PROJECT PHYLAWS
FINAL REPORT

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/

4.1 Final publishable summary report

4.1.1 Executive Summary

Wireless communications have become a universal way to access information for nearly every human around the world. This domination also presents major risks to society, owing to the widely recognized leaks and unsafe technologies in the current wireless networks. Basically all of the security today relies on bit level cryptographic techniques and associated protocols at various levels of the data processing stack, but these solutions have drawbacks and they are often not sufficiently secure. This difficulty is a major retarder to the progress of the digital society.

In the recent years therefore, new approaches have been investigated in order to exploit security opportunities offered by the handling signals operating at the physical layer level. These works have been based on a fundamental analysis of the notion of security in the context of information theory.

The PHYLAWS project intended to elaborate on this knowledge basis in order to develop focused and synthetic ways to benefit from wireless physical layer opportunities in order to enhance the security of wireless communications in an affordable, flexible and efficient manner. The project outputs will thus benefit to a variety of existing and future standards for a large set of needs.

This objective has been reached through a suitably sized consortium combining an excellent academic expertise 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 for the development and test of several competing techniques; a SME involvement perfectly aligned with the application targets; and a strong industrial involvement highly motivated by security in wireless networks as a manufacturer, as an end-user and as a provider of wireless communication services. The complementary skills inside the consortium ensured both innovation and impact towards industrial applications, and they assessed validation of the commercial goals and validation of the society use relevance.

In addition, the project took many benefits from recommendations and advices by an international Advisory Board (AB), constituted of very high level personalities from governmental bodies, standardization bodies or academia. This Board was one of the cornerstones of the project, based on the recognition that excellent technical developments and demonstrations were not enough to ensure their wide spreading. Clearly, the project impact has largely benefit from a proper vision, aided by the AB, in order to penetrate standards and existing systems and ensure support from the major stakeholders.

Ultimately, the convincing feasibility proofs and the intensive dissemination and standardization performed in PHYLAWS have contributed to facilitate the penetration of wireless technologies in the personal and professional sphere, by guaranteeing a more efficient safe access to the digital world through the future internet. In the following years, the achievements of the project will strongly impact the lives of citizens and will very much contribute to trustworthy ICT.

4.1.2 Summary description of project context and objectives

Project's Context:

Phylaws considered 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: simple to implement, requiring easily developed and easily validated algorithms, but also less spectrum resource and less energy consuming.

Project's Objectives:

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

- easy to develop and to validate
- convenient to embed and 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).

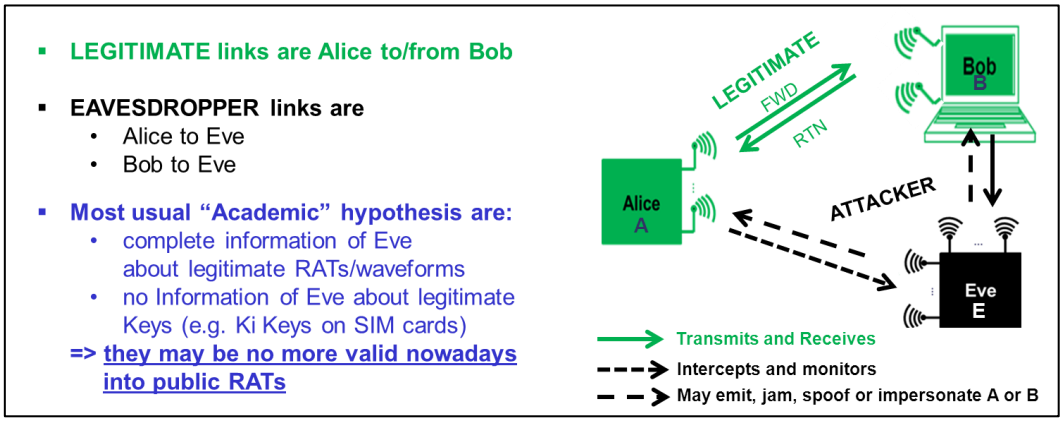


Figure 1: security issues studied by Phylaws - Illustration of the wiretap channel and several kinds of threats

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

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

All partners involved in the project were chosen for their high values skills and complementary competences. This complementarity ensured both innovation and impact towards stakeholders, 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.

Project's basis and achievements:

For an efficient leadership of developments and evaluations of the secure schemes in the project, the Phylaws team based its researches on:

- 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 studies of 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 three patented key-free secure schemes and relevant metrics.

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
    - 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.

4.1.3 Description of the main S&T results/foregrounds

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, patented and experimented three key-free security 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 to enhance privacy of subscribers, and confidentiality of user communication into on-going traffic messages, 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

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.

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 2 - 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 2 - A part. The choice of thee TS sequence from the channel measurement uses a simplified quantization algorithm without any public exchange
- 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.

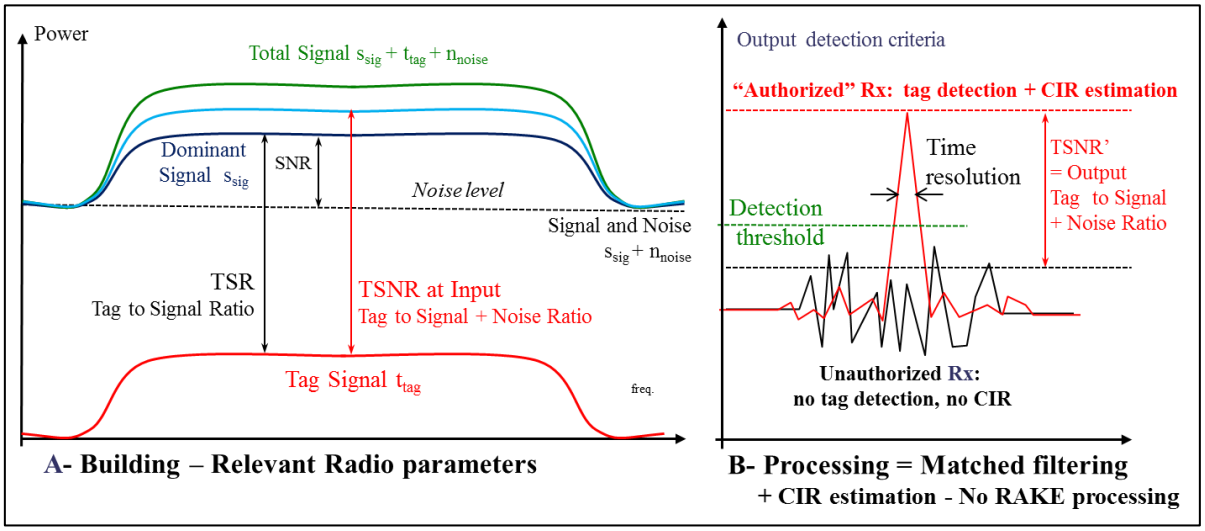


Figure 2: tag signals - configuration of transmission, reception and processing

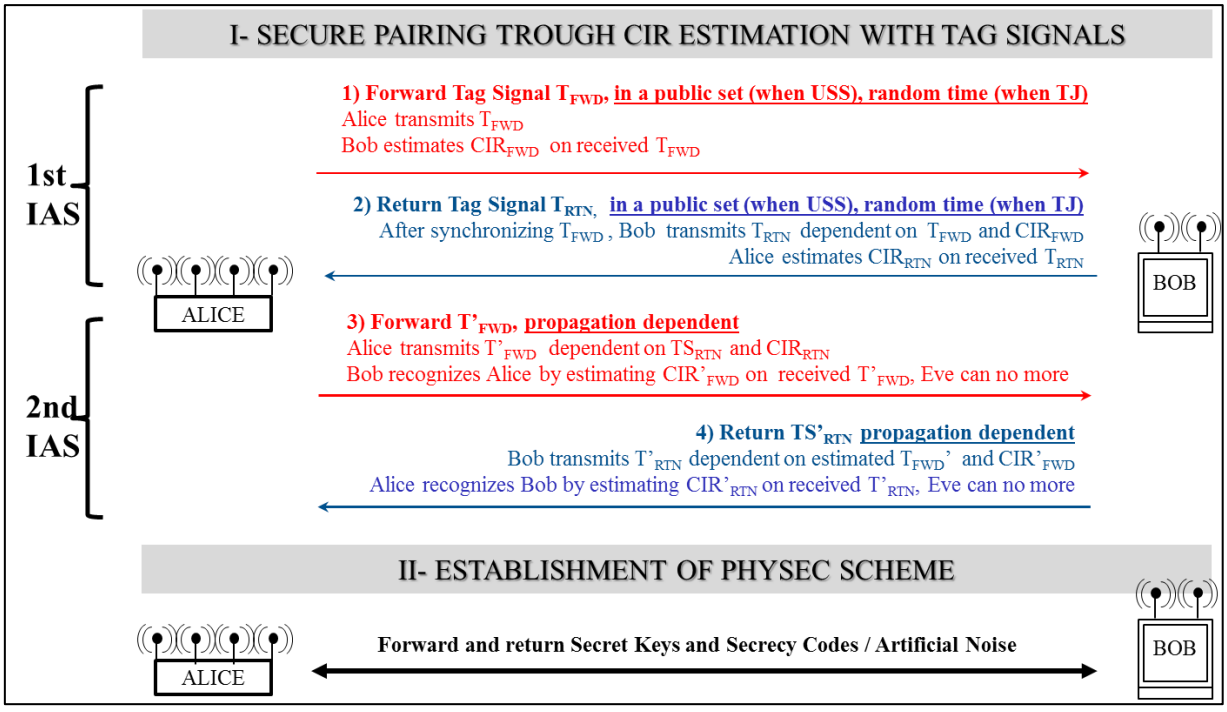


Figure 3: synthesis of the IAS protocol supported by Tag Signals (TS)

Feasibility proof and resilience analysis of Secure Pairing in simplified laboratory environment

Phylaws achieved the feasibility proof of some of the key items of the SP scheme by combining laboratory tests and simulation inputs from real field records from the Wifi test bed:

- capability of defining sets of arbitrary random Tag Signals of significant number and correlation quality
- capability to achieve protection level with Tag Signals which period and spreading factor match the frame length of radio standards
- 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 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, and that are intensively studied for spectrum efficiency enhancements.

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.

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 4 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.

While theoretical foundations of SKG are well described in the literature, we developed during the Phylaws project a complete embeddable SKG scheme with the following key enhancements (see Figure 5):

- 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 6.
- 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 in 2010 by 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.

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

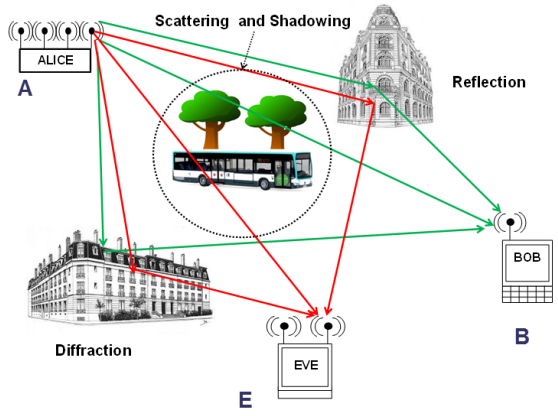
III- At fixed carrier, same angles on obstacles for Alice → Bob and for Bob → Alice

- 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)

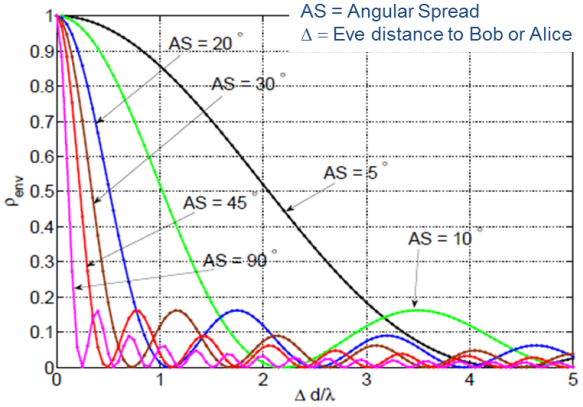


Figure 4: physical foundations of the usage of the radio propagation channel as a private source of randomness This key-free secure scheme is very useful to enhance the protection of clear text signaling and access messages that include sensitive data in most of public radio-networks.

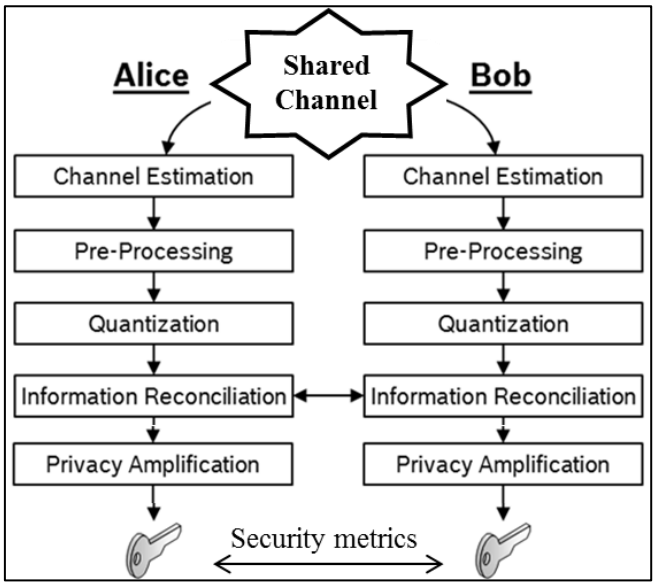


Figure 5: illustration of the SKG algorithm blocks developed and experimented into the Phylaws project

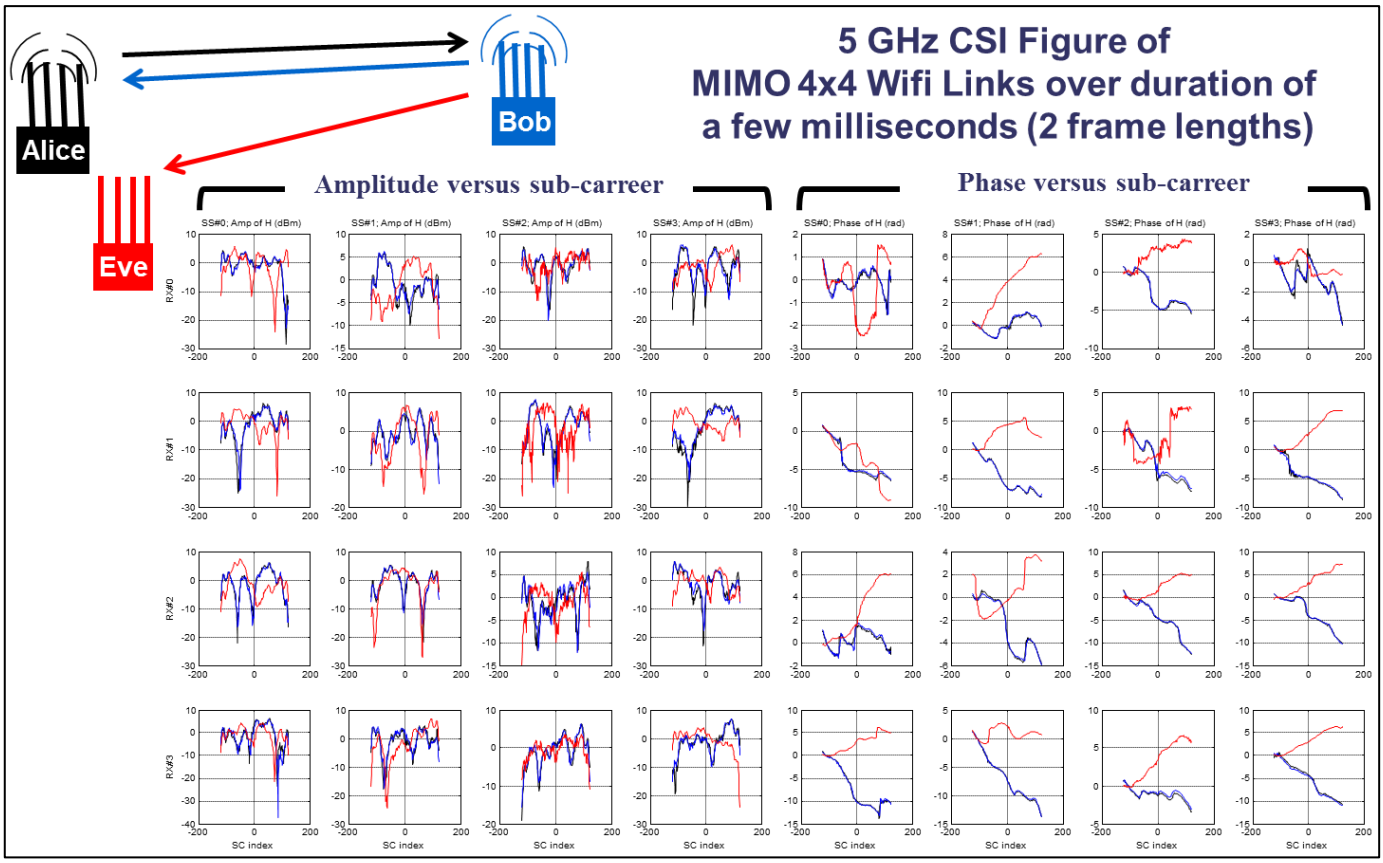


Figure 6: illustration of CSI reciprocity and diversity at the 5 GHz Wi-Fi band: case of CSI in indoor environment. 4x4 MIMO transmitter receiver and eavesdropper over short term duration (a few milliseconds) – Eve-Alice distance is about ten wavelengths (60 cm) - slight mobility of scatterers

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 7) 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 apply very well at the end of the SKG processing.

Thus, after patenting the invented SKG scheme, 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.

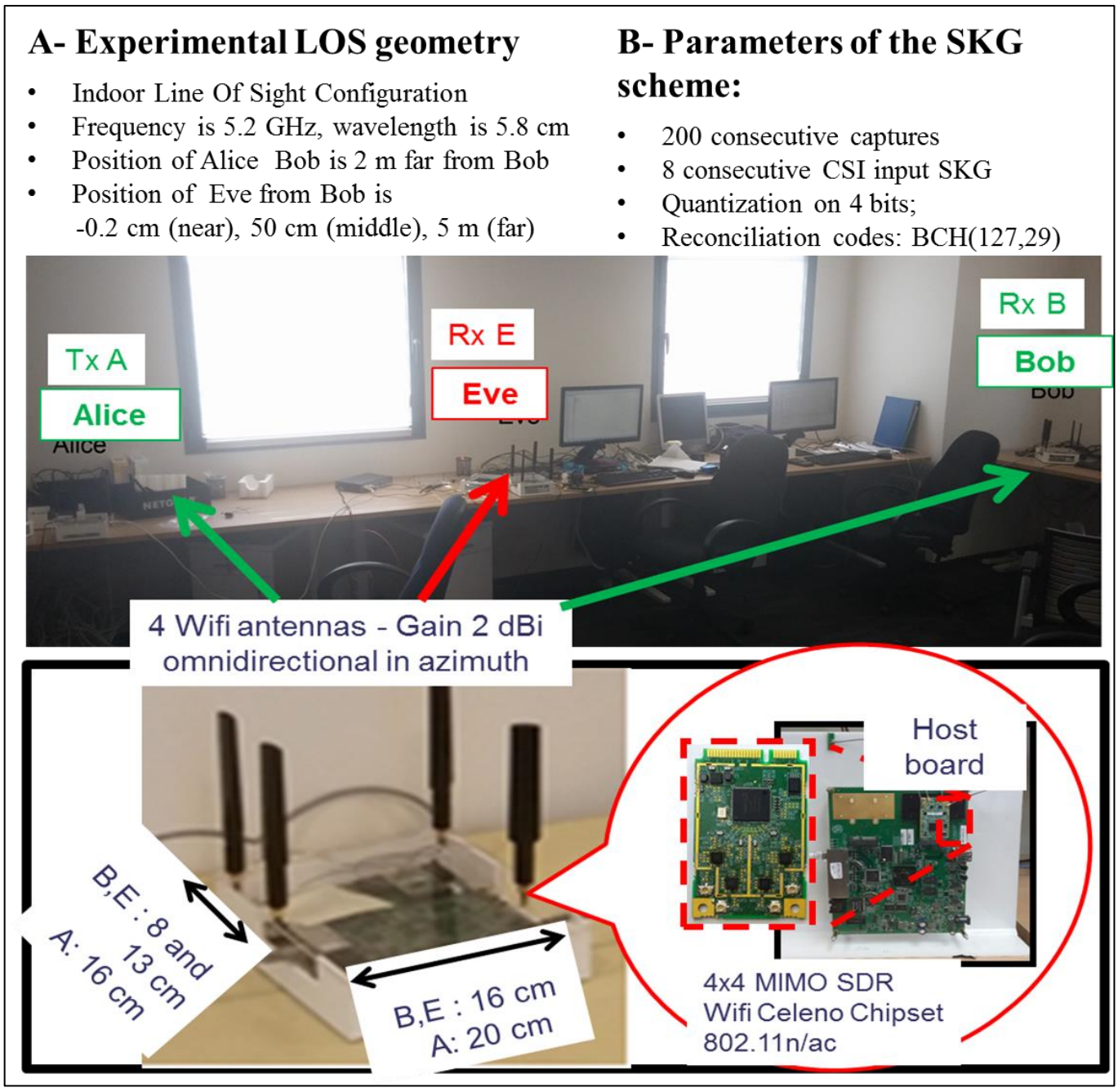


Figure 7: example of geometry for the SKG experiments

Finally, we can consider at the end of Phylaws 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 geometry described Figure 7, Figure 8 illustrates some of the experimental results of our SKG schemes.

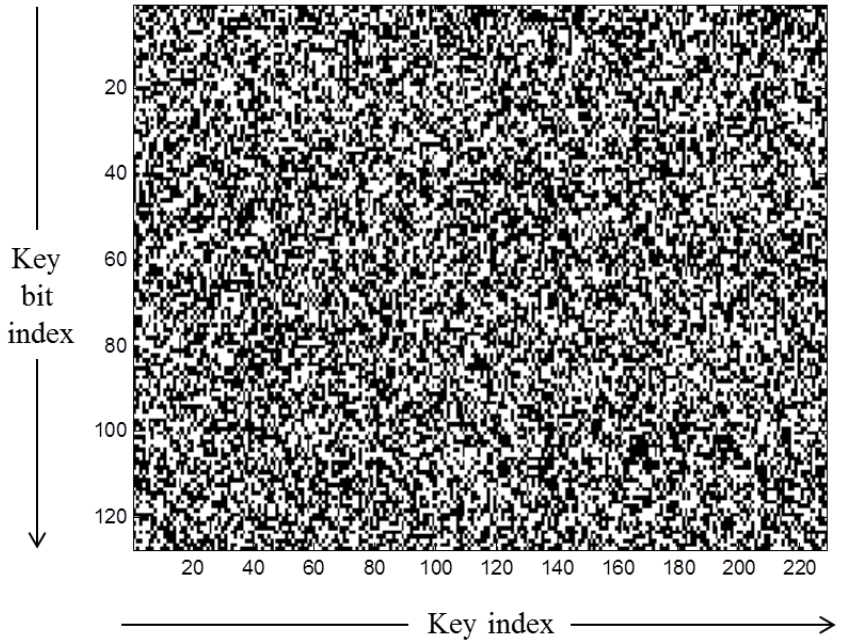


Figure 8: illustration of keys randomness output by the SKG schemes (228 Keys of 127 bits each)

Secrecy Coding (SC):

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).

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 9.

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 by the scientific literature. 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.

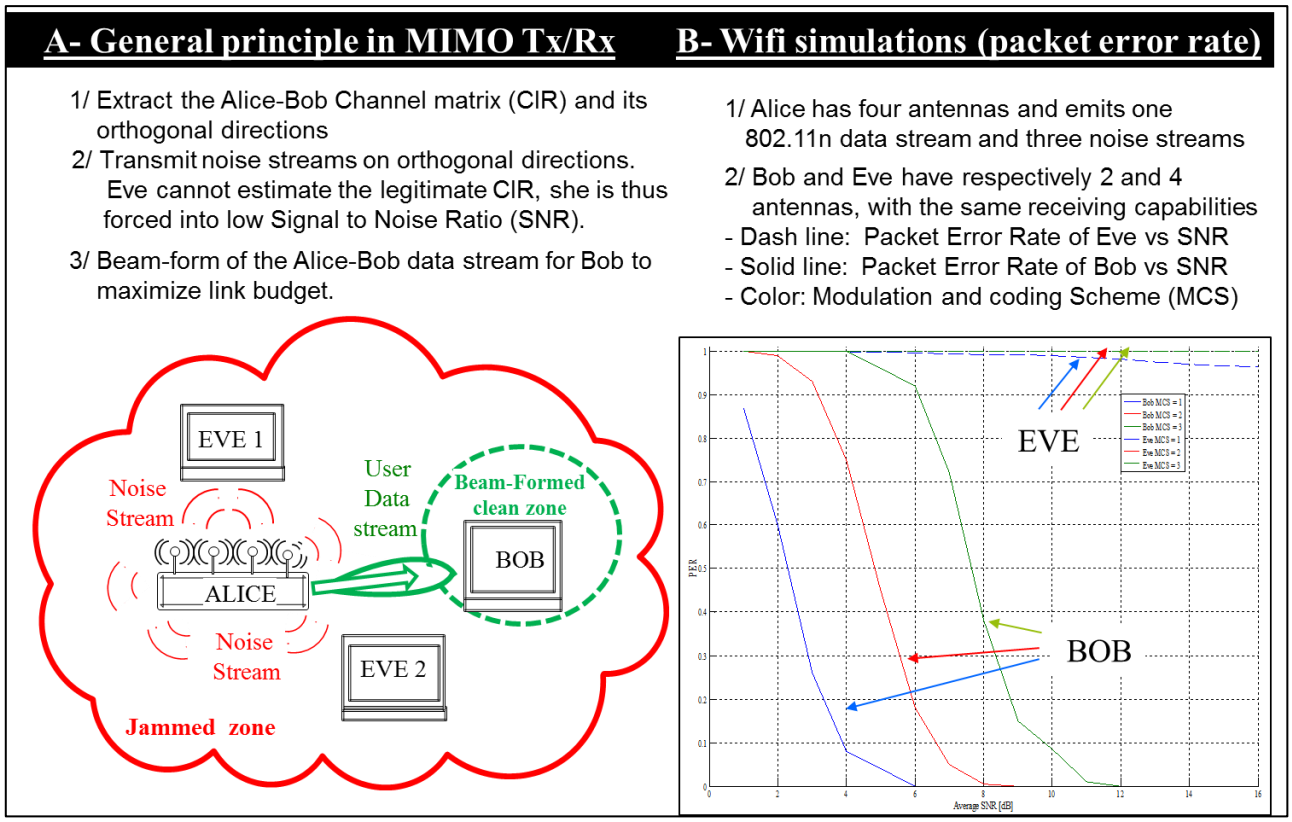


Figure 9: creating a radio advantage with Artificial Noise and Beam-Forming

Inspired by academic results on polar codes that have been proven to provide strong security for discrete channels, 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 10 - 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.

As shown in Figure 10 – 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 10 – 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 10 – 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 10 – B, the BER at the output of the outer decoder is 5*10-5, what leads to perfectly decoded user data as shown Figure 10 – 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.

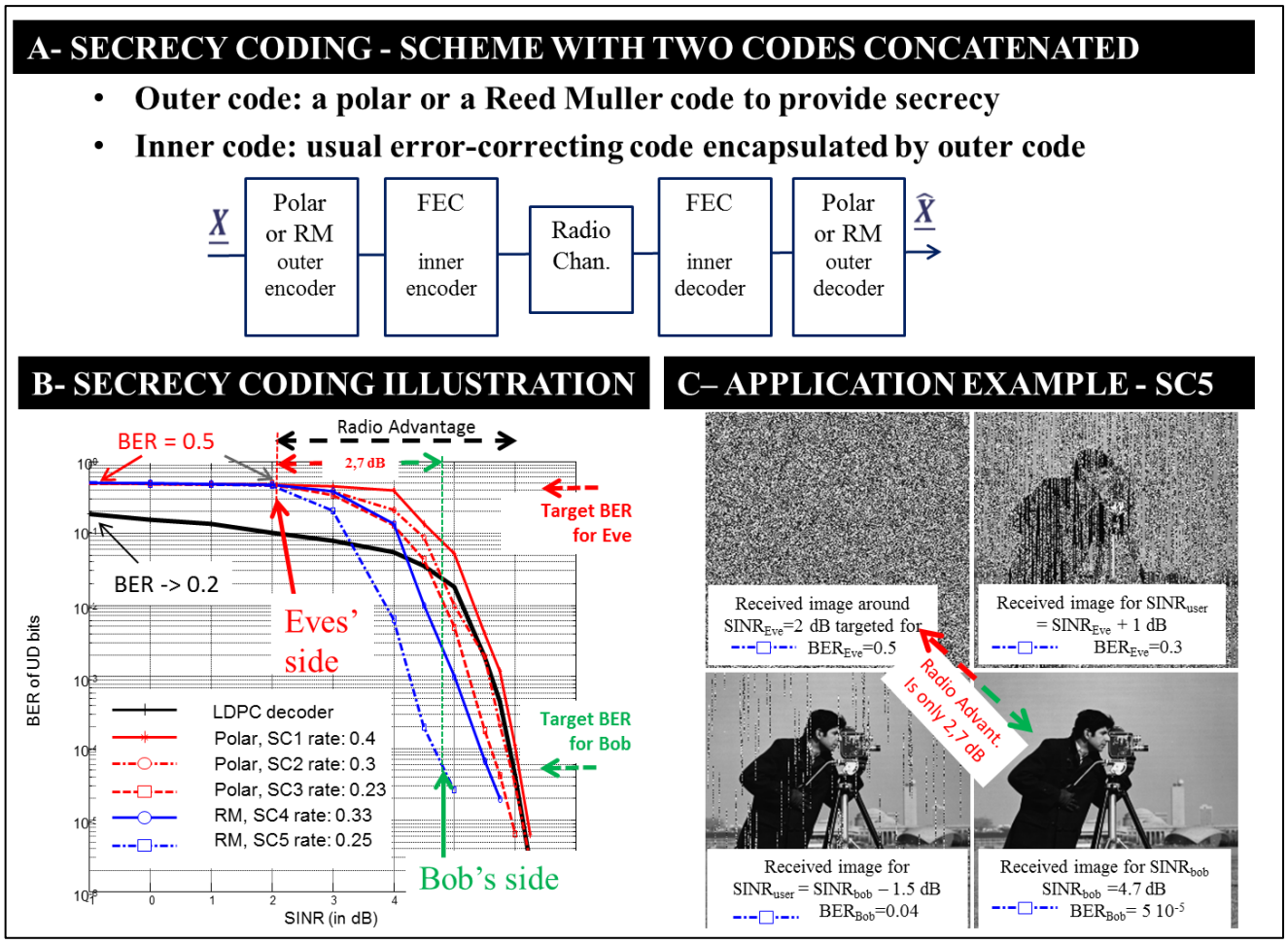


Figure 10: design of the secrecy coding schemes invented by the Phylaws project

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 11) 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 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).
- 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.

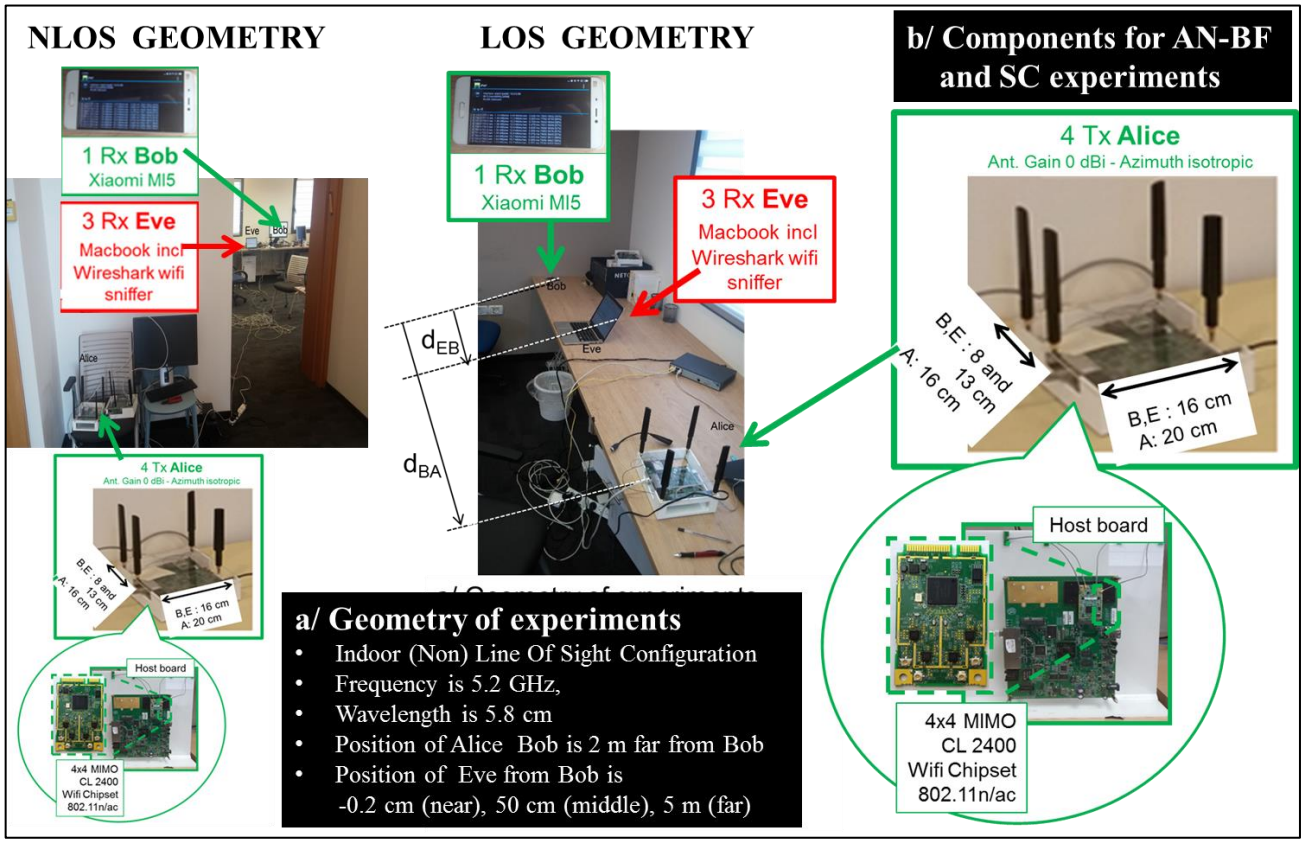


Figure 11: example of experimental configuration of AN-BF and SC on Wi-Fi 2.4 and 5 GHz links

Finally, we can consider at the end of Phylaws 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 11, Figure 12 illustrates some of the experimental results of our SC scheme (built in this case with outer nested polar codes).

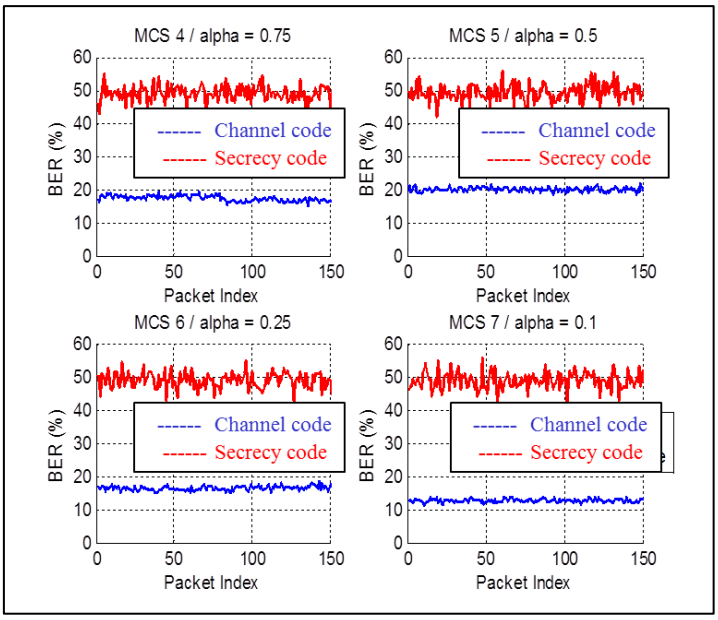


Figure 12: example of experimental BER of channel codes and secrecy codes built with outer nested polar codes applied with AN-BF Wi-Fi 5 GHz links, where Eve is close to Bob and Alice in Non Light of Sight geometry

4.1.4 Potential impact

Global Impact of the project

Figure 13 hereafter synthetizes the major scientific and technical achievements of the project relevant to the three patented secured schemes mentioned in section above.

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**. ($RA \approx SIR_{Alice} - SINR_{Bob}$) 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 13: synthesis of the major scientific and technical achievements of the Phylaws project

Significant results of dissemination activities

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.

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 and reachable at the following URL: http://www.phylaws-ict.org/?page_id=58.

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. 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.

Networking – Collaboration with other projects

During the Phylaws project, several contacts with projects such as Duplo, Prophylaxe and 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.

Patent and IPR strategy of the project (see also section 4.2)

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
- The second one focuses on Secret Key Generation
- The third one focuses on Secrecy Coding under radio advantage of Bob to Eve.

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.

4.1.5 Addresses of the project public website

The Phylaws public web site is reachable at URL = www.phylaws-ict.org/

Deliverables can be uploaded at URL = http://www.phylaws-ict.org/?page_id=48

Dissemination initiatives and reports are reachable at URL = http://www.phylaws-ict.org/?page_id=92

Standardization initiatives and reports are reachable at URL = http://www.phylaws-ict.org/?page_id=58

The partners' 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 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.

4.2 Use and dissemination of foreground

Section A (public)

TEMPLATE A1: LIST OF SCIENTIFIC (PEER REVIEWED) PUBLICATIONS, STARTING WITH THE MOST IMPORTANT ONES

NO.	Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers[1] (if available)	Is/Will open access[2] provided to this publication?
1	Application cases of Secret key generation in communication nodes and terminals"	*C.L. Kameni*	IET Book "Trusted Communications with Physical Layer Security for 5G and Beyond"	-	*IET Book Trung Q. Duong*	*China Worldwide*	*2017*	*Chapter 19*	http://www.phylaws-ict.org/?page_id=92	yes
2	Application cases of Secrecy Coding in communication nodes and terminals"	*C.L. Kameni*	IET Book "Trusted Communications with Physical Layer Security for 5G and Beyond"	-	*IET Book Trung Q. Duong*	*China Worldwide*	*2017*	*Chapter 20*	http://www.phylaws-ict.org/?page_id=92	yes
3	Secret Key Generation scheme from WiFi and LTE reference signals	*C.L. Kameni*	Springer Journal Special Issue, Analog Integrated Circuits & Signal Processing	-	*Springer*	*GER USA Worldwide*	*2017*		http://www.phylaws-ict.org/?page_id=92	yes
4	Combining Artificial Noise Beam Forming And Concatenated Coding Schemes To Effectively Secure Wireless Communications	*C.L. Kameni*	Springer Journal Special Issue, Analog Integrated Circuits & Signal Processing	-	*Springer*	*GER USA Worldwide*	*2017*		http://www.phylaws-ict.org/?page_id=92	yes
5	On the Diversity of Linear Transceivers in MIMO AF Relaying Systems	*C. Song C. Ling*	IEEE Trans. Inform. Theory		*IEEE*	*Worldwide*	*2016*		IEEE Xplore http://www.phylaws-ict.org/?page_id=92	yes
6	Analysis of Secret Key Randomness Exploiting the Radio Channel Variability	*T. Mazloum A..Sibillle*	IJAP		Hindawi	*Worldwide*	*2015*		IEEE Xplore http://www.phylaws-ict.org/?page_id=92	yes
7	Semantically secure lattice codes for the Gaussian wiretap channel	*C. Ling*	IEEE Trans. Inform. Theory		*IEEE*	*Worldwide*	*2014*		IEEE Xplore http://www.phylaws-ict.org/?page_id=92	yes
8	Achieving AWGN channel capacity with lattice Gaussian coding	*C. Ling J.C. Belfiore*	IEEE Trans. Inform. Theory		*IEEE*	*Worldwide*	*2014*		IEEE Xplore http://www.phylaws-ict.org/?page_id=92	yes
9	Security aspects of short-range wireless communication: Risk analysis for the healthcare application	A. Evesti J. Suomalainen	International Journal of Intelligent Computing Research (IJICR)		Infonomics Society	*Worldwide*	*2014*		http://www.phylaws-ict.org/?page_id=92	yes

[1] A permanent identifier should be a persistent link to the published version full text if open access or abstract if article is pay per view) or to the final manuscript accepted for publication (link to article in repository).

[2] Open Access is defined as free of charge access for anyone via Internet. Please answer "yes" if the open access to the publication is already established and also if the embargo period for open access is not yet over but you intend to establish open access afterwards.

TEMPLATE A2: LIST OF DISSEMINATION ACTIVITIES								
NO.	Type of activities[3]	Main leader	Title	Date/Period	Place	Type of audience[4]	Size of audience	Countries addressed
1	Article + Conference presentation	TPT	Analysis of secret key robustness in indoor radio channel measurements	*2016*	IEEE VTC Spring Glasgow, UK	Higher education, Research, Industry	IEEE Xplore *Worldwide*	Worldwide
2	Article + Conference presentation	TPT ICL	Algebraic lattices achieve the capacity of the ergodic fading channel	*2016*	IEEE ITW 2016 Cambridge, UK	Higher education, Research, Industry	IEEE Xplore *Worldwide*	Worldwide
3	Article + Conference presentation	TPT ICL	Algebraic Lattice Codes Achieve the Capacity of the Compound Block-Fading Channel	*2016*	IEEE ISIT 2016 Barcelona, Spain	Higher education, Research, Industry	IEEE Xplore *Worldwide*	Worldwide
4	Article + Conference presentation	TPT	Performance of secret key generation in non-stationary channels	*2015*	EUCAP 2015 Lisbon, Portugal	Higher education, Research, Industry	IEEE Xplore *Worldwide*	Worldwide
5	Article + Conference presentation	TPT	Ray Tracing Simulations of Indoor Channel Spatial Correlation for Physical Layer Security	*2015*	EUCAP 2015 Lisbon, Portugal	Higher education, Research, Industry	IEEE Xplore *Worldwide*	Worldwide
6	Article + Conference presentation	TPT	Analysis of Alice-Bob-Eve scenarios for secret key generation from random channels	*2014*	URSI GASS Beijing, China	Higher education, Research, Industry	IEEE Xplore *Worldwide*	Worldwide
7	Article + Conference presentation	TPT	Ray Tracing Simulations of Indoor Channel Spatial Correlation for Physical Layer Security	*2013*	COST IC1004, 14th MCM Ferrara, Italy	Higher education, Research, Industry	50 pers	Italy
8	Article + Conference presentation	TCS	Secret Key Generation scheme from WiFi and LTE reference signals	*2016*	Wincomm forum US 2016 Reston, USA Virginia	Higher education, Research, Industry	100 pers IEEE Xplore *Worldwide*	Worldwide

[3] A drop down list allows choosing the dissemination activity: publications, conferences, workshops, web, press releases, flyers, articles published in the popular press, videos, media briefings, presentations, exhibitions, thesis, interviews, films, TV clips, posters, Other.

[4] A drop down list allows choosing the type of public: Scientific Community (higher education, Research), Industry, Civil Society, Policy makers, Medias, Other ('multiple choices' is possible).

9	Article + Conference presentation	TCS	Combining Artificial Noise Beam Forming and Concatenated Coding Schemes To Effectively Secure Wireless Communications	*2016*	Wincomm forum US 2016 Reston, USA Virginia	Higher education, Research, Industry	100 pers IEEE Xplore *Worldwide*	Worldwide
10	Article + Conference presentation	TCS	Tag Signals for Early Authentication and Secret Key Generation in Wireless Public Networks	*2016*	EuCNC2015 Paris, Issy les Mx, France	Higher education, Research, Industry	10 pers IEEE Xplore *Worldwide*	Worldwide
11	Article + Conference presentation	TCS	Perspectives of Physec for the improvement of the subscriber privacy and communication confidentiality at the Air Interface . Results for WLANs, IoT and radiocell	*2016*	"ETSI WS on fut. radio techn. Air Interface. Sofia.Antipolis, France	Higher education, Research, Industry	200 pers IEEE Xplore *Worldwide*	Worldwide
12	Article + Conference presentation	VTT	Security risks in the short-range communication of ubiquitous application	*2013*	International Conference for Internet Technology and Secured Transactions London, UK	Higher education, Research, Industry	10 pers IEEE Xplore *Worldwide*	Worldwide
13	Article + Conference presentation	VTT	Security pairings using physical layer properties of wireless communications	*2014*	International Conference on Privacy and Security in Mobile Systems Aarlborg, Denmark	Higher education, Research, Industry	10 pers IEEE Xplore *Worldwide*	Worldwide
…	…	…	…	…	…	…	…	…
14	PhD Dissertation and report	TPT	Lattice Codes for the Continuous Wiretap Channels	*2014*	Telecom Paris Tech Hamed Mirghasemi	Higher education, Research,	50 pers.	Paris, France
15	PhD Dissertation and report	TPT	Analysis and modeling of the radio-channel for Secret Key Generation	2016	Telecom Paris Tech Taghrid Mazloum	Higher education, Research,	50 pers.	Paris, France
…	…	…	…	…	…	…	…	…
16	WORKSHOP	ICL TPT	Analysis and modeling of the radio-channel for Secret Key Generation	2013	Special session at PIMRC 2013	Scientific + industry,	50 pers.	London, UK
17	WORKSHOP	TCS	Deployment perspectives of Physical Layer Security into wireless public RATs	2016	Special Workshop at PIMRC 2016	Scientific + industry,	50 pers.	Valencia, Spain
…	…	…	…	…	…	…	…	…

NOTE : Numerous other publications and dissemination actions are referenced and detailed in the dissemination reports of the project:

- Deliverable D1.6 “Dissemination planning report”
- Deliverable D1.7, “Dissemination intermediate report”
- Deliverable D1.8 “Dissemination final report”

All these deliverables can be uploaded at URL = http://www.phylaws-ict.org/?page_id=48

All the publications of the project can be uploaded at URL = http://www.phylaws-ict.org/?page_id=92

Section B (Confidential[5] or public: confidential information to be marked clearly)
Part B1

TEMPLATE B1: LIST OF APPLICATIONS FOR PATENTS, TRADEMARKS, REGISTERED DESIGNS, ETC.					
Type of IP Rights[6]:	Confidential Click on YES/NO	Foreseen embargo date dd/mm/yyyy	Application reference(s)	Subject or title of application	Applicant (s) (as on the application)
Patent	NO	29/12/2015	1502713	PROCEDE D'ASSOCIATION UNIVALENTE ET UNIVOQUE ENTRE EMETTEURS ET RECEPTEURS DE TRANSMISSION A PARTIR DU CANAL DE PROPAGATION	THALES TEKNOLOGIAN TUTKIMUSKESKUS VTT-OY
Patent	NO	29/12/2015	1502712	PROCEDE D'EXTRACTION UNIVALENTE ET UNIVOQUE DE CLES A PARTIR DU CANAL DE PROPAGATION	THALES TELECOM ParisTech, CELENO COMMUNICATION LTD
Patent	NO	29/12/2015	1502710	PROCEDE DE CODAGE UNIVOQUE ET SECRET DE TRANSMISSION SUR UN CANAL DE PROPAGATION A AVANTAGE DE CAPACITE	THALES TELECOM PARIS TECH, IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

In addition to the tables above and below, the text below explains the exploitable foreground relevant to the three patents 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].

[5] Note to be confused with the "EU CONFIDENTIAL" classification for some security research projects.

[6] A drop down list allows choosing the type of IP rights: Patents, Trademarks, Registered designs, Utility models, Others.

Part B2

Type of Exploitable Foreground[7]	Description of exploitable foreground	Confidential Click on YES/NO	Foreseen embargo date dd/mm/yyyy	Exploitable product(s) or measure(s)	Sector(s) of application[8]	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner & Other Beneficiary(s) involved
Patent	1502713	NO	29/12/2015	RADIO COMMUNICATIONS NODES AND TERMINALS	INDUSTRIALS AND OPERATORS OF RADIO NETWORKS	**2020**		THALES TEKNOLOGIAN TUTKIMUSKESKUS VTT-OY
Patent	1502712	NO	29/12/2015	RADIO COMMUNICATIONS NODES AND TERMINALS	INDUSTRIALS AND OPERATORS OF RADIO NETWORKS	**2020**		THALES TELECOM ParisTech, CELENO COMMUNICATION LTD
Patent	1502710	NO	29/12/2015	RADIO COMMUNICATIONS NODES AND TERMINALS	INDUSTRIALS AND OPERATORS OF RADIO NETWORKS	**2020**		THALES TELECOM PARIS TECH, IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

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.

[19] A drop down list allows choosing the type of foreground: General advancement of knowledge, Commercial exploitation of R&D results, Exploitation of R&D results via standards, exploitation of results through EU policies, exploitation of results through (social) innovation.

[8] A drop down list allows choosing the type sector (NACE nomenclature) : http://ec.europa.eu/competition/mergers/cases/index/nace_all.html

4.3 Report on societal implications

A General Information *(completed automatically when **Grant Agreement number** is entered.*

Grant Agreement Number:	317562
Title of Project:	PHYsical LAyer Wireless Security
Name and Title of Coordinator:	François Delaveau, Senior Expert Engineer, TCS

B Ethics

1. Did your project undergo an Ethics Review (and/or Screening)? • If Yes: have you described the progress of compliance with the relevant Ethics Review/Screening Requirements in the frame of the periodic/final project reports? Special Reminder: the progress of compliance with the Ethics Review/Screening Requirements should be described in the Period/Final Project Reports under the Section 3.2.2 *'Work Progress and Achievements'*	***NO***
2. Please indicate whether your project involved any of the following issues (tick box) :	***YES***
RESEARCH ON HUMANS	
• Did the project involve children?	***NO***
• Did the project involve patients?	***NO***
• Did the project involve persons not able to give consent?	***NO***
• Did the project involve adult healthy volunteers?	***NO***
• Did the project involve Human genetic material?	***NO***
• Did the project involve Human biological samples?	***NO***
• Did the project involve Human data collection?	***NO***
RESEARCH ON HUMAN EMBRYO/FOETUS	
• Did the project involve Human Embryos?	***NO***
• Did the project involve Human Foetal Tissue / Cells?	***NO***
• Did the project involve Human Embryonic Stem Cells (hESCs)?	***NO***
• Did the project on human Embryonic Stem Cells involve cells in culture?	***NO***
• Did the project on human Embryonic Stem Cells involve the derivation of cells from Embryos?	***NO***
PRIVACY	
• Did the project involve processing of genetic information or personal data (eg. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)?	***NO***
• Did the project involve tracking the location or observation of people?	***NO***
RESEARCH ON ANIMALS *NO*	
• Did the project involve research on animals?	***NO***
• Were those animals transgenic small laboratory animals?	***NO***
• Were those animals transgenic farm animals?	***NO***
• Were those animals cloned farm animals?	***NO***
• Were those animals non-human primates?	***NO***
RESEARCH INVOLVING DEVELOPING COUNTRIES	
• Did the project involve the use of local resources (genetic, animal, plan, etc.)?	***NO***
• Was the project of benefit to local community (capacity building, access to healthcare, education etc)?	***NO***
DUAL USE	
• Research having direct military use	***NO***

• Research having the potential for terrorist abuse	***NO***

C Workforce Statistics

3. Workforce statistics for the project: Please indicate in the table below the number of people who worked on the project (on a headcount basis).

Type of Position	**Number of Women**	**Number of Men**
Scientific Coordinator	0	1
Work package leaders	0	5
Experienced researchers (i.e. PhD holders)	0	4
PhD Students	1	1
Other	2	2

4. How many additional researchers (in companies and universities) were recruited specifically for this project?	**2**
Of which, indicate the number of men:	1

D Gender Aspects

5. Did you carry out specific Gender Equality Actions under the project?

☺ Yes
○ No

6. Which of the following actions did you carry out and how effective were they?

	Not at all effective				Very effective
❑ Design and implement an equal opportunity policy	○	○	○	☺	○
❑ Set targets to achieve a gender balance in the workforce	○	○	😐	○	○
❑ Organise conferences and workshops on gender	○	○	😐	○	○
❑ Actions to improve work-life balance	○	○	○	☺	○

○ Other:

7. Was there a gender dimension associated with the research content – i.e. wherever people were the focus of the research as, for example, consumers, users, patients or in trials, was the issue of gender considered and addressed?

○ Yes- please specify

☺ No

E Synergies with Science Education

8. Did your project involve working with students and/or school pupils (e.g. open days, participation in science festivals and events, prizes/competitions or joint projects)?

☺ Yes- please specify: 2 PhD Thesis

○ No

9. Did the project generate any science education material (e.g. kits, websites, explanatory booklets, DVDs)?

☺ Yes- please specify: Website with complete information

○ No

F Interdisciplinarity

10. Which disciplines (see list below) are involved in your project?

○ Main discipline[9]: radio-communications and information theory.

○ Associated discipline[9]: coding

○ Associated discipline[9]: applied mathematics

G Engaging with Civil society and policy makers

11a Did your project engage with societal actors beyond the research community? *(if 'No', go to Question 14)*

☺ Yes
○ No

11b If yes, did you engage with citizens (citizens' panels / juries) or organised civil society (NGOs, patients' groups etc.)?

○ No

☺ Yes- in determining what research should be performed

○ Yes - in implementing the research

[9] Insert number from list below (Frascati Manual).

☺ Yes, in communicating /disseminating / using the results of the project

11c In doing so, did your project involve actors whose role is mainly to organise the dialogue with citizens and organised civil society (e.g. professional mediator; communication company, science museums)?	○ ☺	Yes No

12. Did you engage with government / public bodies or policy makers (including international organisations)

- ○ No
- ○ Yes- in framing the research agenda
- ○ Yes - in implementing the research agenda
- ○ Yes, in communicating /disseminating / using the results of the project

13a Will the project generate outputs (expertise or scientific advice) which could be used by policy makers?

- ☺ Yes – as a **primary** objective (please indicate areas below- multiple answers possible)
- ○ Yes – as a **secondary** objective (please indicate areas below - multiple answer possible)
- ○ No

13b If Yes, in which fields? Research and Innovation , Information Society

Agriculture		Energy		Human rights	
Audiovisual and Media		Enlargement		Information Society	
Budget		Enterprise		Institutional affairs	
Competition		Environment		Internal Market	
Consumers		External Relations		Justice, freedom and security	
Culture		External Trade		Public Health	
Customs		Fisheries and Maritime Affairs		Regional Policy	
Development Economic and Monetary Affairs		Food Safety		Research and Innovation	
		Foreign and Security Policy		Space	
Education, Training, Youth		Fraud		Taxation	
Employment and Social Affairs		Humanitarian aid		Transport	

13c If Yes, at which level?

- ○ Local / regional levels
- ○ National level
- ○ European level
- ☺ International level

H Use and dissemination

14. How many Articles were published/accepted for publication in peer-reviewed journals?	**More than 10**
To how many of these is open access[10] provided?	**All are open access via the project web site**
How many of these are published in open access journals?	
How many of these are published in open repositories?	**All via the project website**
To how many of these is open access not provided?	-
Please check all applicable reasons for not providing open access:	-
❑ publisher's licensing agreement would not permit publishing in a repository ❑ no suitable repository available ❑ no suitable open access journal available ❑ no funds available to publish in an open access journal ❑ lack of time and resources ❑ lack of information on open access ❑ other[11]: ……	-

15. How many new patent applications ('priority filings') have been made? *("Technologically unique": multiple applications for the same invention in different jurisdictions should be counted as just one application of grant).*		**3**
16. Indicate how many of the following Intellectual Property Rights were applied for (give number in each box).	Trademark	**0**
	Registered design	**3**
	Other	**0**
17. How many spin-off companies were created / are planned as a direct result of the project?		**0**
Indicate the approximate number of additional jobs in these companies:		

18. Please indicate whether your project has a potential impact on employment, in comparison with the situation before your project:

☺	Increase in employment, or	☺	In small & medium-sized enterprises
❑	Safeguard employment, or	☺	In large companies
❑	Decrease in employment,	❑	None of the above / not relevant to the project
❑	Difficult to estimate / not possible to quantify		

[10] Open Access is defined as free of charge access for anyone via Internet.
[11] For instance: classification for security project.

19. For your project partnership please estimate the employment effect resulting directly from your participation in Full Time Equivalent (*FTE = one person working fulltime for a year*) jobs:	**10**
Difficult to estimate / not possible to quantify	❑

I Media and Communication to the general public

20. As part of the project, were any of the beneficiaries professionals in communication or media relations?

○ Yes 😐 No

21. As part of the project, have any beneficiaries received professional media / communication training / advice to improve communication with the general public?

○ Yes 😐 No

22 Which of the following have been used to communicate information about your project to the general public, or have resulted from your project?

❑	Press Release	☺	Coverage in specialist press
❑	Media briefing	❑	Coverage in general (non-specialist) press
❑	TV coverage / report	❑	Coverage in national press
❑	Radio coverage / report	❑	Coverage in international press
❑	Brochures /posters / flyers	☺	Website for the general public / internet
❑	DVD /Film /Multimedia	☺	Event targeting general public (festival, conference, exhibition, science café)

23 In which languages are the information products for the general public produced?

❑	Language of the coordinator	😐	English
❑	Other language(s)		

***Question F-10*:** Classification of Scientific Disciplines according to the Frascati Manual 2002 (Proposed Standard Practice for Surveys on Research and Experimental Development, OECD 2002):

FIELDS OF SCIENCE AND TECHNOLOGY : Mathematics and computer sciences, Physical sciences; communication engineering and systems

1. NATURAL SCIENCES
1.1 Mathematics and computer sciences [mathematics and other allied fields: computer sciences and other allied subjects (software development only; hardware development should be classified in the engineering fields)]
1.2 Physical sciences (astronomy and space sciences, physics and other allied subjects)
1.3 Chemical sciences (chemistry, other allied subjects)
1.4 Earth and related environmental sciences (geology, geophysics, mineralogy, physical geography and other geosciences, meteorology and other atmospheric sciences including climatic research, oceanography, vulcanology, palaeoecology, other allied sciences)
1.5 Biological sciences (biology, botany, bacteriology, microbiology, zoology, entomology, genetics, biochemistry, biophysics, other allied sciences, excluding clinical and veterinary sciences)

2 ENGINEERING AND TECHNOLOGY

2.1 Civil engineering (architecture engineering, building science and engineering, construction engineering, municipal and structural engineering and other allied subjects)

2.2 Electrical engineering, electronics [electrical engineering, electronics, communication engineering and systems, computer engineering (hardware only) and other allied subjects]

2.3. Other engineering sciences (such as chemical, aeronautical and space, mechanical, metallurgical and materials engineering, and their specialised subdivisions; forest products; applied sciences such as geodesy, industrial chemistry, etc.; the science and technology of food production; specialised technologies of interdisciplinary fields, e.g. systems analysis, metallurgy, mining, textile technology and other applied subjects)

3. MEDICAL SCIENCES

3.1 Basic medicine (anatomy, cytology, physiology, genetics, pharmacy, pharmacology, toxicology, immunology and immunohaematology, clinical chemistry, clinical microbiology, pathology)

3.2 Clinical medicine (anaesthesiology, paediatrics, obstetrics and gynaecology, internal medicine, surgery, dentistry, neurology, psychiatry, radiology, therapeutics, otorhinolaryngology, ophthalmology)

3.3 Health sciences (public health services, social medicine, hygiene, nursing, epidemiology)

4. AGRICULTURAL SCIENCES

4.1 Agriculture, forestry, fisheries and allied sciences (agronomy, animal husbandry, fisheries, forestry, horticulture, other allied subjects)

4.2 Veterinary medicine

5. SOCIAL SCIENCES

5.1 Psychology

5.2 Economics

5.3 Educational sciences (education and training and other allied subjects)

5.4 Other social sciences [anthropology (social and cultural) and ethnology, demography, geography (human, economic and social), town and country planning, management, law, linguistics, political sciences, sociology, organisation and methods, miscellaneous social sciences and interdisciplinary , methodological and historical S1T activities relating to subjects in this group. Physical anthropology, physical geography and psychophysiology should normally be classified with the natural sciences].

6. HUMANITIES

6.1 History (history, prehistory and history, together with auxiliary historical disciplines such as archaeology, numismatics, palaeography, genealogy, etc.)

6.2 Languages and literature (ancient and modern)

6.3 Other humanities [philosophy (including the history of science and technology) arts, history of art, art criticism, painting, sculpture, musicology, dramatic art excluding artistic "research" of any kind, religion, theology, other fields and subjects pertaining to the humanities, methodological, historical and other S1T activities relating to the subjects in this group]

2. FINAL REPORT ON THE DISTRIBUTION OF THE EUROPEAN UNION FINANCIAL CONTRIBUTION

Report on the distribution of the European Union financial contribution between beneficiaries

Name of beneficiary	Final amount of EU contribution per beneficiary in Euros
TCS Thales Communications and Security	1 058 451
TPT Institut Mines Telecom - Telecom Paris Tech	373 083
ICL Imperial Collegeof Science and Medicine of London	234 521
VTT Teknologian Tutkimuskeskus VTT-OY	532 007
CEL Celeno Communication LTD	938 384
Total	**3 136 446**