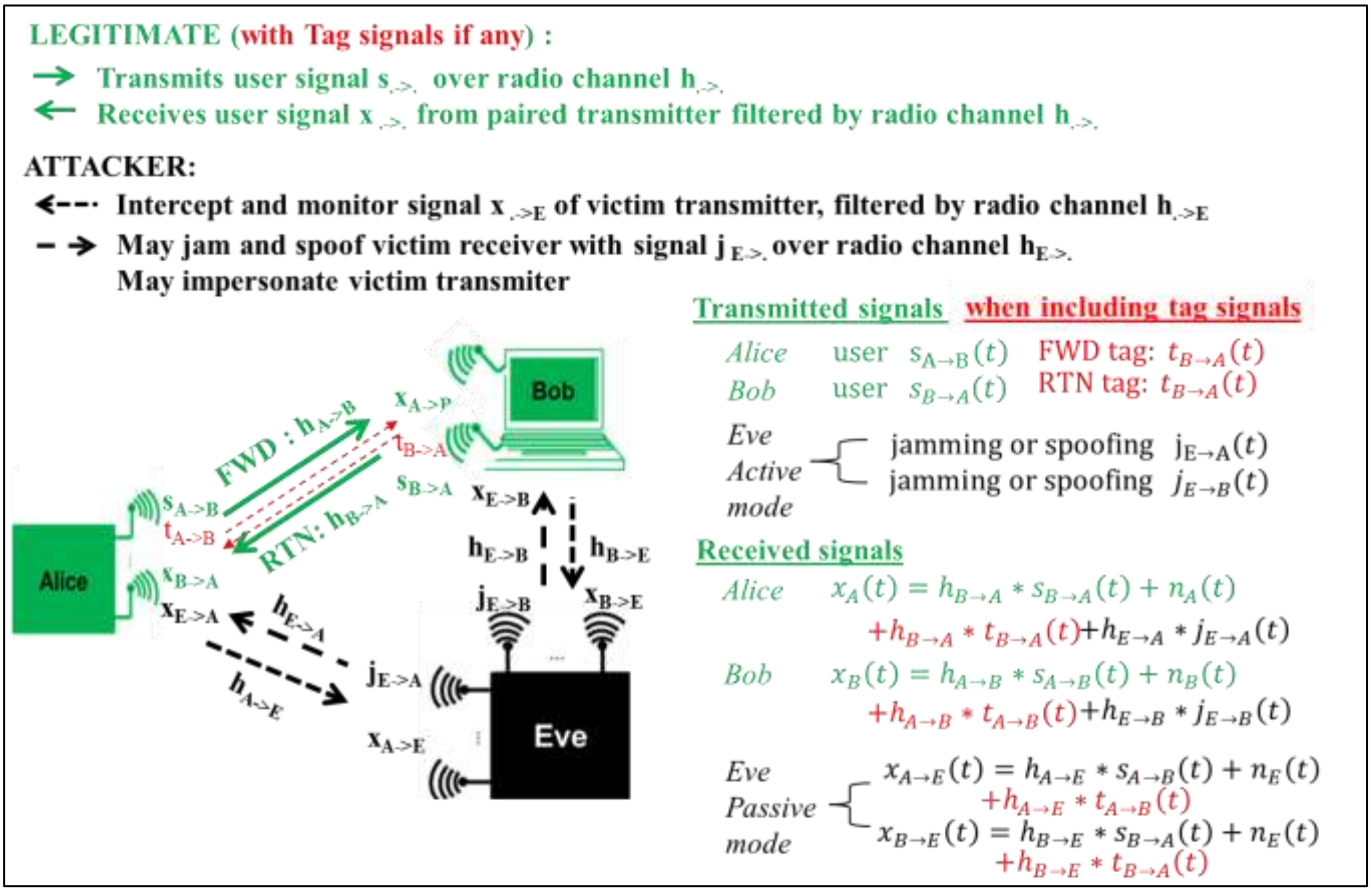

Mid term satdards
01/ Dual sense Tag Signal Tx/Rx under beacon channels
Secure pairing of UE and MME with Interrog. Ack. Sequences
02/ Channel State Information
1/ Establishment of physec protections (SKG, AN-BF, SC)
11/ Pre-identification procedure – with «Physeced » messages
2/ Authentication procedure – with «Physeced » messages
3/ Completed Identification procedure with «Physeced » messages
... then ciphering establishment etc.
UE
DL SYNCH and TS
UL TS
MME
HSS
SKG, SC
User HLR request
User HLR response (HLR ID)
Authentication data request
Authentication data r... (RAND, XRES, AUTN, KSI_ASME)
Valid network?
Authentication request (RAND, AUTN, ...)
Authentication reponse (RES)
Valid UE?
User identity request
User identity response (IMSI)

Figure 30: mid-term evolution proposals of the radio access protocols of 3GPP including combined/enhanced key-free Physec-based protections and modification the protocol order of Authentication and Identification procedures

Annex 7 – Review of the threat models considered into Phylaws

A7.1- Introduction figure to typical radio-configuration and exchanged radio signals

Figure 31 below recalls the radio scenarios which were considered in Phylaws with passive, active and man in the middle Eve. It also recalls which are the radio channels and the transmitted and received signals over legitimate and attacker propagation channels. Information theoretic notions and theoretical foundations of Physical layer Security are recalled in annex 8.



LEGITIMATE (with Tag signals if any) :

→ Transmits user signal $s_{.->.}$ over radio channel $h_{.->.}$

← Receives user signal $x_{.->.}$ from paired transmitter filtered by radio channel $h_{.->.}$

ATTACKER:

←--- Intercept and monitor signal $x_{.->E}$ of victim transmitter, filtered by radio channel $h_{.->E}$

- -→ May jam and spoof victim receiver with signal $j_{E->.}$ over radio channel $h_{E->.}$

May impersonate victim transmiter

Transmitted signals when including tag signals

Alice user $s_{A\to B}(t)$ FWD tag: $t_{B\to A}(t)$

Bob user $s_{B\to A}(t)$ RTN tag: $t_{B\to A}(t)$

Eve Active mode jamming or spoofing $j_{E\to A}(t)$; jamming or spoofing $j_{E\to B}(t)$

Received signals

Alice $x_A(t) = h_{B\to A} * s_{B\to A}(t) + n_A(t) + h_{B\to A} * t_{B\to A}(t) + h_{E\to A} * j_{E\to A}(t)$

Bob $x_B(t) = h_{A\to B} * s_{A\to B}(t) + n_B(t) + h_{A\to B} * t_{A\to B}(t) + h_{E\to B} * j_{E\to B}(t)$

Eve Passive mode

$x_{A\to E}(t) = h_{A\to E} * s_{A\to B}(t) + n_E(t) + h_{A\to E} * t_{A\to B}(t)$

$x_{B\to E}(t) = h_{B\to E} * s_{B\to A}(t) + n_E(t) + h_{B\to E} * t_{B\to A}(t)$

Figure 31: legitimate link and eavesdropper links – notations relevant to signals and propagation channels

A7.2- Model of Passive Eve

Eve's procedures

- Records every signal.
- Demodulates and decodes signalling and data messages between Alice and Bob.
- Does not emit any signal.
- Has a finite number of receiving antennas.

Eve's limits / drawbacks

- Cannot influence the legitimate exchanges.
- Very sensitive to radio conditions.
- None of the Eve's receiving antennas are co-located neither with Bob's antennas, nor with Alice's ones.

Eve's advantages

- No real-time constraints of any kind.

Main risks for legitimate users

- Maximal risk occurs when Eve is informed about their Subscribers keys (Ki on SIM, K on USIM, etc.) and can also reproduce the complete the legitimate protocol with off-line processing.

Remark

- Such risks illustrate the limits the current approach of public wireless security based only on cryptographic key distribution.

Passive Eve's Model

- Passive Eve is mainly modeled
  - For her receiving part, by the classical MIMO receiver model affected with Gaussian Noise, propagation delays $\tau_{A \rightarrow E}$, $\tau_{\rightarrow E}$ and propagation channel matrix $H_{A \rightarrow E}$ and $H_{B \rightarrow E}$
  - For her processing part,
    - by optimal time frequency phase and angular resolution capabilities on received signals (that achieve the Cramer-Rao Bounds[1]),
    - by optimal demodulation and decoding capabilities that achieve the theoretical performance[2].

A7.3- Model of "Intelligent Jamming" (IJ) or "Protocol Aware" Eve

Eve's procedures

- Partially aware of the legitimate protocol.
- Informed about dedicated sequences between Alice and Bob in signalling and in negotiation (for example the authentication protocol, the CSI protocol and the relevant messages).
- Influences the radio access protocol of legitimate users, especially at the negotiation stage.
- Deny high level services such as 3G and 4G, highest data rates, MIMO RATs enabling, etc…

[1] See for example. Harald Cramer "Mathematical Methods of Statistics", Princeton Landmarks in Mathematics, Woodward "Probability and Information Theory, with Applications to Radar" Pergamon Press ed.

[2] J. Proakis, M. Salehi "Digital Communications", 5th Edition

Eve's limits / drawbacks

- Synchronization is needed at legitimate frame/protocol/target messages.
- None of the Eve's Tx/Rx antennas are co-located neither with Bob's antennas, nor with Alice's antennas.

Eve's advantages

- Jamming only, no necessity for demodulation or modulation of Rx Tx signals.
- Jams only few messages with dedicated signals => short time, furtive, low mean power.
- No significant real time constraints (propagation time can be easily anticipated when synchronization is achieved).

Main risks for legitimate users

- Deny high security level services into 3G and 4G and force less access in less protected 2G and 3G services.
- Deny high level services such as highest data rates, MIMO RATs enabling, Channel State Information, Artificial Noise + beam Forming enabling, SKG and SC, even cipher enabling in some cases…
- Forcing into a less secure protocol then monitoring in passive mode.

Remark

- Intelligent jamming is quite simple to achieve inside public RATs. It is one of the major risks at starting communications and at negotiation stages between Alice and Bob.

"Intelligent Jamming" Eve's Model

Intelligent jamming Eve is mainly modeled:

- For her receiving part, by the classical MIMO receiver model affected with Gaussian Noise, propagation delays $\tau_{A\rightarrow E}$, $\tau_{B\rightarrow E}$ and propagation channel matrix $H_{A\rightarrow E}$ and $H_{B\rightarrow E}$.
- For her processing part, by optimal time frequency phase and angular resolution capabilities on received signals that achieve the Cramer Rao Bounds[1].
- For her transmitting part, by optimal emission of synchronized jamming signals without distortion up to a given (parameterized) Equivalent Isotropic Radiated Power (EIRP, considered at the antenna Front End.
- Intelligent Jamming Eve does not impersonate Alice or Bob: the jamming signal of Eve can be AWGN or colored Noise or modulated signals, continuous or impulsive, it can be synchronized on Alice's and Bob's received frames. Nevertheless, the IJ signal remains uncorrelated with Alice's and Bob's message content. Thus the IJ signal is interpreted at Alice and Bobs such as noise, but it is never interpreted as real messages.

A7.4- Model of "Man-In-The-Middle" Eve (MITM)

Eve's procedures

- Aware bout the complete legitimate protocol.
- Intercepts, processes, replays exchanged messages between Alice and Bob.
- Impersonate legitimate Tx (and even operators in some cases) and / or spoofs legitimate Rx messages, in order to overpass the authentication, to modify the computation of cipher keys, to force emission and/or repetition of legitimate messages, etc.

Eve's limits / drawbacks

- Very sensitive to network engineering conditions (power of impersonated BS versus power of Eve's TX.
- Very sensitive to radio conditions (receiving part of Eve), while power control of legitimate is not achieved.
- Maximal real time constraints.
- Basic MITM systems are quite indiscrete because they disrupt the roaming of the target mobile into his home or visited network when the impersonating or spoofing is partial only ("basic" IMSI catchers).
- Advanced MITM threats are very complex:
  - accurate synchronization is needed at legitimate protocol/frame/messages
  - real time demodulation and modulation of Rx Tx signals are required
- None of the Eve's Tx/Rx antennas are co-located neither with Bob's antennas, nor with Alice's antennas

Eve's advantages

- Complete control of the legitimate protocol: influences authentication, ciphering, subscriber data, can selectively deny advanced services into network access, force messages transmission and repetition, etc.

Main risks for legitimate users

- Robbery of Subscriber data (IMSI, Agendas, even subscriber K/Ki keys of terminal WAP keys in ultimate cases).
- Forcing protocol sequences: attach, location update, cell selection and handover, etc.
- Forcing transmission of messages, forcing repetition of messages.
- Full monitoring of exchanged data (access and on-going communication).
- Deny of any kind of protected communication services.

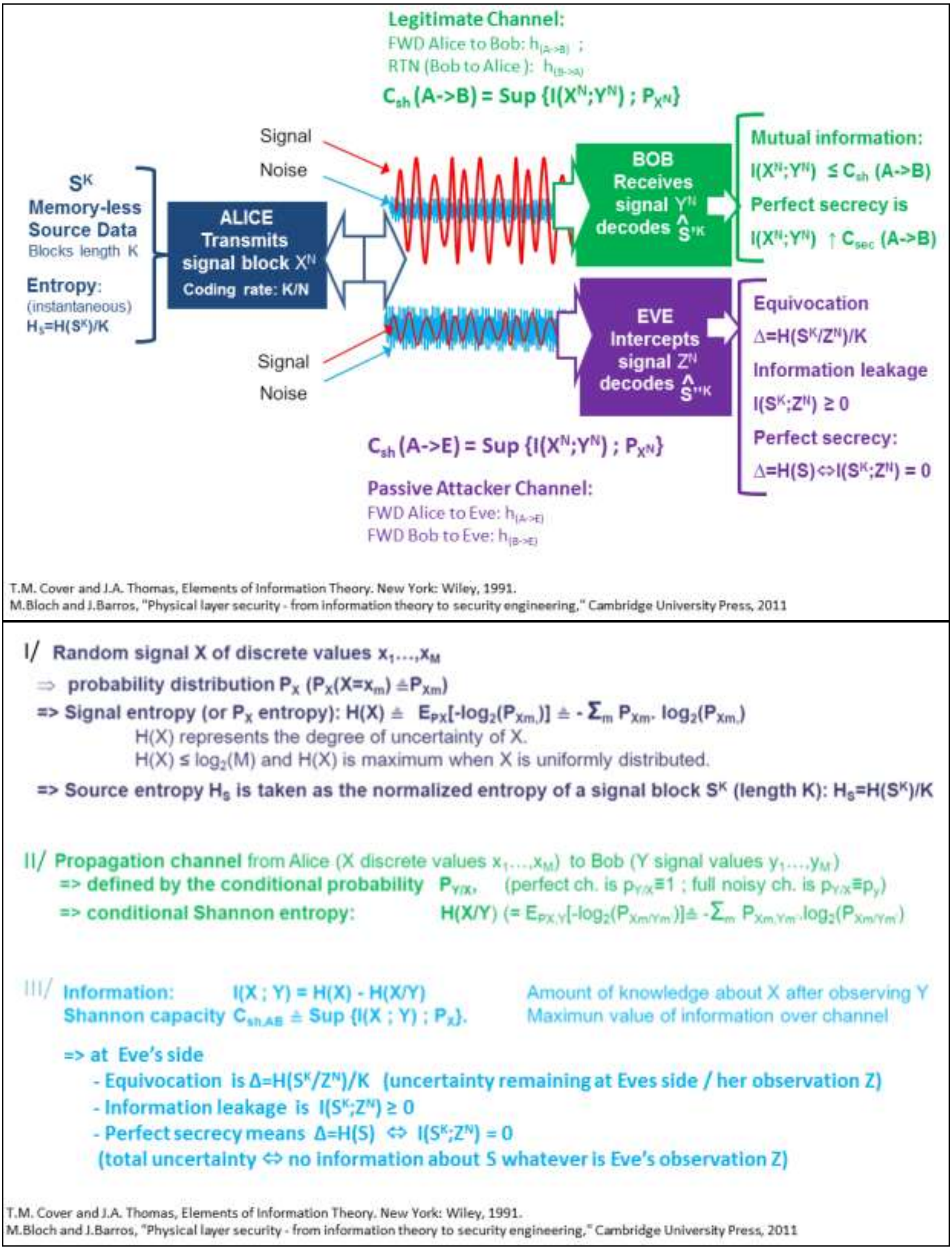
"Man In the Middle" Eve's Model

Man In the Middle Eve is mainly modeled:

- For her receiving and synchronizing part, by the classical MIMO receiver model affected with Gaussian Noise, propagation delays $\tau_{A\rightarrow E}$, $\tau_{B\rightarrow E}$ and propagation channel matrix $h_{A\rightarrow E}$ and $h_{B\rightarrow E}$
- For her processing part,
  - by optimal time frequency phase and angular resolution capabilities on received signals that achieve the Cramer Rao Bounds[1],
  - by optimal demodulation and decoding capabilities that achieve the theoretical performance[2]
- For her transmitting part, by optimal synchronized emission of coherent signals without distortion at a given parameterized Equivalent Isotropic Radiated Power (EIRP, considered at the antenna Front End.
- Man in the middle Eve tries to impersonate Alice and/or Bob: the signal of Eve is coherent and synchronized with Alice's and Bob's transmitted messages. Thus the MITM signal can be interpreted at Alice and Bob such as real messages.

Annex 8 - Theoretical notions and principles relevant to Physical Layer Security

The following figures provide a synthesis of the main key theoretical key points relevant to Physec.



Legitimate Channel:
FWD Alice to Bob: $h_{(A\text{->}B)}$;
RTN (Bob to Alice): $h_{(B\text{->}A)}$
C_{sh} (A->B) = Sup {$I(X^N;Y^N)$; P_{X^N}}

S^K
Memory-less Source Data
Blocks length K
Entropy:
(instantaneous)
$H_s=H(S^K)/K$

ALICE
Transmits signal block X^N
Coding rate: K/N

BOB
Receives signal Y^N
decodes $\hat{S}'^K$

Mutual information:
$I(X^N;Y^N) \leq C_{sh}$ (A->B)
Perfect secrecy is
$I(X^N;Y^N) \uparrow C_{sec}$ (A->B)

EVE
Intercepts signal Z^N
decodes $\hat{S}''^K$

Equivocation
$\Delta=H(S^K/Z^N)/K$
Information leakage
$I(S^K;Z^N) \geq 0$
Perfect secrecy:
$\Delta=H(S) \Leftrightarrow I(S^K;Z^N) = 0$

C_{sh} (A->E) = Sup {$I(X^N;Y^N)$; P_{X^N}}

Passive Attacker Channel:
FWD Alice to Eve: $h_{(A\text{->}E)}$
FWD Bob to Eve: $h_{(B\text{->}E)}$

T.M. Cover and J.A. Thomas, Elements of Information Theory. New York: Wiley, 1991.
M.Bloch and J.Barros, "Physical layer security - from information theory to security engineering," Cambridge University Press, 2011

I/ Random signal X of discrete values $x_1,\dots,x_M$

⇒ probability distribution P_X ($P_X(X=x_m) \triangleq P_{Xm}$)

=> Signal entropy (or P_X entropy): $H(X) \triangleq E_{PX}[-\log_2(P_{Xm})] \triangleq -\Sigma_m P_{Xm}.\log_2(P_{Xm})$

H(X) represents the degree of uncertainty of X.
$H(X) \leq \log_2(M)$ and H(X) is maximum when X is uniformly distributed.

=> Source entropy H_s is taken as the normalized entropy of a signal block S^K (length K): $H_s=H(S^K)/K$

II/ Propagation channel from Alice (X discrete values $x_1,\dots,x_M$) to Bob (Y signal values $y_1,\dots,y_M$)
=> defined by the conditional probability $P_{Y/X}$, (perfect ch. is $p_{Y/X}\equiv 1$; full noisy ch. is $p_{Y/X}\equiv p_y$)
=> conditional Shannon entropy: $H(X/Y)$ (= $E_{PX,Y}[-\log_2(P_{Xm/Ym})] \triangleq -\Sigma_m P_{Xm,Ym}.\log_2(P_{Xm/Ym})$)

III/ Information: $I(X ; Y) = H(X) - H(X/Y)$ Amount of knowledge about X after observing Y
Shannon capacity $C_{sh,AB} \triangleq$ Sup {$I(X ; Y)$; P_x}. Maximun value of information over channel

=> at Eve's side
- Equivocation is $\Delta=H(S^K/Z^N)/K$ (uncertainty remaining at Eves side / her observation Z)
- Information leakage is $I(S^K;Z^N) \geq 0$
- Perfect secrecy means $\Delta=H(S) \Leftrightarrow I(S^K;Z^N) = 0$
(total uncertainty ⇔ no information about S whatever is Eve's observation Z)

T.M. Cover and J.A. Thomas, Elements of Information Theory. New York: Wiley, 1991.
M.Bloch and J.Barros, "Physical layer security - from information theory to security engineering," Cambridge University Press, 2011

Figure 32: wiretap channel, entropy mutual information and capacity

IV/ Perfect secrecy can be achieved with secret codes $\Delta = H_S \Leftrightarrow I(S^K;Z^N) \equiv 0$

=> Secrecy capacity $C_{sec}(A\text{->}B/E)$ achieves Max {$I(X^N;Y^N)$
over X distribution P_X and over constraint $\Delta = H_S$

=> In practice achieving secrecy requires a "radio-channel advantage", i.e. :
$C_{sh}(A\text{->}B) > C_{sh}(A\text{->}E)$ (AWGN case : $SNR_B > SNR_E$)

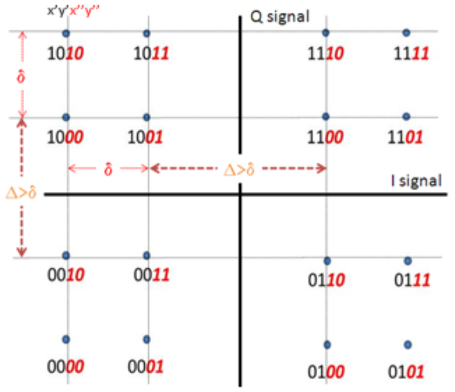
=> under the previous conditions and some symmetry assumptions
$C_{sec}(A\text{->}B/E) = C_{sh}(A\text{->}B) - C_{sh}(A\text{->}E)$
$\leq C_{sh}(A\text{->}B)$

=> Existence of secrecy codes is proven,
but proof is not constructive

=> the key for achieving secrecy coding is
- the existence of subcodes in the channel codes
- the suitable mapping of bits to be protected

Illustration of (weak) secrecy (QAM)

16 QAM symbol = 4 bits x'y'x'' y'' beeing "0" ou "1"
Worst protected bits : x' y' quadran designation
Best protected bits : x'' y'' symbol in the quadran



Aaron Wyner. The Wire-Tap Channel". In: Bell Syst. Tech. J. 54.8 (Oct. 1975), pp. 1355{1387).
Leung Yan Cheong and Martin Hellman. \The Gaussian Wire-Tap Channel". In: IEEE Trans. Inform. Theory 24 (1978), pp. 451{456.
Frederique Oggier, Patrick Sole, and Jean-Claude Belore. \Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis". Mar. 2011.

V/ Secret keys of significant length can be generated

=> known Channel Quantization Algorithm (CQA)
based on RSSI (Received Signal Strength Indication)
based on CSI (Channel State Information) : ampl. and phase of paths

⇒ Number of generated bits:

$$I_K = I\left(h_{(A\to B)}\,;h_{(B\to A)}\right)$$

in case of reciprocal channels
$(h_{(A\to B)} = h_{(B\to A)})$, $\mathrm{I_K} = \mathrm{H}(\mathrm{h}_{A\to B})$

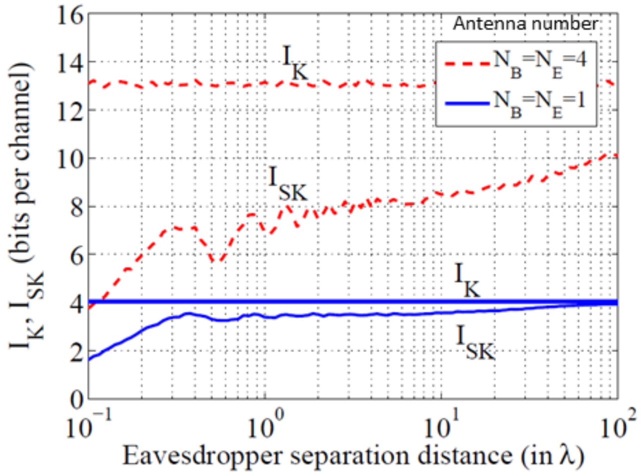
⇒ Number of secure bits:

$$I_{SK} = I(h_{A\to B}\,;h_{B\to A}|\mathrm{h}_{A\to E}, h_{B\to E})$$

⇒ Number of non-secure bits:

$$I_{VK} = I_K - I_{SK}$$

Illustration of SKG scenario with « disk distributed scatters »



U.Maurer, "Secret key agreement by public discussion from common information," IEEE Transactions on Information Theory, 1993, pp. 733-742.
J. Wallace and R. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: measurement and analysis," IEEE Trans. Inf. Forensics and Security, vol. 5, no. 3, pp. 381-392, Sep. 2010.

Figure 33: main theoretical principles relevant to the existence of Secret Codes and to the Generation of Secret Keys