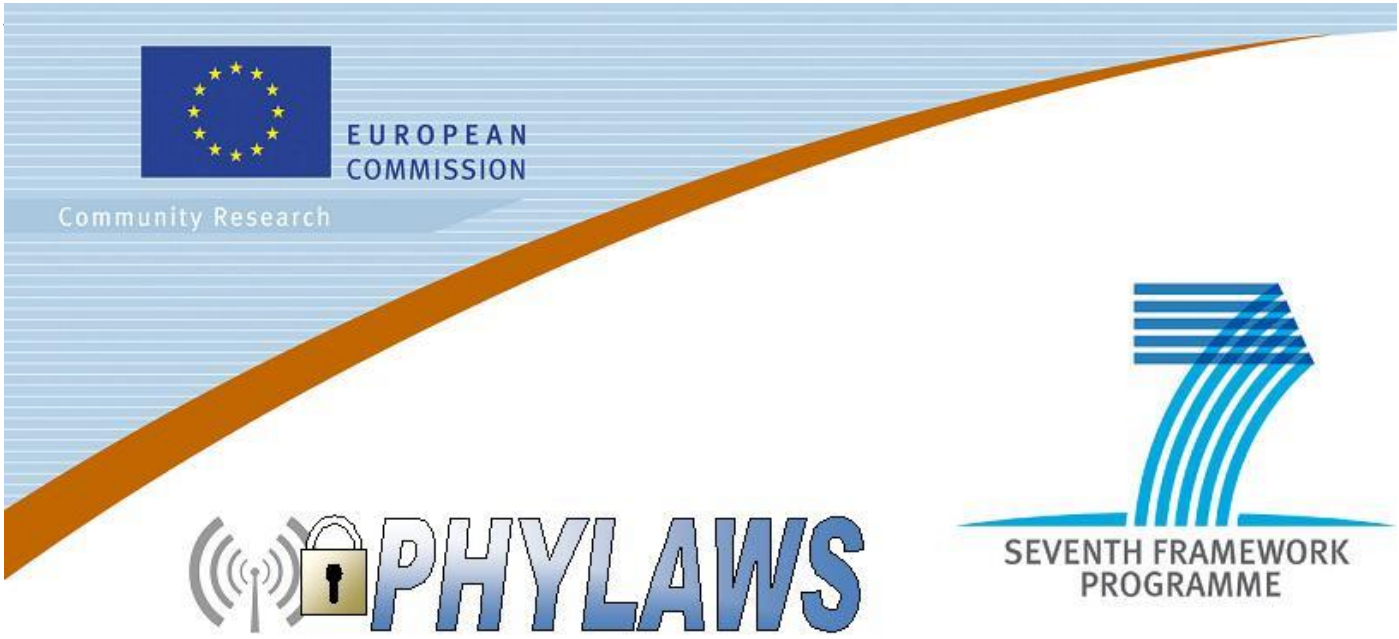

Project PHYLAWS (Id 317562)
PHYsical LAyer Wireless Security

Deliverable D1.8: Dissemination final report

Version 1.0 - 31 / 10 / 2016

FP7 Collaborative Projects, Networks of Excellence, Coordination and Support Actions in Collaborative Projects, Research for the benefit of Specific Groups (in particular SMEs)

Contractual Date of Delivery: October 30, 2016

Actual Date of Delivery: October 31, 2016

Editor(s): A. Sibille (TPT)

Contributor(s): F. Delaveau (TCS), A. Kotelba (VTT), C. Ling (IC), N. Shapira

Participant(s): all partners

Workpackage: WP1

Dissemination level: PU

Abstract: This deliverable provides the final results achieved by the project in terms of dissemination activities. It covers the achieved participation to scientific conferences and publications and the participation of PHYLAWS to dedicated events.

Executive Summary

Deliverable D1.8 is the 3rd and final among three reports dedicated to dissemination activities of PHYLAWS. It contains details on the dissemination activities achieved subsequently to the delivery of the intermediate report D1.7. The activities here described are:

- contribution to scientific conferences and scientific publications
- participation of dedicated PHYLAWS events
- involvement in clustering and other liaisons with relevant European projects
- dissemination towards stakeholders

Authors and Document History

Partner	Contributor	Date
TPT	A. Sibille	02/10/2016
VTT	A. Kotelba	10/10/2016
VTT	C. Ling	11/10/2016
TCS	F. Delaveau	11/10/2016
CEL	N. Shapira	11/10/2016
TPT	A. Sibille	31/10/2016
TCS	F. Delaveau	31/10/2016

Project 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. In a more concrete manner, the potential leaks and possible ways to avoid them have also started to be seriously addressed. The objective of the PHYLAWS project is 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. Efficient here means simple to implement, requiring easily developed and easily validated algorithms, but it also means techniques that will consume less resources, let that be in terms of energy (especially at the terminal level) and in terms of data consumption overhead (i.e. acting on the overall net spectral efficiency). The project outputs will thus benefit to a variety of existing and future standards for a large set of needs.

This objective will be 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 wave forms and versatile radio access protocols; a major research centre 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 will ensure both innovation and impact towards industrial applications, and they will assess validation of the commercial goals and validation of the society use relevance.

The project will benefit from recommendations and advices by an international Advisory Board, constituted of very high level personalities from governmental bodies, standardization bodies or academia. This Board will be one of the cornerstones of the project, based on the recognition that excellent technical developments and demonstrations will not be enough to ensure their wide spreading. Clearly, the project impact will 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, PHYLAWS will 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. This achievement will strongly impact the lives of citizens and will very much contribute to trustworthy ICT in the following years.

Administrative and contract references

[PHYLAWS_GA-A] PHYLAWS Grant Agreement, referenced FP7-ICT-317562-PHYLAWS version date 2012-07-03, part A

[PHYLAWS_GA-WP] PHYLAWS Grant Agreement, referenced FP7-ICT-317562-PHYLAWS version date 2012-07-03, Work Plan

[PHYLAWS_GA-AM] PHYLAWS Amendment n°1 to Grant Agreement FP7-ICT-317562-PHYLAWS version date 2015-03-10.

[PHYLAWS_GA-DOW2] PHYLAWS Grant Agreement, referenced 317562 version V2.2 date 2014-12-19 (revised Description of Work - part B of the Grant Agreement).

[PHYLAWS_GA-WP2] PHYLAWS Grant Agreement, referenced FP7-ICT-317562-PHYLAWS version date 2014-12-19 (revised Work Plan).

[PHYLAWS_D.1.1v2] PHYLAWS Management plan – updated version V2 version date 2015-05-31.

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

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

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

[PHYLAWS_D.1.10] PHYLAWS Standardization plan – Intermediate report - version V1 date 2015-05-07.

[PHYLAWS_D.1.12] PHYLAWS Advisory Board year 1 meeting report – version V1 date 2013-11-08

[PHYLAWS_D.1.13] PHYLAWS Advisory Board year 2 meeting report – version V1 date 2016-02-14

Other references

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

Presentations of PHYLAWS dedicated workshops (joint PROPHYLAXE and PHYLAWS workshops, Aug. 2015, PIMRC, Sept. 2016): http://www.phylaws-ict.org/?page_id=21

Presentations of Phylaws 2nd Advisory Board meeting (January 2016): http://www.phylaws-ict.org/?page_id=431

PHYLAWS publications: http://www.phylaws-ict.org/?page_id=92

PHYLAWS deliverables: http://www.phylaws-ict.org/?page_id=48

PhD thesis manuscript of H. Mirghasemi (Oct. 2014) and T. Mazloum (Feb. 2016): http://www.phylaws-ict.org/?page_id=457

Acronyms and Abbreviations

3GPP	3rd Generation Partnership Project
AB	Advisory Board
CIR	Channel Impulse Response
COMSOC	COMmunications SOCiety
COST	COoperation in Science and Technology
DoW	Description of Work
ETSI	European Telecommunications Standards Institute
FP7	7th Framework Programme
IET	Institution of Engineering and Technology
ICT	Information and Communication Technologies
IEEE	Institute of Electrical and Electronics Engineers
IET	Institution of Engineering and Technology
ISO	International Standards Organization
ITU	International Telecommunications Union
NETSEC	NETwork SECurity
PIMRC	Personal, Indoor and Mobile Radio Communications
PHYSEC	PHYsical SECurity
QUANT	Quantitative
RAT	Radio Access technology
SC	Secrecy Coding
SDR	Software Defined Radio
SKG	Secret Key Generation
STREP	Small and medium-scale focused research project
TRANSEC	TRANsmission SECurity
WP	Work Package
Y1	Year 1
Y2	Year 2
Y3	Year 3

Table of Contents

List of figures

List of tables

1. Introduction

This deliverable “Dissemination final report” is an update and summary of activities regarding the dissemination activities carried out the PHYLAWS project. It is organized in relation to the main aspects of these activities:

- web site
- scientific dissemination
- dissemination towards stakeholders and future users

It is reminded that standardization activities, together with the associated specific disseminations, are not part of this report, being covered by another dedicated task and deliverable D1.11: “Standardization final report”.

Some quantitative goals have been defined in the DoW and are recalled below:

Objective	Indicator	Nature
Scientific dissemination	Number of refereed international communications or publications (IEEE or similar): 17	QUANT
Scientific/technology users dissemination	Number of workshops: 3	QUANT

Table 1: Dissemination performance indicators

2. Web site

The specifications of the PHYLAWS web site have been detailed in the first version of this report (deliverable D1.6, provided at M3). In this section, we account for the actual availability of the web site, in relation with these specifications.

2.1. Actual public web site

The home page of the PHYLAWS portal is shown in Figure 1. The publicly accessible contents are as follows:

- A home page providing general information on PHYLAWS and its objectives and including downloadable presentations
- List of partners with their web sites
- Advisory board members with their affiliations and main position and conclusions of 2013 and 2016 meeting minutes
- Up-to-date deliverables. At the delivery date of the current report, 19 deliverables are available (Table 2)
- Publications. Apart from general presentations on the PHYLAWS project, a large set of conference presentations and journal by the consortium are readily downloadable. As yet, this amounts to 47 document publicly available
- Contributions to standardization events, with downloadable documents. This refers to two ETSI meetings, two 3GPP meetings and one ITU meeting
- Detailed contents for the workshops organized by PHYLAWS, i.e. the PIMRC 2016 workshop, the 2015 joint PROPHYLAXE and PHYLAWS workshop and the 2013 PIMRC workshop
- Two PhD thesis manuscripts relevant to works fully carried out within the context of the PHYLAWS project
- A contact page, which allows to send requests to the coordinator by whoever wishes

D1.6 - Dissemination planning report	D4.1 - TRANSEC upgrades of existing RATs - study report
D1.7 - Dissemination intermediate report	D4.2 - TRANSEC upgrades of existing RATs - upgrades of existing RATs - simulation and analyses complements
D1.8 - Dissemination final report (present document)	D4.3 - NETSEC upgrades of existing RATs - study report
D1.9 - Standardization planning report	D4.4 - NETSEC upgrades of existing RATs - simulation analyses complements (to be published November 2016)
D1.10 - Standardization intermediate report	D4.5 - New Rats and Wave Forms taking benefit of Physec upgrades – interim report
D1.11 - Standardization final report (to be published November 2016)	D4.6 - New Rats and Wave Forms taking benefit of Physec upgrades – final report (to be published November 2016)
D1.12 – Advisory Board meeting year 1 report	D5.1 - WiFi Testbed Setup - Development Report
D1.13 – Advisory Board meeting year 2 report	D5.2 - WiFi Testbed Experiment Campaign Plan
D1.14 – Advisory Board year 3 final report (to be published November 2016).	D5.3 - Intermediate Report on WiFi interceptor experiments with the test bed
D2.1 - Analysis of threats, countermeasures and self-protection techniques	D5.4 - Final report on interception experiments on test bed, synthesized with complementary simulation results. Final analysis on PHYSEC methods proof of concept (to be published November 2016)
D2.2 - security architectures in wireless terminals	D5.5 - Concluding report on experimental support for standardization proposals for WiFi PHYSEC upgrades (to be published November 2016)
D2.3 - Fundamental aspects of Physical Layer Security	D6.1 - Modelling of LTE-based cellular system
D2.4 - New opportunities provided by modern wave forms new security protocols and sensing/measure of radio environments	D 6.2 - Simulation of Interception of waveform signals in LTE-based cellular system
D3.1 - Channel based random generators - Interim report	D6.3. LTE Simulations results - Final Report
D3.2 - Channel based random generators - Final report	
D3.3 - Coding techniques and algorithms for secrecy coding and secret key generation	
D3.4 - CIR Measurements and Modeling in ISM 2.4 GHz and 5 GHz bands(to be published November 2016)	
D3.5 - Simulations report of PHYSEC methods using measured CIRs (To be published November 2016)	

Table 2: Deliverables downloadable from the public part of the web site

Figure 1: Upper part of the PHYLAWS Website

2.2. Private zone (authentified access)

The private zone is fully compliant with the specifications listed in deliverable D1.6. Access requires authentication from the following shown Figure 2

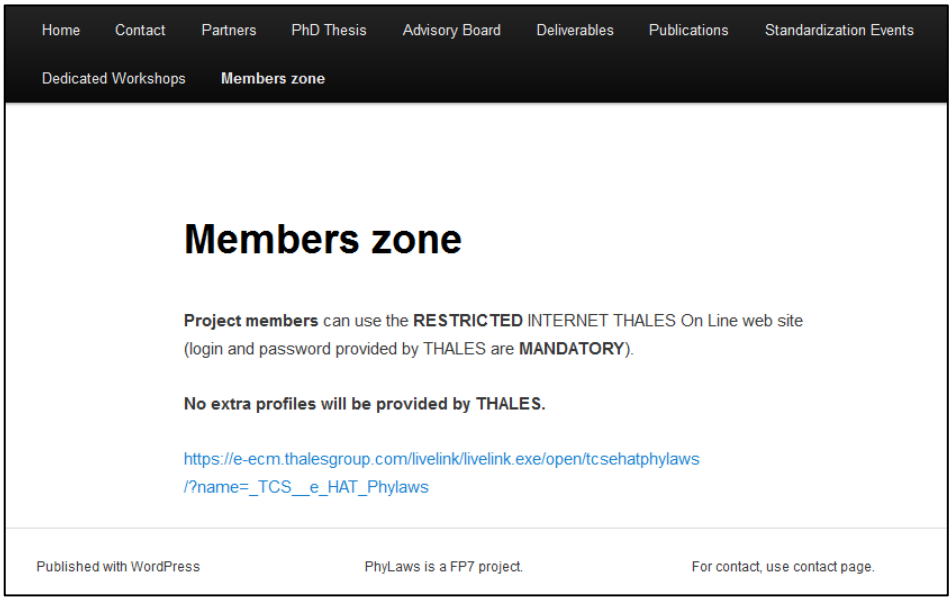

Figure 2: Access to the private zone

The relevant home page is shown in Figure 3. It provides access:

- of shared documents to the consortium partners
- of deliverable to the European Commission (04- EC_dedicated zone).
- of deliverable to reviewers of the European Commission (04- EC_dedicated zone/Reviewers).

Figure 3: Home page of the private zone

3. Scientific dissemination and dissemination towards stakeholders

In this section we provide a detailed account about the achieved dissemination from the project beginning until the date of delivery of D1.8.

3.1. Achieved participation to scientific dissemination

In deliverable D1.6, the following quantitative goals have been identified regarding the contribution of the PHYLAWS partners to scientific symposia, conferences, workshops & related dissemination activities:

- 2 international communications / academic partner / year ($\rightarrow$ 12 in total)
- 1 international communication / other partner ($\rightarrow$ 3 in total)

In the following table, the activities achieved by the consortium until the delivery date of the present report are listed. Lines 25 to 34 refer to communications indicated subsequently to the previous version (D1.7) of this deliverable.

It can be noticed that the conferences cover differing scientific communities and audiences, meaning that the dissemination target is suitably realized.

A second remark is that the quantitative objectives over the whole project are fully achieved and even exceeded.

N°	Type	Title	Main authors	Title	Dates	Publisher	Place	Year
1	Seminar	Génération de clés secrètes à partir du canal radio	Taghrid Mazloum et Alain Sibille	AREMIF	May 27		Paris, France	2013
2	Article + Conference presentation	A Disc of Scatterers Based Radio Channel Model for Secure Key Generation	Taghrid Mazloum and Alain Sibille	COST IC1004, 13th MCM	Sept. 25-27		Ghent, Belgium	2013
3	Article + Conference presentation	Security risks in the short-range communication of ubiquitous application	Antti Evesti, Jani Suomalainen, and Reijo Savola	International Conference for Internet Technology and Secured Transactions	Dec 9-10	IEEE Xplore	London, UK	2013
4	Article + Conference presentation	A Disc of Scatterers Based Radio Channel Model for Secure Key Generation	Taghrid Mazloum, Francesco Mani and Alain Sibille	EUCAP 2014	April 6-11	IEEE Xplore	The Hague, netherlands	2014
5	Article + Conference presentation	Ray Tracing Simulations of Indoor Channel Spatial Correlation for Physical Layer Security	Francesco Mani, Enrico M. Vitucci, Taghrid Mazloum, Alain Sibille and Vittorio Degli Esposti	COST IC1004, 14th MCM	Feb. 5-7		Ferrara, Italy	2014
6	Article + Conference presentation	Security pairings using physical layer properties of wireless communications	Jani Suomalainen, Antti Evesti, and Adrian Kotelba	International Conference on Privacy and Security in Mobile Systems	May 11-14	IEEE Xplore	Aarlborg, Denmark	2014
7	Article + Conference presentation	Analysis of Alice-Bob-Eve scenarios for secret key generation from random channels	Alain Sibille	URSI GASS	Aug. 17-23	IEEE Xplore	Beijing, China	2014

8	Article + Conference presentation	Performance of secret key generation in non stationary channels	Taghrid Mazloum and Alain Sibille	EUCAP 2015	April 13-17	IEEE Xplore	Lisbon, Portugal	2015
9	Article + Conference presentation	Ray Tracing Simulations of Indoor Channel Spatial Correlation for Physical Layer Security	Enrico M. Vitucci, Francesco Mani, Taghrid Mazloum, Alain Sibille and Vittorio degli Esposti	EUCAP 2015	April 13-17	IEEE Xplore	Lisbon, Portugal	2015
10	Article + Conference presentation	Active and passive eavesdropper threats within public and private civilian wireless networks - existing and potential future countermeasures	François Delaveau, Antti Evesti, Jani Suomalainen, Reijo Savola , Nir Shapira	Winncomm 2013	June 11	Winncomm Forum	Munich, Germany	2013
11	Article + Conference presentation	PHYSEC concepts for wireless public networks – introduction, state of the art and perspectives	Cong Ling, François Delaveau, Erice Garrido, Alain Sibille, Jean-Claude Belfiore	Winncomm 2013	June 11	Winncomm Forum	Munich, Germany	2013
12	Seminar	Providing Radio Advantage for Establishing Secrecy by Tag Signals	David Depierre, Renaud Molière, François Delaveau	GDR Isis on Physec	May 22	GDR ISIS	Paris, France	2014
13	Article + Conference presentation	Towards a key-free radio protocol for authentication and security of nodes and terminals in advanced waveforms	Eric Nicollet, François Delaveau, Renaud Molière, Christiane Kameni, Claude Leménager, Taghrid Mazloum et Alain Sibille	Winncomm 2015 San Diego	Marsh 26	Winncomm Forum	San Diego, USA	2015
14	Article + Conference presentation	Tag Signals for Early Authentication and Secret Key Generation in Wireless Public Networks	Renaud Molière, Christiane Kameni, Claude Leménager, François Delaveau, Taghrid Mazloum et Alain Sibille	EuCNC2015	June 29-July 2	IEEE Xplore	Paris, Issy les Mx, France	2015
15	Article + Conference presentation	Secrecy gain, flatness factor, and secrecy-goodness of even unimodular lattices	Fuchun Lin, Cong Ling, and Jean-Claude Belfiore	IEEE ISIT 2014	June 29-July 4	IEEE Xplore	Honolulu, USA	2014
16	Article + Conference presentation	Achievable diversity-rate tradeoff of MIMO AF relaying systems with MMSE transceivers	Changick Song and Cong Ling	IEEE ISIT 2014	June 29-July 4	IEEE Xplore	Honolulu, USA	2014
17	Article + Conference presentation	Lattice Gaussian Coding for Capacity and Secrecy:Two Sides of One Coin	Cong Ling and Jean-Claude Belfiore	IZS on Communications 2014	February 26-28	ETH-Zürich	Zürich, Switzerland	2014
18	Article + Conference presentation	Achieving the AWGN channel capacity with lattice Gaussian coding	Cong Ling and Jean-Claude Belfiore	IEEE ISIT 2013	July 7-12	IEEE Xplore	Istanbul, Turkey	2013

19	Article + Conference presentation	MIMO broadcasting for simultaneous wireless information and power transfer: Weighted MMSE approaches	Changick Song, Cong Ling, Jaehyun Park and Bruno Clerckx	Globecom Workshops 2014	December 8-12	IEEE Xplore	Austin, USA	2014
20	Article + Conference presentation	Independent Metropolis-Hastings-Klein Algorithm for Lattice Gaussian Sampling	Zheng Wang and Cong Ling	IEEE ISIT 2015	June 14-19	IEEE Xplore	Hongkong, China	2015
21	Article + Conference presentation	On the capacity of the modulo lattice channels	Hamed Mirghasemi and Jean-Claude Belfiore	51st Allerton Conference	September	IEEE Xplore	Allerton, IL, USA	2013
22	Article + Conference presentation	The un-polarized bit-channels in the wiretap polar coding scheme	Hamed Mirghasemi and Jean-Claude Belfiore	IEEE Wireless VITAE 2014	May 11-14	IEEE Xplore	Aalborg, Denmark	2014
23	Article + Conference presentation	Codes for wireless wiretap channels	Jean-Claude Belfiore	IEEE ITW 2014	November 2-5	IEEE Xplore	Hobart, Australia	2014
24	Article + Conference presentation	The semantic secrecy rate of the lattice Gaussian coding for the Gaussian wiretap channel	Hamed Mirghasemi and Jean-Claude Belfiore	IEEE ITW 2014	November 2-5	IEEE Xplore	Hobart, Australia	2014
25	Article + Conference presentation	Perspectives of Physec for the improvement of the subscriber privacy and communication confidentiality at the Air Interface . Results for WLANs, IoT and radiocell	F. Delaveau, A. Mueller , G. Wunder and ali	"ETSI WS on fut. radio techn. Air Interface.	27-28 /01/16	IEEE Xplore	Sofia.Antipolis, France	2016
26	Article + Conference presentation	Secret Key Generation scheme from WiFi and LTE reference signals	Christiane L. Kameni Ngassa; Renaud Molière; François Delaveau; Taghrid Malzoum;; Alain Sibille	Wincomm forum US 2016	17 March 2016	IEEE Xplore	Reston, Wincomm forum, Technical Session 6: SDR, CR and DSA Applications 1	2016
27	Article + Conference presentation	Combining Artificial Noise Beam Forming And Concatenated Coding Schemes To Effectively Secure Wireless Communications	Christiane L. Kameni Ngassa; Jean-Claude Belfiore; Renaud Molière; François Delaveau; Nir Shapira	Wincomm forum US 2016	17 March 2016	IEEE Xplore	Reston, Wincomm forum, Technical Session 6: SDR, CR and DSA Applications 1	2016
28	Article + Conference presentation	Further Results on Independent Metropolis-Hastings-Klein Sampling	Zheng Wang and Cong Ling	IEEE ISIT 2016	July	IEEE Xplore	Barcelona, Spain	2016

29	Article + Conference presentation	Algebraic Lattice Codes Achieve the Capacity of the Compound Block-Fading Channel	Antonio Campello, Cong Ling and Jean-Claude Belfiore	IEEE ISIT 2016	July	IEEE Xplore	Barcelona, Spain	2016
30	Article + Conference presentation	Almost universal codes for fading wiretap channels	Laura Luzzi, Cong Ling and Roope Vehkalahti	IEEE ISIT 2016	July	IEEE Xplore	Barcelona, Spain	2016
31	Article + Conference presentation	Symmetric Mettropolis-within-Gibbs Algorithm for Lattice Gaussian Sampling	Zheng Wang and Cong Ling	IEEE ITW 2016	Septemb er	IEEE Xplore	Cambridge, UK	2016
32	Article + Conference presentation	Algebraic lattices achieve the capacity of the ergodic fading channel	Antonio Campello, Cong Ling, Jean-Claude Belfiore	IEEE ITW 2016	Septemb er	IEEE Xplore	Cambridge, UK	2016
33	Article + Conference presentation	Analysis of secret key robustness in indoor radio channel measurements	T. Mazloum, F. Mani et A. Sibille	IEEE VTC Spring	May	IEEE Xplore	Glasgow, UK	2015

Table 3: Achieved scientific conference communications

3.2. Publications in scientific journals

In deliverable D1.6, the following quantitative goals have been identified regarding the contribution of the PHYLAWS partners to scientific symposia, conferences, workshops & related dissemination activities:

- 1 international journal paper / academic partner ($\rightarrow$ 2 in total)

In the following table, the activities achieved by the consortium until the delivery date of the present report are listed. Lines 3 to 8 refer to publications indicated subsequently to the previous version (D1.7) of this deliverable.

As a remark, it is noteworthy that PHYLAWS contributed through two chapters to a book under preparation by IET "Trusted Communications with Physical Layer Security for 5G and Beyond". This is both an effort from the consortium and a valuable initiative from the editor to disseminate practical PHYSEC technologies toward the general wireless networks R&D community and make them better known and recognized as viable means to enhance security in wireless access.

N°	Type	Title	Main authors	Title	Dates	Publisher	Year
1	Article	Semantically secure lattice codes for the Gaussian wiretap channel	Cong Ling, Laura Luzzi, Jean-Claude Belfiore, and Damien Stehle	IEEE Trans. Inform. Theory	October	IEEE Xplore	2014
2	Article	Achieving AWGN channel capacity with lattice Gaussian coding	Cong Ling and Jean-Claude Belfiore	IEEE Trans. Inform. Theory	October	IEEE Xplore	2014
3	Article	Security aspects of short-range wireless communication: Risk analysis for the healthcare application	Antti Evesti, Jani Suomalainen, Reijo Savola	International Journal of Intelligent Computing Research (IJICR)	December	Infonomics Society	2014
4	Book chapter	Application cases of Secret key generation in communication nodes and terminals"	Francois Delaveau, Christiane Kameni Ngassa, Renaud Molière, Adrian Kotelba, Jani Suomalainen, Sandrine Boumard, Taghrid Mazloum, Alain Sibille, Nir Shapira	IET Book "Trusted Communications with Physical Layer Security for 5G and Beyond	To be published end 2016	IET book	To be publishe d end 2016

5	Book chapter	Application cases of Secrecy Coding in communication nodes and terminals"	Francois Delaveau, Christiane Kameni Ngassa, Adrian Kotelba, Jani Suomalainen, Sandrine Boumard, Cong Ling, Ling Liu	IET Book "Trusted Communications with Physical Layer Security for 5G and Beyond	To be published end 2016	IET book	To be published end 2016
6	Journal paper selected by the Wincomm TPC	Secret Key Generation scheme from WiFi and LTE reference signals	Christiane L. Kameni Ngassa ; Renaud Molière; François Delaveau; Taghrid Malzoum; Alain Sibille; Nir Shapira	Springer Journal Special Issue, Analog Integrated Circuits & Signal Processing	To be published end 2016	Springer	To be published end 2016
7	Journal paper selected by the Wincomm TPC	Combining Artificial Noise Beam Forming And Concatenated Coding Schemes To Effectively Secure Wireless Communications	Christiane L. Kameni Ngassa ; Jean-Claude Belfiore; Renaud Molière; François Delaveau; Nir Shapira	Springer Journal Special Issue, Analog Integrated Circuits & Signal Processing	To be published end 2016	Springer	To be published end 2016
8	Article	On the Diversity of Linear Transceivers in MIMO AF Relaying Systems	Changick Song, Cong Ling	IEEE Trans. Inform. Theory	January	IEEE Xplore	2016
9	Article	Analysis of Secret Key Randomness Exploiting the Radio Channel Variability	T. Mazloum et A. Sibille	IJAP	Septembe r	Hindawi	2015

Table 4: Achieved journal publications

3.3. PhD dissertations

Two PhD students dissertations, fully resulting from work carried out within PHYLAWS (Task T3.1), have been defended:

- Hamed Mirghasemi (Telecom ParisTech) defended on October 10, 2014, a thesis entitled "Lattice Codes for the Continuous Wiretap Channels"
- Taghrid Mazloum (Telecom ParisTech) defended on February 12, 2016, a thesis entitled "Analysis and modeling of the radio-channel for Secret Key Generation"

3.4. Organization of PHYLAWS dedicated events and dissemination towards stakeholders

3.4.1. Initial planning of PHYLAWS dedicated events

The planned events as anticipated at the project start were as follows:

- 1 joint international workshop or special session on PHYSEC around the end of Y1
- 1 joint international workshop or special session on PHYSEC around the end of Y2
- 1 dedicated PHYLAWS workshop at the end of Y3

(→ 3 events in total)

The two first events had the objective to gather international competencies in the area of wireless physical layer security, mainly European and mainly academic, in order to ensure an excellent integration of PHYLAWS research in the international up-to-date effort on the topic, and at the same time ensure a good awareness of these communities into what's going on within PHYLAWS (cross-fertilization).

The last event would be more focused on PHYLAWS results, assumed to be applicable to real world use cases.

3.4.2. Dedicated events held by the PHYLAWS team

The first of these events was fully realized shortly before the end of Y1: a special session about Physical Layer Security took place during the PIMRC congress in London (Sept. 8, 2013) and comprised 15 papers.

On a less global scale, PHYLAWS was represented through RAS cluster meeting participation in Brussels and through a panel in a conference session on secure communications in USA (2015). Also, Phylaws was invited as a panelist at the workshop on Physical Layer Security to be held on June 8, 2015 at the IEEE International Conference on Communications (ICC) London, UK.

The updated contributions to or organization of events can be found in table 5 below.

N°	Type of activities	Main leader (O: organizer ; C: contributor)	Title	Event / Details	Date	Place	Type of audience).	Size of audience	Countries addressed
1	Special session	TPT (O), IC (O)	Special session on Physical Layer security	PIMRC 2013	Sept. 8, 2013	London, UK	Scientific + industry	40	All (world level event)
2	Seminar - paper	TCS (C)	Several contribution to RAS Cluster meeting (4) and papers	RAS Cluster	on going 2013	Brussels, Belgium	Coordinator of EC projects, EC members, invited persons	50	Europe
3	Seminar - paper	TCS (C)	Several contribution to RAS Cluster meeting and papers	RAS Cluster	on going 2015	Brussels, Belgium	Coordinator of EC projects, EC members, invited persons	50	Europe
4	Workshop session	TCS (C)	Panelist within a Workshop session	IEEE ICC 2015	2015, June 8	London, UK	Students, scientists, Indrusties, regulators	50	All (world level event)
5	Conference panel	VTT ('C)	Panelist within conference session on secure communications	MILCOM 2015	2015, October 26-28	Tampa, USA	Students, scientists, Indrusties, regulators	50	All (world level event)
6	Workshop session	TCS ('O), VTT ('C), CEL ('C)	Panelist with a workshop session	PIMRC 2016	2016, September 4	Valencia, Spain	Students, scientists	20	All (world level event)
7	Workshop paper	TCS ('O), FUBerlin ('C)	Perspectives of Physical Layer Security (Physec) for the improvement of the subscriber privacy and communication confidentiality at the Air Interface	ETSI B-COM WS on fut. radio techn. Air Interface	2016, March	Cesson Sevigné, France	scientists, engineers, stakeholders	50	All (world level event)
8	Seminar - paper	FUBerlin ('O), TCS ('C)	Physical Layer Security in a 5G Setting	EUCNC 2016	2016 June	Athens, Greece	scientists, engineers, stakeholders	50	All (world level event)
9	Workshop paper (invited)	VTT ('C)	Implantation and simulation of Physec security schemes into LTE cellular links - Results and relevant standardization perspectives	PIMRC 2016 WS 8	2016, September 4	Valencia, Spain	Students, scientists	20	All (world level event)
10	Workshop paper (invited)	CEL ('O), TCS('C)	Implantation and experimentation of Physec security schemes into Wifi radio links - Results and relevant standardization perspectives	PIMRC 2016 WS 8	2016, September 4	Valencia, Spain	Students, scientists	20	All (world level event)

Table 5: Special sessions, workshops and related

3.4.3. Focus on the final open Workshop of the PHYLAWS project

One major effort has concerned the organization of an open workshop, in the context of the IEEE COMSOC flagship conference PIMRC 2016, which took place on Sunday, September 4, 2016, in Valencia (Spain). The program can be found in Figure 4. The presentations are available on the public part of the web site.

Workshop W8
Deployment perspectives of Physical Layer Security into wireless public RATs

9h00 – Welcome - Introduction - by F.Delaveau, Thales Communications and Security, France

9h15 - Session 1 - Chaired by Dr Arsenia Chorti, University of Essex (achorti@essex.ac.uk)

About new academic and experimental results on Physec schemes

Introducing Keynote 1, by Dr Arsenia Chorti, University of Essex (30' talk + 5' questions)

About the State of the art of Physec.

Paper 1: (20' talk + 5' questions)

"Secure Compute-and-Forward Transmission With Artificial Noise and Full-Duplex Devices" by Pr Stefano Tomasin, University of Padova.

Speaker: Stefano Tomasin tomasin@dei.unipd.it

Paper 2: (20' talk + 5' questions)

"Semi-orthogonal selection for secure multiuser MISO communication systems with quantized feedback" by Berna Ozbek and Ozgecan Ozdogan (Izmir Institute of Technology, Izmir) and Gunes¸ Karabulut Kurt (Istanbul Technical University, Istanbul).

Speaker: Berna Ozbek bernaozbek@iyte.edu.tr.

10h40 - Pause 30' – Test bed presentation and demo in the WS room

11h00 - Session 2 - Chaired by Pr S. Tomasin. University of Padova (tomasin@dei.unipd.it)

About the implantation perspectives of physec schemes.

Paper 3: (20' talk + 5' questions)

"RECiP: Wireless Channel Reciprocity Restoration Method for Varying Transmission Power", by Gerhard Wunder, Rick Fritschek, Khan Reaz (Heisenberg Communications and Information Theory Group Freie Universität Berlin)

Speaker: Gerhard Wunder wunder@zedat.fu-berlin.de

Invited paper 4: (20' talk + 5' questions)

"Implantation and simulation of Physec security schemes into LTE cellular links – results and relevant standardization perspectives", by Adrian Kotelba and Sandrine Boumard (VTT- Oy Finland). Speaker: Adrian Kotelba Adrian.Kotelba@vtt.fi

Invited paper 5: (20' talk + 5' questions)

"Implantation and experimentation of Physec security schemes into Wifi radio links – results and relevant standardization perspectives", by Nir Shapira (Celeno Communications Ldt Israel), Christiane Kameni, Renaud Molière François Delaveau (ThalesCommunciations and Security, France). Speaker: Nir Shapira Nir.Shapira@celeno.com

Concluding Keynote 2, by Pr Stefano Tomasin, university of Padova (30' talk + 4')

*"*Experiments and implementations of physical layer security schemes"

12h50 – Conclusion - by F.Delaveau, Thales Communications and Security, France (1')

Figure 4: Program of the PIMRC 2016 workshop

Figure 5: Demonstration of the wifi test bed including PHYSEC schemes at the PIMRC 2016 workshop

Figure 6: Pictures of the PHYLAWS team at the PIMRC 2016 workshop

3.4.4. Dissemination towards stakeholders

For a maximum impact of the project results, it is important to make the main objectives and the progress be known from potential stakeholders, able to use or exploit the PHYLAWS technology. In deliverable D1.6, the main stakeholders have been identified as follows:

1. wireless products manufacturers (large companies, techno-providers)
2. major telecom operators
3. regulators
4. local operators (e.g. WIFI hotspots)
5. software developers
6. scientific community: universities, research centers

The first second and third category are widely covered through the initiatives of the PHYLAWS consortium into standardization bodies such as ETSI, 3GPP, ITU and IEEE: Manufacturers such as Huawei, Nokia, Qualcomm, Siemens, Gemalto and numerous operators such as Orange, Vodaphone, Telecom Italia, China telecom etc. were reached by our dissemination during sessions of standardization bodies, especially at 3GPP SA3 and ITU-R. Same applied for frequency administration (France, Germany, etc.) at ITU-R. See more details in deliverable D1.11 PHYLAWS Standardization plan – Final report.

The last category was widely covered through the scientific dissemination detailed in sections 3.1-3.2 above.

Categories 3 and 4 are also reached through both standardization initiatives and dissemination actions towards scientific community, through their internal R&D departments, although in a more scattered and indirect manner.

However, the solid and continued participation of PHYLAWS in suitable congresses, workshops, technical forum and standardization bodies is a suitable way to trigger the interest of major actors. This in particular involves the Wireless Innovation Forum (SDR Forum Version 2.0), especially in relation with the "WINNF Spectrum Sharing Annual Report" (see ref. [WINFORUM_SSAR], for security aspects relevant to Physical Layer.

In particular,

- Two presentations have been given at the Winncomm Forum in Münich, Germany, June 2013
- One presentation has been given at the Winncomm Forum in San Diego, USA California, March 2015
- Two presentations have been given at the Winncomm Forum in Reston, USA, March 2016

See also deliverable D1.11 PHYLAWS Standardization plan – Final report.

3.4.5. Dissemination through the Advisory Board

Another instrument to help dissemination to stakeholders is via the PHYLAWS Advisory Board (Table 6). The AB had its first meeting in Paris in October 2013, and the outcome has been reported in deliverable D1.7.

The 2nd AB meeting took place in Paris on January 20, 2016, with the participation of the full consortium. The minutes, including the various conclusions, recommendations and presentation slides are available from the public part of the web site.

1 **Professor Lee Pucker** (USA – Canada) MSc. PMC. Chief Executive Officer. The Wireless Innovation Forum
2 **Professor Doctor Srdjan Capkun** (CH) Associate Professor of Computer Science, ETH Zurich. Internationally known expert in physical layer for security, computer security, privacy, networking.
3 **Doctor Scott W Cadzow** (UK) Chief Executive Officer of C3L company Chair or vice-chair of ETSI ITS WG5 (Security), TETRA WG6 (Security), TA SFPG (Security), ISO TC204.16.7 (Security) and specialist task force expert for security in ETSI TISPAN, ETSI MTS, ETSI HF.
4 **Professor Joseph Mitola** (USA) Fellow of the IEEE US Advisor Regarding Trustable Cognitive Systems
5 **Doctor Peter Mueller** (CH) IBM Zurich Research Laboratory CH
6 **Mr Philippe Aubineau** (CH) Counsellor, ITU-R Study Group 1, CPM and SC Study Group Department. Radiocommunication Bureau International Telecommunication Union. Genève CH

Table 6: Composition of the advisory board

Figure 7: View of the AB meeting in Telecom ParisTech premises on January 20, 2016

PHYLAWS Advisor Board meeting, 20 January 2016, Paris - Agenda

A/ 10h00 STARTING TIME : Welcome (TPT + TCS) – Agenda proposal

B/ Brief Recalls about the Phylaws project – scope, organization, fundamentals, status - answers to questions: (TCS + partners)

C/ Overview of the past and technical current work–year 2015- start 2016:

- Academic study of radio channel + Secret Key Generation
- Development of a complete SKG Scheme
- Academic study of Secrecy Coding
- Study, implantation and simulation of a SC scheme
- Study of a SP scheme
- Development of a test bed - 2015 and following 2016
- Development of a simulation - 2015 and following 2016
- first experimental test of SKG schemes - 2015 and following 2016
- Interactive discussion of partners with Advisory Board members
- Overview of dissemination and standardization
- How to enhance the impact of this work
- for dissemination and standardization ?

D/ Discussion of any theoretical items to be followed on

- Interactive discussion of partners with Advisory Board Members

12h30 PAUSE - LUNCH IN THE MEETING ROOM

E/ Return on the experimental items to be followed on (CEL + TCS):

- Interactive discussion of partners with Advisory Board Members

F/ Return on the simulation items to be followed on (VTT + TCS)

- Interactive discussion of partners with Advisory Board Members

G/ Return on the dissemination initiatives (TPT + partners)

- Interactive discussion of partners with Advisory Board Members

H/ Focus on standardization initiatives (TCS + partners)

- Interactive discussion of partners with Advisory Board Members

I/ Conclusion – Thanks (TCS + all).

END OF THE MEETING AND CLOSING TIME 17h00

Figure 8: Agenda of the AB meeting in Telecom ParisTech premises on January 20, 2016

3.5. Patent strategy

Three patents have been filed, first in France then expected to be extended to a wide international set of countries in the short term. **Table 7** below sum up the relevant information and status available end October 2016.

No. de dépôt :	1502713
Date de dépôt :	29 décembre 2015
Titre officiel :	PROCEDE D'ASSOCIATION UNIVALENTE ET UNIVOQUE ENTRE EMETTEURS ET RECEPTEURS DE TRANSMISSION A PARTIR DU CANAL DE PROPAGATION
Inventeurs :	François DELAVEAU, Renaud MOLIERE, Christiane KAMENI NGASSA, Claude LEMENAGER, Adrian KOTELBA, Jani SUOMALAINEN
Déposants:	THALES, TEKNOLOGIAN TUTKIMUSKESKUS VTT
Status:	Publication accepted by French MoD Delivery accepted by the French Patent bureau (acceptance 27 October 2016) International extensions in progress

No. de dépôt :	1502712
Date de dépôt :	29 décembre 2015
Titre officiel :	PROCEDE D'EXTRACTION UNIVALENTE ET UNIVOQUE DE CLES A PARTIR DU CANAL DE PROPAGATION
Inventeurs :	Renaud MOLIERE, Christiane KAMENI NGASSA, François DELAVEAU, Claude LEMENAGER, Alain SIBILLE, Taghrid MAZLOUM, Nir SHAPIRA
Déposants :	THALES, TELECOM ParisTech, CELENO COMMUNICATION LTD
Status:	Publication accepted by French MoD Delivery accepted by the French Patent bureau (acceptance 27 October 2016) International extensions in progress

No. de dépôt :	1502710
Date de dépôt :	29 décembre 2015
Titre officiel :	PROCEDE DE CODAGE UNIVOQUE ET SECRET DE TRANSMISSION SUR UN CANAL DE PROPAGATION A AVANTAGE DE CAPACITE
Inventeurs :	Christiane KAMENI NGASSA, François DELAVEAU, Jean-Claude BELFIORE, Cong LING
Déposants :	THALES, TELECOM ParisTech, IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE
Status:	Publication accepted by French MoD Delivery in progress by the French Patent bureau (expected November 2016) International extensions in progress

Table 7: Patents filed from the foreground knowledge generated by the PHYLAWS project

4. Clustering activities

Previously mentioned clustering activities are the following (referring to deliverable D1.7):

- ICT FP7 call 8 project DUPLO (STREP)
- COST Action IC1004
- “Radio Access and Spectrum” (RAS) cluster of FP7

Subsequently, liaisons have been established with several European projects relevant to PHYSEC:

- 5G-Ensure: Note that cross-participation to meeting and coordinated proposal to 3GPP occurred especially with project 5G-Ensure, which deals with 5G security.
- Coherent
- Sonata

Since these liaisons are relevant with respect to standardization issues, they are mentioned in more detail in deliverable D1.11.

5. Conclusion

The PHYLAWS consortium has regarded dissemination as an important part of the project outputs, given that in the minds of many researchers and even more many engineers, PHYSEC is still seen as a technology of the future or a purely theoretical dream. In this respect, the dissemination activities have been quite effective on all aspects expected for an R&D project:

- Scientific/academic dissemination
  - 33 conference presentations, mostly peer reviewed with proceedings
  - 9 journal papers or book chapters
  - 8 participations in dedicated events
  - 2 special session/workshop organized
  - 2 PhD defenses
- Dissemination toward stakeholders
  - 2 Advisory Board meetings
  - Continued participation to the Winncomm Forum
  - A set of 6 clustering/liaison activities
  - 3 patents, first filed in France then to be widely extended internationally

Overall, the dissemination plan has been fully respected and even exceeded with respect to the quantitative indicators of the DoW.