



WinnComm USA 2016 – Reston Virginia, 15 - 17th March 2016

SECRET KEY GENERATION SCHEME FROM WIFI AND LTE SIGNALS

SDR'16 Winncomm, Reston, 17 March 2016
Technical Session 6: SDR, CR and DSA Applications 1

Eric Nicollet(*)

Christiane Kameni Ngassa(*), François Delaveau(*), Renaud Molière(*)
Taghrid Mazloum(**), Alain Sibille(**)

(*) Thales Communications & Security; Gennevilliers, France
(**) Telecom ParisTech, Paris, France

E. Nicollet eric.nicollet@thalesgroup.com phone : + 33 (0)1 46 13 21 32
R. Moliere renaud.moliere@thalesgroup.com phone : + 33 (0)1 41 30 33 60
F. Delaveau francois.delaveau@thalesgroup.com phone : + 33 (0)1 46 13 31 32
C. Kameni christiane.kameni@thalesgroup.com phone : + 33 (0)1 41 30 30 19

Presentation of PHYLAWS project EC FP7 ICT Id-317562
www.phylaws-ict.org

Summary/Agenda

- **Recall of project phylaws: goal and outputs**
- **Brief introduction to PHYsical Layer SECurity (PHYSEC):**
  - Studied configuration of wireless links
  - Exploiting the multipaths randomness of wireless radio Channel
  - Our Fondamentals - Our current progresses
- **Principle of Secret Key Generation**
- **Pre-industrial results of Secret Key Generation**
  - Single sense test bed and Implantation into LTE-TDD and Wifi Links at 2.4 GHz
  - LTE and Wifi Records – Secret Key Generation from these records
  - Dual sense test bed and implantation into Wifi Links networks 5 GHz
  - 5 GHz Wifi dual sense records – Secret Key Generation from these records
- **Conclusion - Technical maturity of Secret Key Generation Perspective for other RATs**
- **Annex**

Note: This paper is a follow up of Winncomm Munich 2013 and San Diego + Erlangen 2015 papers

"Active and passive eavesdropper threats within public and private civilian networks – Existing and potential future countermeasures – An overview"

"PHYSEC concepts for wireless public networks – introduction, state of the art and perspectives"

"Towards a key-free radio protocol for authentication and security of nodes and terminals in advanced waveforms"

"Physical layer security based protocols to effectively secure wireless communications without key distribution"

Recall of Project Phylaws: goals and outputs

- **MAIN GOALS:**

  To improve security of wireless links:
  - **. Radio cell and WLAN**
  - **. Slight to strong mobility (of terminal or scatters)**

  To search for key-free solutions based on Physec

  To experiment these solutions in real field

  To search for practical implantations in existing and future public RATs

- **AN ORIGINAL APPROACH:**

  Merging academic and industrial skills on radio-propagation, radio-communications and security.

  Integrating usual hypothesis with return of practical experience

  Considering any kind of threats at physical layer: passive Eve + various active Eve

  Concentrating on signaling and access phases of RATs, and not only on established data links.

PHYLAWS

PHYsical Layer Wireless Security

Project Coordinator:
Thales Communications and Security
François Delaveau
Tel: +33 (0)1 46 43 31 32
Fax: +33 (0)1 46 13 25 55
Email: francois.delaveau@thalesgroup.com
Project website: www.phylaws-ict.org

+ Five Partners:
Institut Mines-Telecom ParisTech (France,
Imperial College of Science, Technology and Medicine (Unted Kingdom),
Teknologian tutkimuskeskus VTT – OY (Finland),
Celeno Communications Israel Ldt (Israël).

Duration 4 years:
November, 2012 – October, 2016

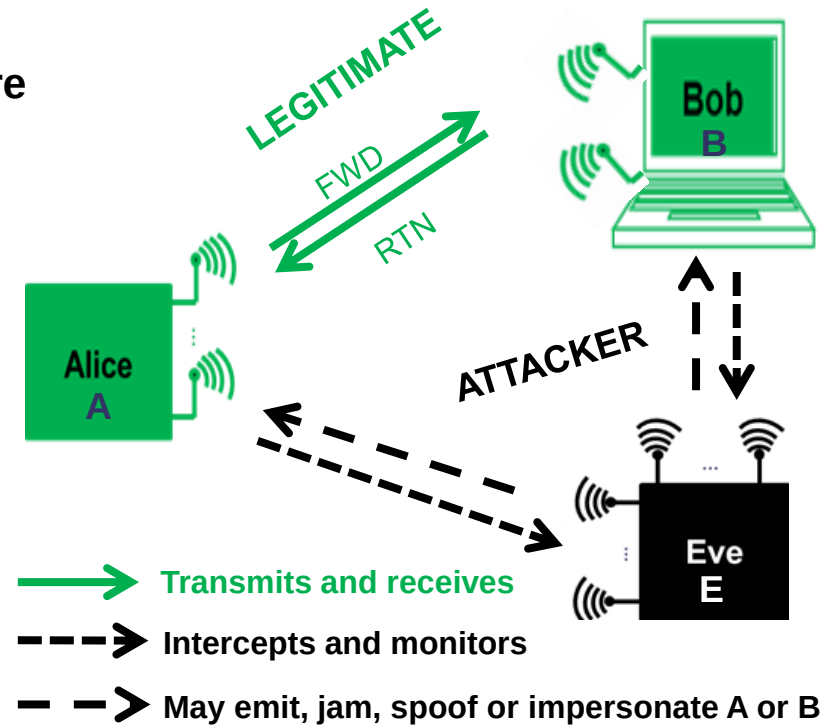
Funding scheme: STREP

Contract Number: CNECT-ICT-317562

Brief introduction to PHYSEC
Studied configuration of wireless links

- **LEGITIMATE links are Alice to/from Bob**
- **EAVESDROPPER and RADIO HACKER links are**
  - Alice to Eve…and even (active) Eve to Alice
  - Bob to Eve… and even (active) Eve to Bob
- **THREAT MODELS**
  - Passive Eve
  - Intelligent (protocol aware) jamming Eve
  - Man in The Middle / Wormhole Eve, etc.
- **Most usual academic hypothesis are:**
  - complete information of Eve about legitimate RATs/waveforms
  - no Information of Eve about legitimate Keys (e.g. K/Ki Keys on SIM cards)

=> **they may be no more valid nowadays especially into public RATs (ex : hacking of Subscriber data bases)**



OUR MAIN APPLICATIONS

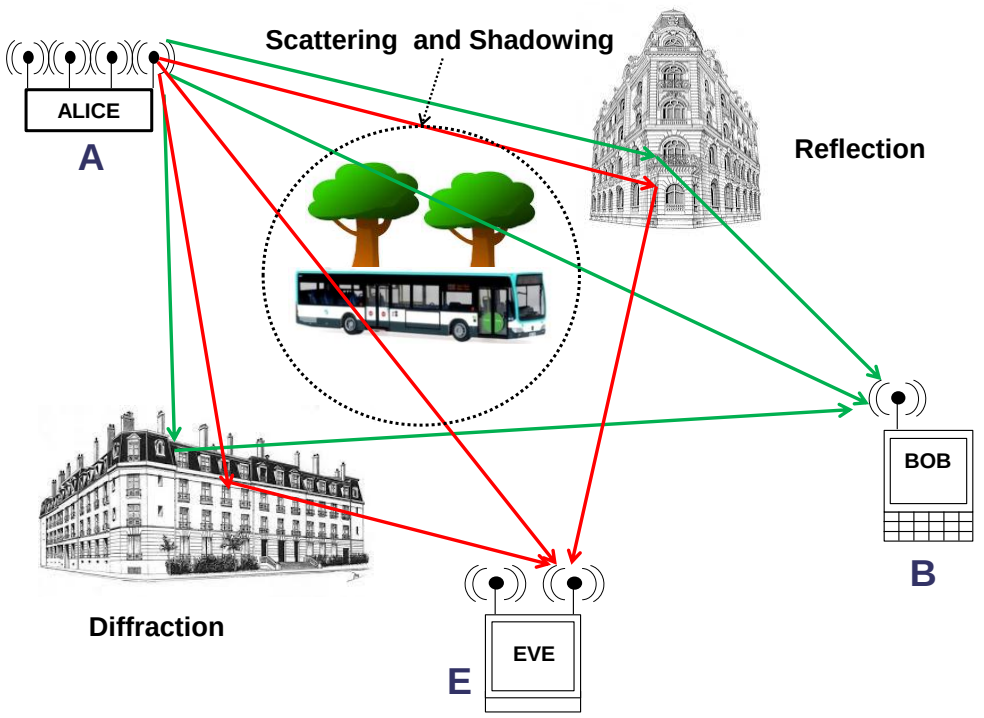
- **TRANSEC (Transmission Security) is the protection of the transmitted Alice's and Bob's signals face to interception and intrusion attempts of the user receiver (and even jamming and direction finding)**
- **NETSEC (Network Transmission Security) is the protection of the signalling and acces messages of Alice and Bob (usual solutions are authentication and integrity control, sometimes ciphering of signalling in military networks)**
- **COMSEC (Communication Security) is the protection of the data messages of Alice and Bob (voice, sms, mms, high speed data). Most of solutions are based on ciphering+integrity control schemes of signalling and data.**

Brief introduction to PHYSEC

Exploiting the randomness of radiochannel

(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



Complex wave propagation + unpredictable scattering objects

- Channel Randomness
- Received waveforms cannot be recovered by computation

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

Used for Secret Key Generation

Additional "radio" random for disturbing Eve:

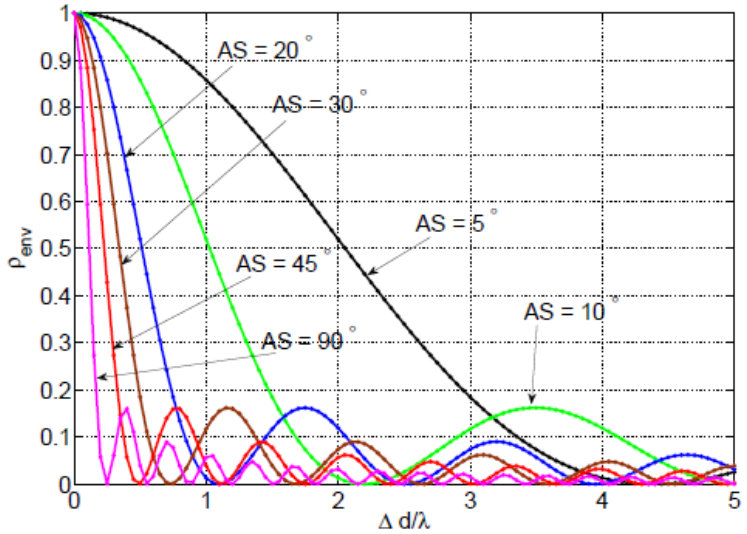
- **Alice and Bob Antennas: patterns and orientations**
- **Artificial noise and Beamforming : SNR advantage to A and B.**

Brief introduction to PHYSEC
Exploiting the randomness of radiochannel

Modelisation of the radio channel envelope correlation

- Rich scatterer environment => AS > 45°
  - => spatial decorrelation when Δd > λ/2
  - typical exemple : **NLOS outdoor and indoor**
- Poor scatterer environment => AS -> 5°
  - => Decorrelation when Δd > 4λ
  - typical exemple : **LOS rural outdoor and LOS indoor**

One-ring scatter model.
AS = Angular Spread



Channel envelope correlation vs Bob-Eve distance
(X. He, H. Dai, proceeding IEEE INFOCOM 2013)

Provisory Conclusion

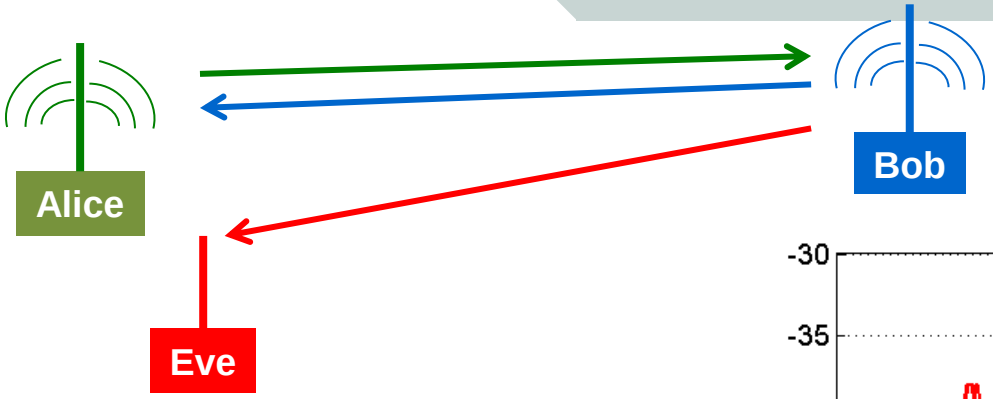
- When reciprocity of the channel
  - => Alice and Bob obtain the same channel estimation
- NLOS Bob – Eve dist. > λ/2 (WiFi 2.4 GHz -> 6 cm)
- or LOS Bob – Eve dist. > 5λ (WiFi 2.4 GHz -> 60 cm)
  - => Decorrelated waveforms at Bob and Eve sides
  - => Eve cannot obtain the same estimation than Bob
- Complex wave propagation and mobile obstacles
  - => Eve cannot compute Alice – Bob channel estimate

In any TDD cases, Secret Keys can be Generated from the channel randomness => Achieves security pairing !

In many TDD and FDD cases, Secret Codes can be computed => Provides information theoretic security !

Brief introduction to PHYSEC

Randomness of radiochannel – practical case

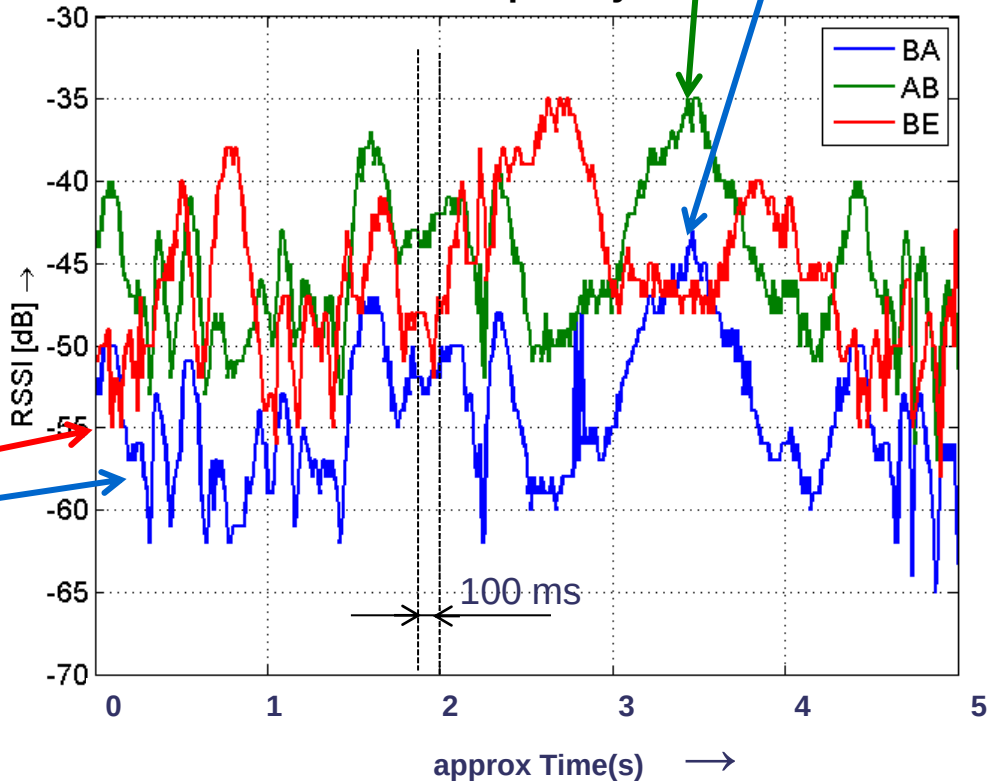


Same RSSI figure (after normalisation)

In sense Alice -> Bob

In sense Bob -> Alice

⇒ **Channel Reciprocity**



Different RSSI figure

In sense Bob -> Eve

In sense Bob -> Alice

⇒ **Channel spatial decorrelation**

Example of RSSI measurement over time

Signal is IEEE 802.11n, 2.4 GHz, BW=20 MHz E is located ~ 15cm next to Alice. Slight mobility of Scatterers.

Source: German project Prophylaxe

In addition:

Indoor time coherence is 50 to 100 ms

Brief introduction to PHYSEC

Phylaws Fundamentals and current progresses

Our Fondamentals = current academic knowledge about PHYSEC:

- Key-less security technique exploiting propagation randomness to establish secret
- Theory is OK since 1980's, academic reasearch is intensive, Applications in realistic radio-environment now exist (IoT in project Prophylaxe, Wireless and WLAN in project Phylaws)

Our current progresses = 3 protection schemes:

Presented Wincomm 2015 San Diego

- Secure Pairing (SP) with Tag Signals (TS) & Interrog. Ackn. Sequences (IASs)
  - ➔ new concepts invented, study in progress.
- Secret Key Generation (SKG)
  - ➔ pre-industrial application to IoT (project Prophylaxe)
  - ➔ Experimented for WLAN and LTE networks (project Phylaws)
- Artificial Noise-Beam Forming (AN-BF) + Secrecy Coding (SC)
  - ➔ Simulation OK, implantation in progress, promises inform. theoretic secrecy

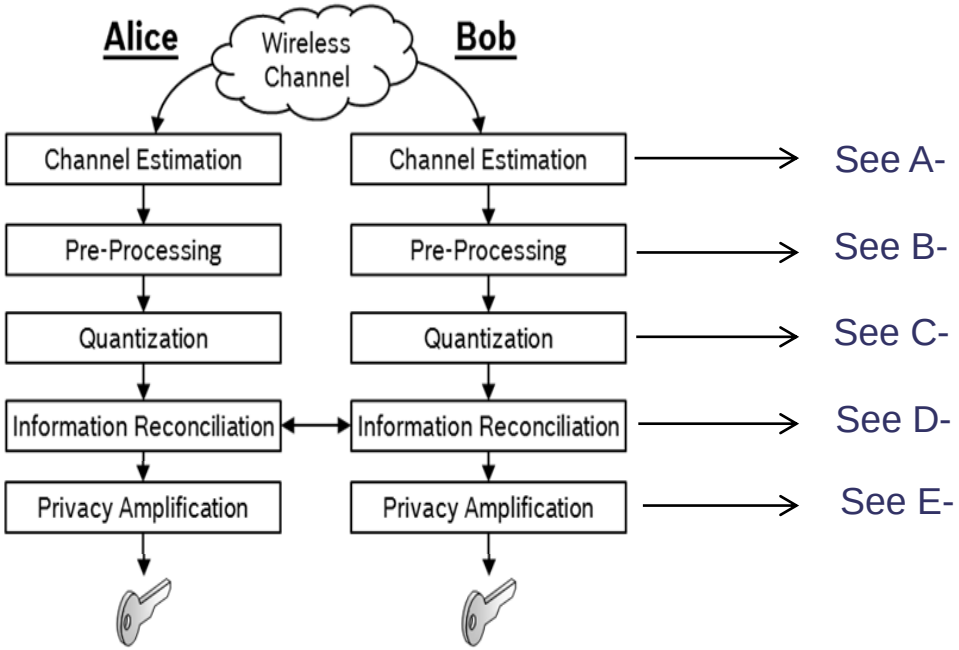
Following of the presentation

Complements on security flaws and threats of public RATs	www.phylaws-ict.org deliverable D2.1.
Complements on legitimate and attacker signals	www.phylaws-ict.org deliverables D2.4, D4.1, D4.3
Fundations of Physical layer security	www.phylaws-ict.org deliverables D2.3, D3.1, D3.2, D3.3
Complements and results about on Physec schemes developed in Phylaws	www.phylaws-ict.org deliverables D2.4, D4.1, D4.2, D4.3, D5.1, D6.1

Principles of Secret Key Generation

General procedure for exploiting radio channel randomness

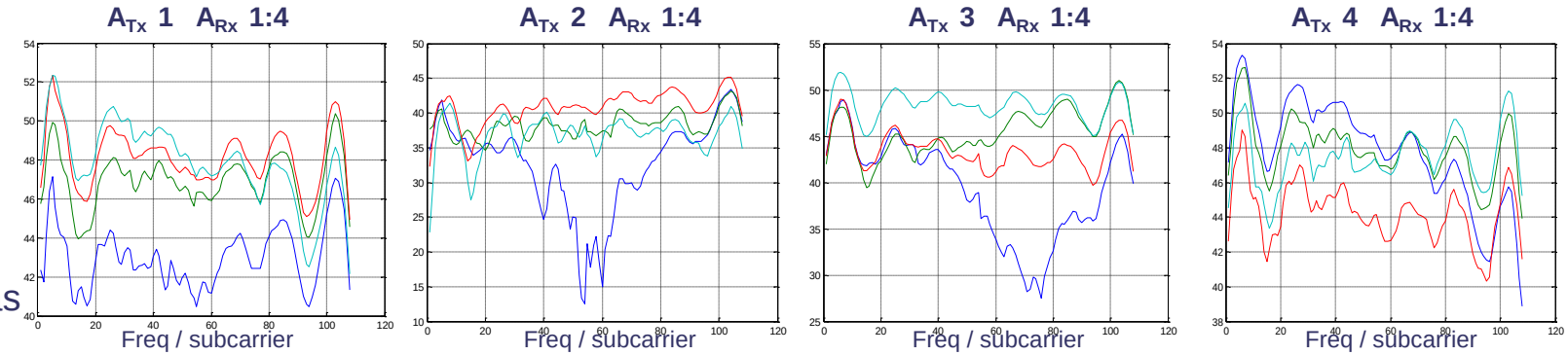
General procedure for channel-based secret key generation



A- Example of CSI measurement results (amplitude only shown) over one Non Data Packet (NDP) – fixed position

From IEEE 802.11ac chipsets (Celeno Communication Ltd) - 5 GHz, BW=40 MHz. Alice and Bob / Eve are 4 x 4 MIMO

LOS Tx and Rx are 4 antennas



Etc.

Principles of Secret Key Generation

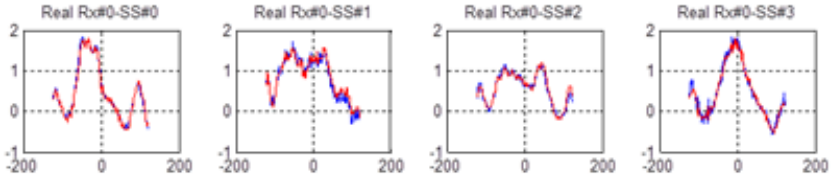
Basic Pre-processing

B- Need for pre-processing

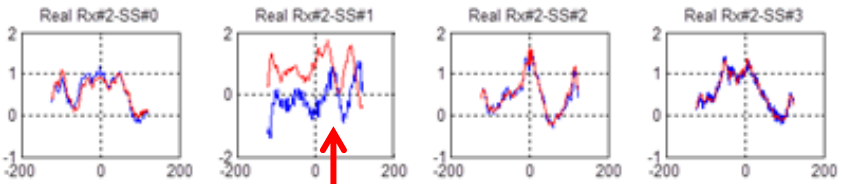
B1- Tx/Rx calibration

In order to take the plain benefit of Channel reciprocity: ex of a 4x2 MIMO config. at Wifi 802.11ac

Alice antenna 1 to 4 to Bob's antenna 1
Bob's antenna 1 Alice's antenna 1 to 4

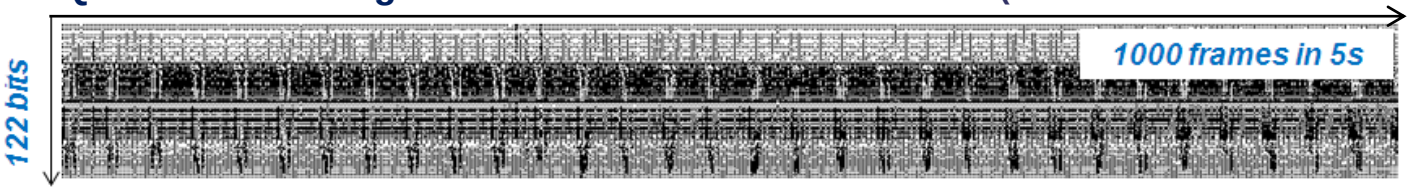


Alice antenna 1 to 4 to Bob's antenna 2
Bob's antenna 2 to Alice's antenna 1 to 4

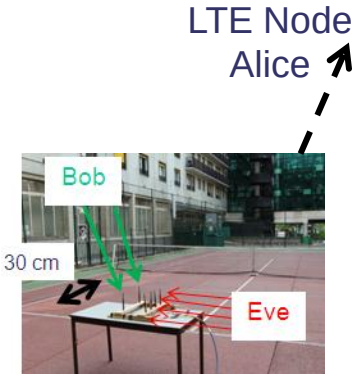


B2- Channel de-correlation techniques

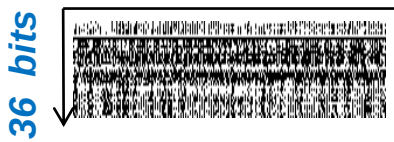
Quantization using all available Channel coefficients (case LTE 2.6 GHz - PSS BW 1.4 MHz - indoor LOS)



High temporal correlation that can be exploited by Eve to recover Bob's key



Resulting Quantization after classical correlation test



Selected Frame number reduced to 200 in 5s

=> No obvious pattern is repeated in the keys

=> enhances the channel randomness at input of SKG scheme

Principles of Secret Key Generation

Quantization

C- Core of the SKG scheme = Quantization

- Objective: generate binary symbols from channel measurements
- Possibility to quantize received amplitude (RSSI) or Channel State Information including amplitudes + phases (CSI)

Classical RSSI quantization schemes

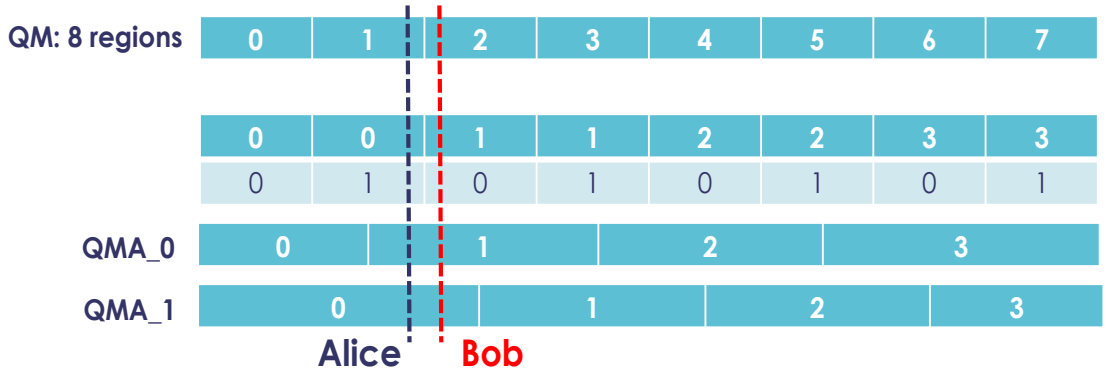
Robust but low richness for randomness extraction

Advanced CSI quantization scheme:

"Channel Quantization Alternate" (Wallace 2010)
+ High richness random extraction
+ Bit disagreement reduction

. CSI based,
. **2 alternate quantization Maps computed by Alice and Bob from CSIs**
. geometrical criterion

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



The Alice choses symbol 0 & informs Bob about her map (QMA_1)
Thus Bob choses symbol 0 on ma QMA_1 with reduced mismatch risks at low SNR
No information leakage (map index is transmitted, symbol not)

Principles of Secret Key Generation

Reconciliation – Privacy amplification

D- Reconciliation

- Objective: correct bit disagreement between Alice and Bob
- Based on sketch transmission from Alice to Bob

  + Error bit Correction (basic Forward Error Code)
- Well known and similar to classical error correction (applied here to key bits)

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

E- Privacy amplification

- Objective: mitigate any information leackage towards Eve (after reconciliation)
- Based on entropy estimation + hash functions with key length reduction + test of NIST or Intel RNG criterias
- Well known and similar to basic techniques used in crypto.

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

Pre-industrial results of Secret Key Generation

- Test bed for single sense radio channel measurement

Estimation of wireless radio Channel in real field – test bed 0.4 – 4 .4 GHz

- **PURPOSE**

Compatible with main RATs

- WiFi (2.4GHz)
- LTE (800/2600MHz)
- UMTS (2.1GHz)
- GSM (900/1800MHz)

Achieve significant recording capabilities

- Up to 6 channels for WiFi/LTE 20MHz
- Up to 12 channels for UMTS/GSM or LTE 10MHz

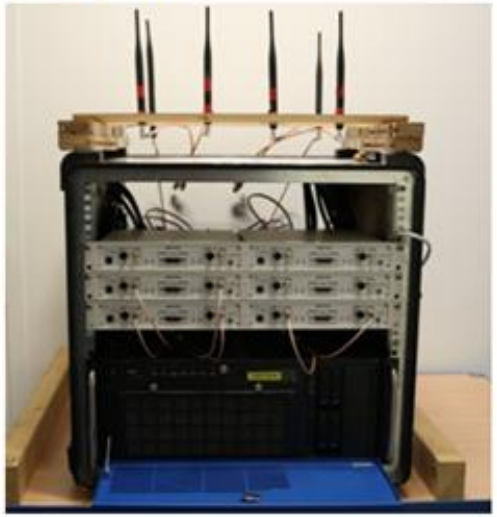
Real field records of AP and BTS, terminals

Measurements of radio channel

Model of Eve

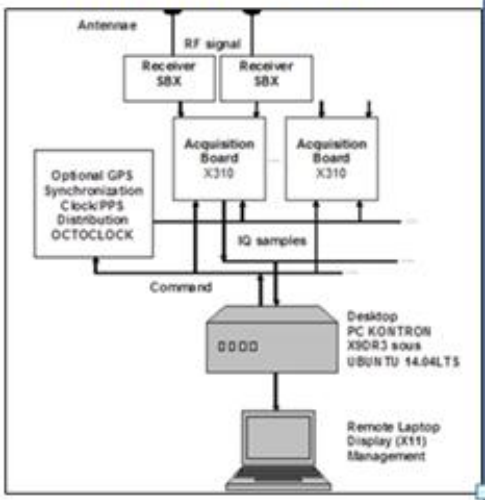
WiFi Access Point

- **VIEW**



Base Transceiver Station (BTS)

- **ARCHITECTURE**



RADIO CHARACTERISTICS:
Analog BW: 120MHz
Sampling IQ: 200MHz
RF range: 400MHz 4.4GHz
NF: 5dB (Typical)

SYNCHRONIZATION
Octoclock board: PPS, 10MHz, GPS

INTERFACE:
PCIe,
Ethernet

STORAGE/PROCESSING:
PC MP sous UBUNTU 14.04

IHM: Remote X11

Pre-industrial results of Secret Key Generation

Single sense indoor/outdoor signals records

6 Rx SIMO Records and analysis at LTE and Wifi carriers in different radio environments

Wifi records in the following

Open space

LTE records in the following

Indoor/Outdoor

LTE records in the following

Classroom

Street

LTE records in the following

Amphitheater

Corridor

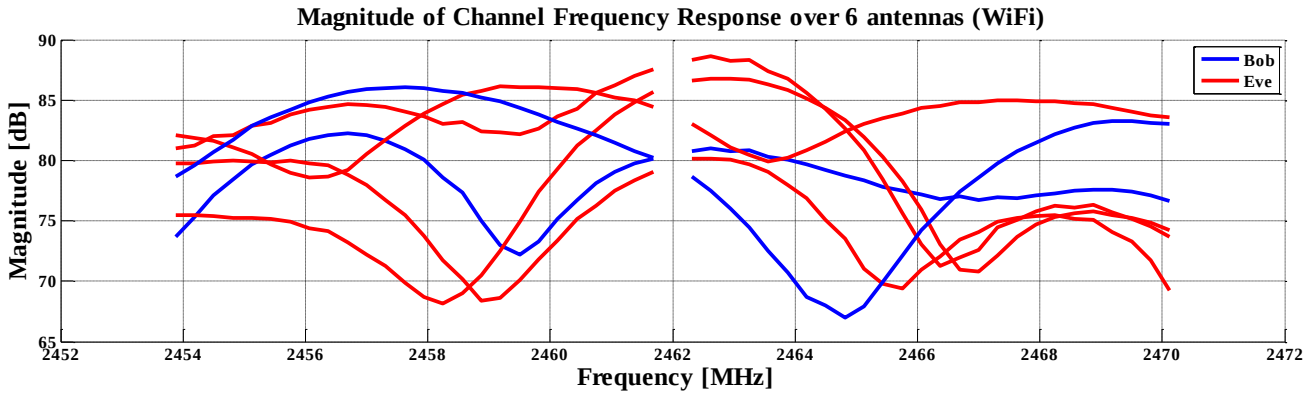
Pre-industrial results of Secret Key Generation

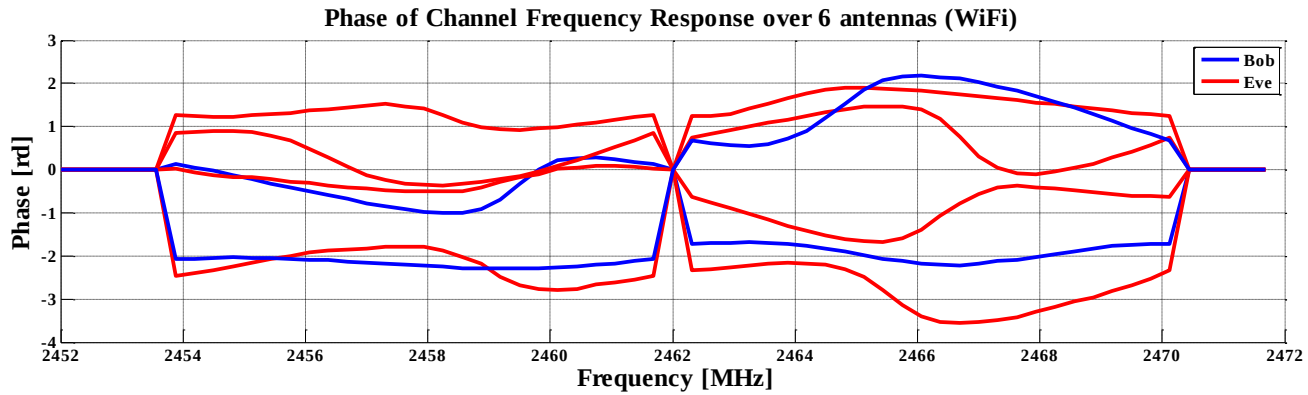
Single sense indoor/outdoor radiochannel extraction

Estimation of wireless radio Channel in real field – Wifi 2.4 GHz & LTE results

Example of Channel Frequency Response over Wifi carrier

Even in this indoor LOS case, the spatial diversity is significant





Confirms previous papers

W.C. Jakes Jr., « Microwave Mobile Communiations ». Piscataway, NJ: Wiley-IEEE Press

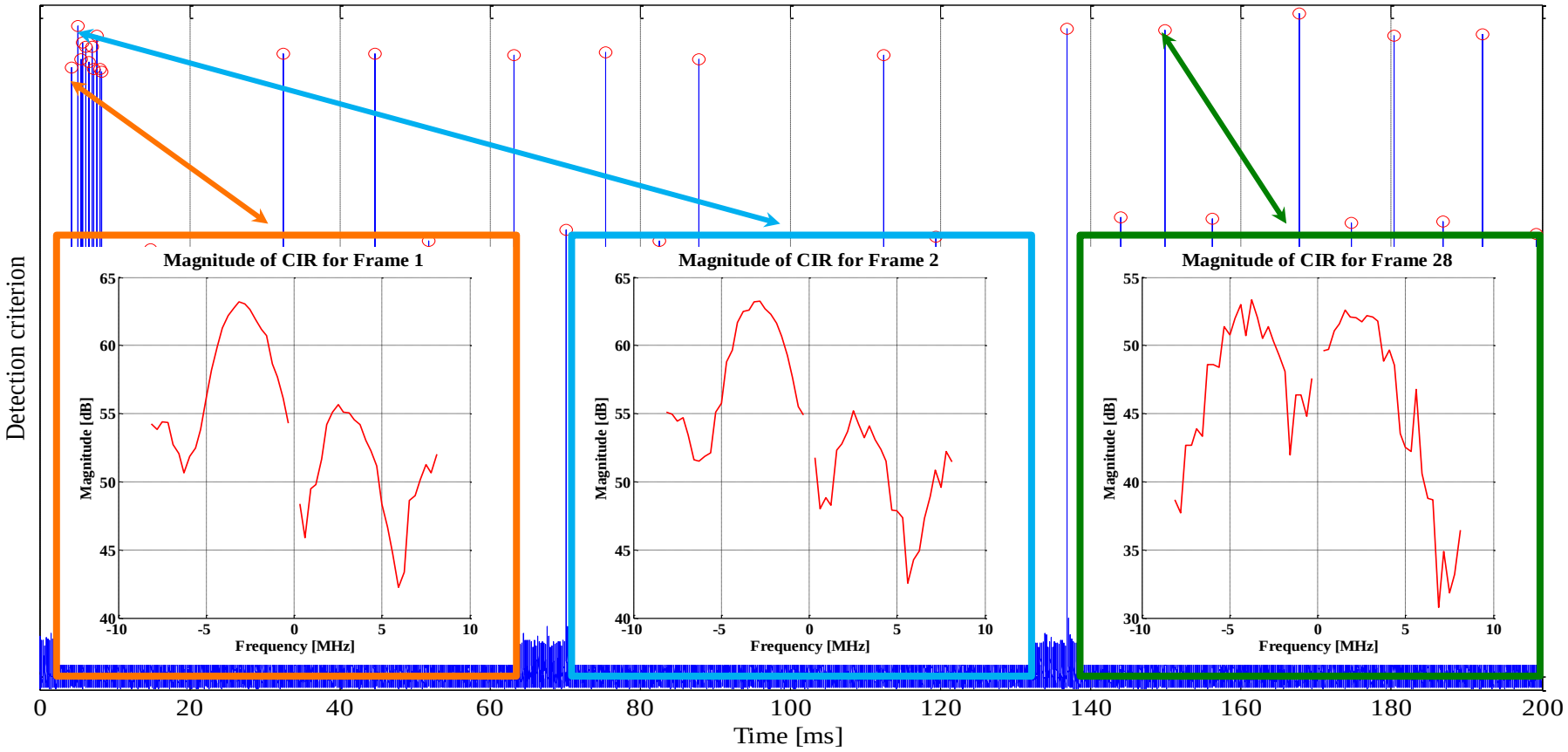
J.Wallace and R.Sharma, "Automatic secret keys from reciprocal MIMO Wireless channels: measurement and analysis," IEEE Trans. on info. for. and sec., September 2010

Pre-industrial results of Secret Key Generation

Single sense indoor/outdoor radiochannel extraction

Estimation of wireless radio Channel in real field – Wifi 2.4 GHz & LTE results

Example of Channel Frequency Response over short to mean time



- **High time diversity enables computation of good secret keys (length, randomness)**
- **Allow to regenerate secret-key bits after 100 ms (indoor case)**

Pre-industrial results of Secret Key Generation

- Single sense SKG for LTE and Wifi 802.11n 2.4 GHz

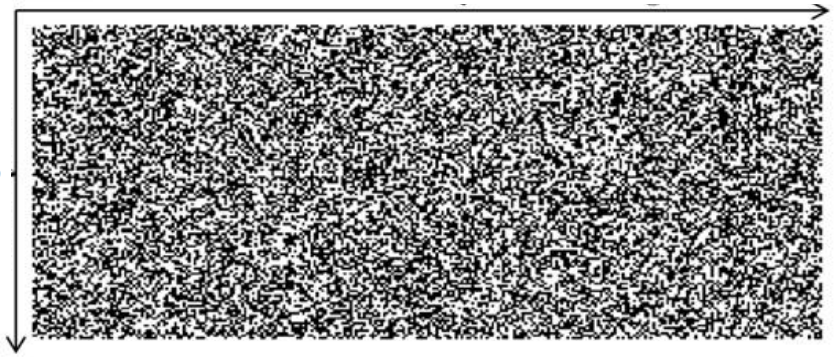
Outdoor Street

Wifi and LTE results
SKG is single sense
SKG based on CSI

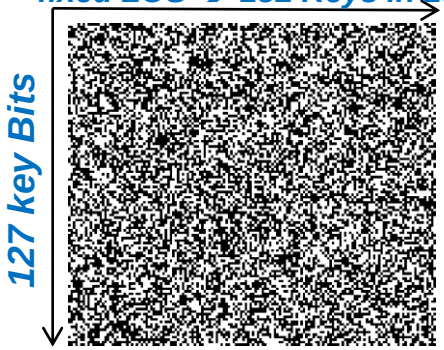
Indoor office

Indoor classroom

LTE 2600 MHz Urban Street ➔ 284 Keys in 5s

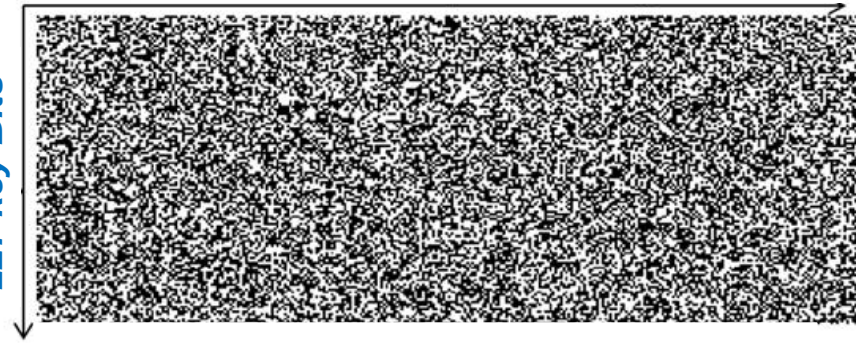


Wifi 2400 MHz Indoor fixed LOS ➔ 152 Keys in 2s

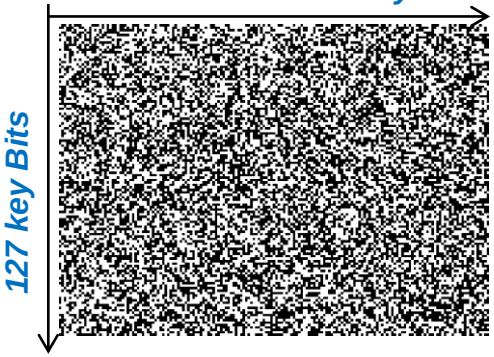


LTE indoor 2645 MHz Classroom fixed position ➔ 49 Keys in 5s

LTE 800 MHz Urban Street ➔ 348 Keys in 5s



Wifi 2400 MHz Indoor. Slight mobile NLOS ➔ 171 Keys in 2s



EVEN IN THE MOST DIFFICULT CASE, SKG WORKS WELL.

NOTE : ONE KEY WOULD BE SUFFISANT FOR PROTECTION OF SIGNALLING AND ACCESS MESSAGES.

Pre-industrial results of Secret Key Generation

NIST criterias at SKG for LTE-TDD and Wifi

Focus on key quality after SKG - Wifi and LTE

NIST frequency monobit tests

Determines whether the numbers of 0s and 1s in the key are approximately the same as would be expected for a truly random sequence.

LTE	Indoor (2.6GHz)	Outdoor (2.6GHz)
Quantization only	**98%** (48/49)	**99%** (281/284)
Quant+Reconciliation +Amplification	**100%** (49/49)	**100%** (284/284)

WIFI indoor	LOS (2.4 GHz)	NLOS (2.4 GHz)
Quantization	**87%** (132/152)	**100%** (171/171)
Quant+Reconciliation +Amplification	**99%** (151/152)	**100%** (171/171)

NIST Runs tests

Determines whether the oscillation between 0s and 1s is too fast or too slow.

LTE	Indoor (2.6GHz)	Outdoor (2.6GHz)
Quantization only	**27%** (13/49)	**80%** (228/284)
Quant+Reconciliation +Amplification	**100%** (49/49)	**100%** (284/284)

WIFI Indoor	LOS (2.4 GHz)	NLOS (2.4 GHz)
Quantization only	**84%** (128/152)	**99%** (169/171)
Quant.+Reconciliation +Amplification	**98%** (149/152)	**99%** (170/171)

Other tests in are progress (NIST and others, entropy etc.)

Pre-industrial results of Secret Key Generation

- Dual sense Test bed for Wifi 802.11ac 5 and 2.4 GHz

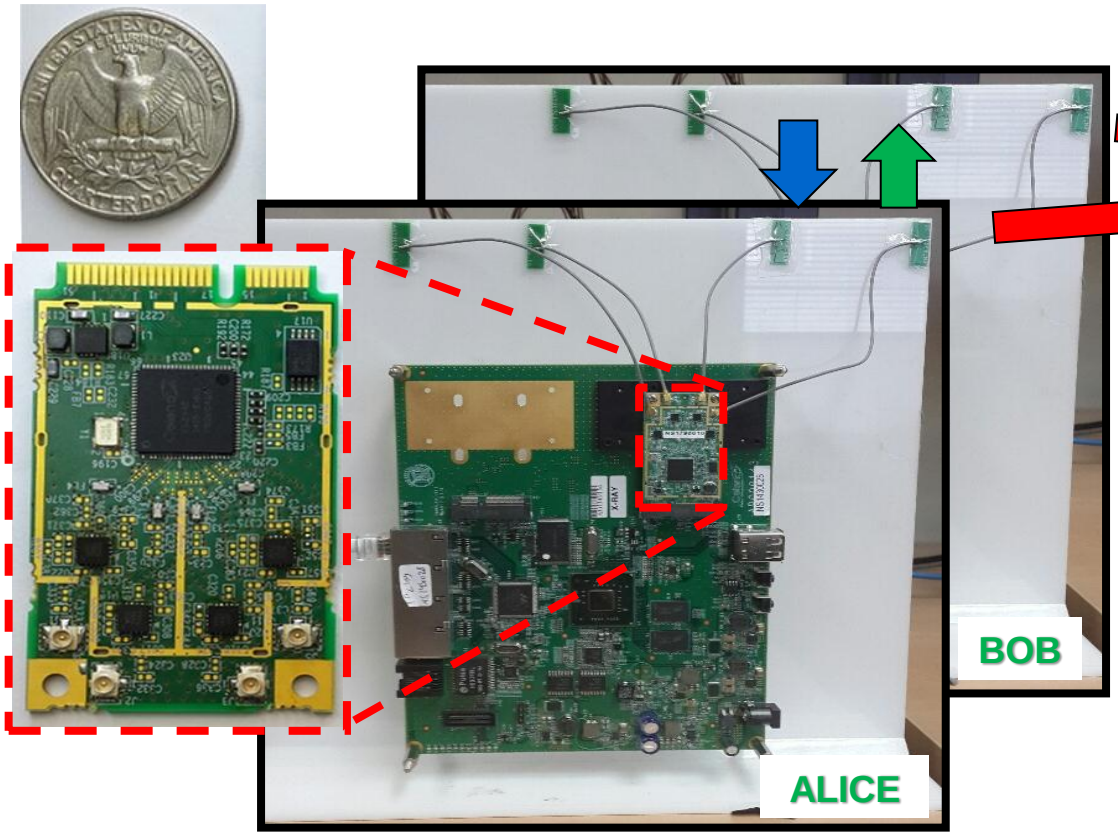
RECENT NEW RESULTS

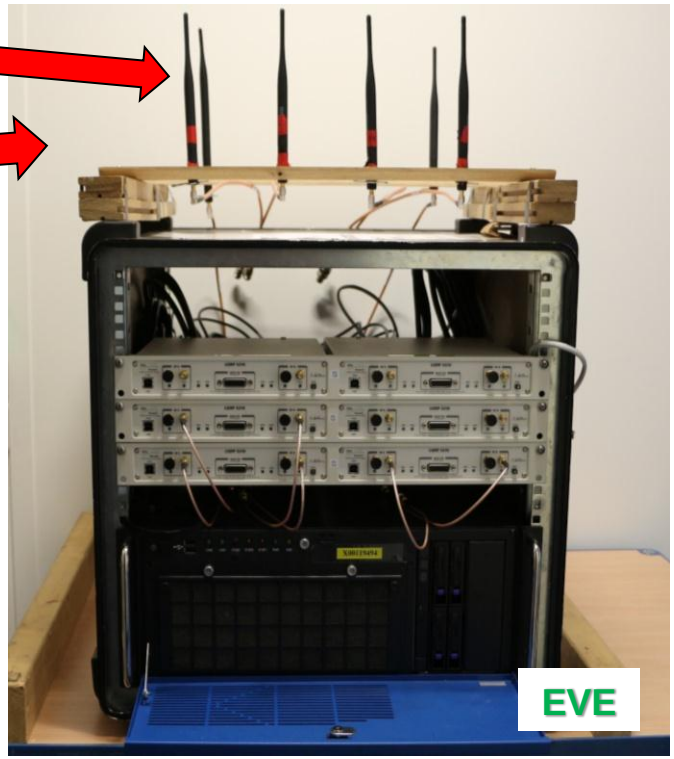
LEGITIMATE PART

Base = Chipset CL 2440 + Host board + PCI interface built by Celeno Communication Ltd

ATTACKER PART

1 to 6 antennas are dedicated to Eve





LEGITIMATE PART NOW
CEL real Wifi 4x4 MIMO BOARDS ⊃

EAVESDROPPER PART NOW
USRP BOARDS AND 6x1 SIMO Rx ⊃

Pre-industrial results of Secret Key Generation

Dual sense Wifi CIR indoor measurTs (802.11ac 5.2 GHz - BW 40 MHz)

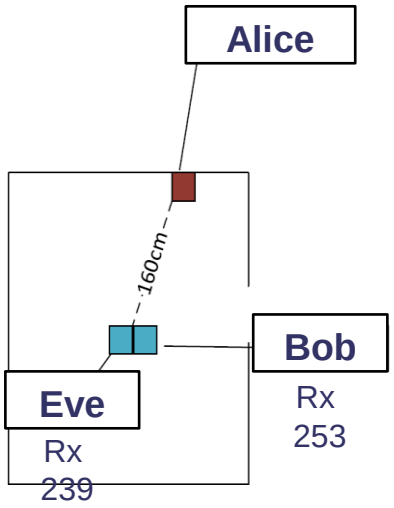
RECENT NEW RESULTS

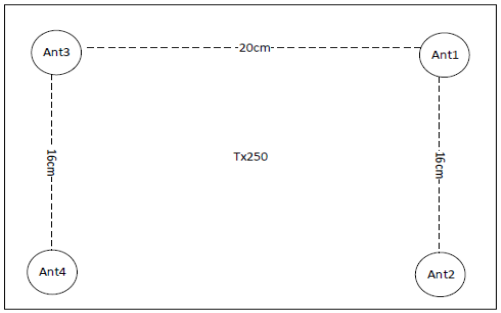
Indoor experiments by Celeno Communication Ltd:

The setup is 2 RX 4x4 MIMO receive a unique Non Data Packet (NDP)

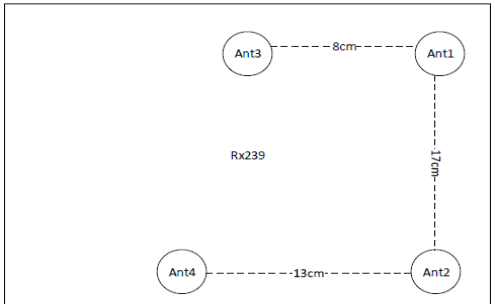
One RX is 1 to 4 antenna Bob, One RX is 4 antenna Eve

The signal is 40MHz 4 SS





Alice's antennas



Bob's, Eve's antennas

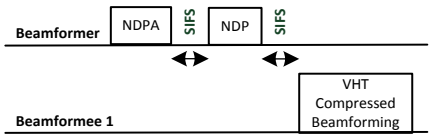
Scenarios - description:

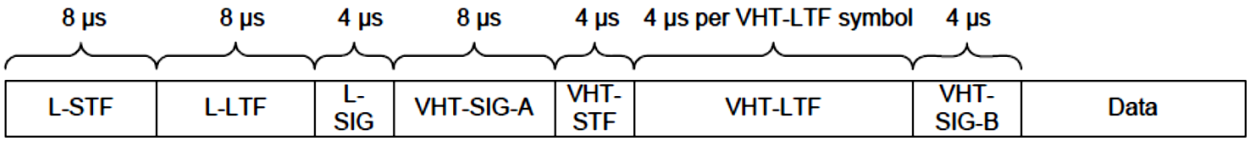
Bob and Eve are very close to each other

Alice is 1.6 meter distance

All is static

Wifi Channel sounding procedure





Pre-industrial results of Secret Key Generation

Dual sense SKG on Wifi 802.11ac indoor CIRs (5.2 GHz - BW 40 MHz)

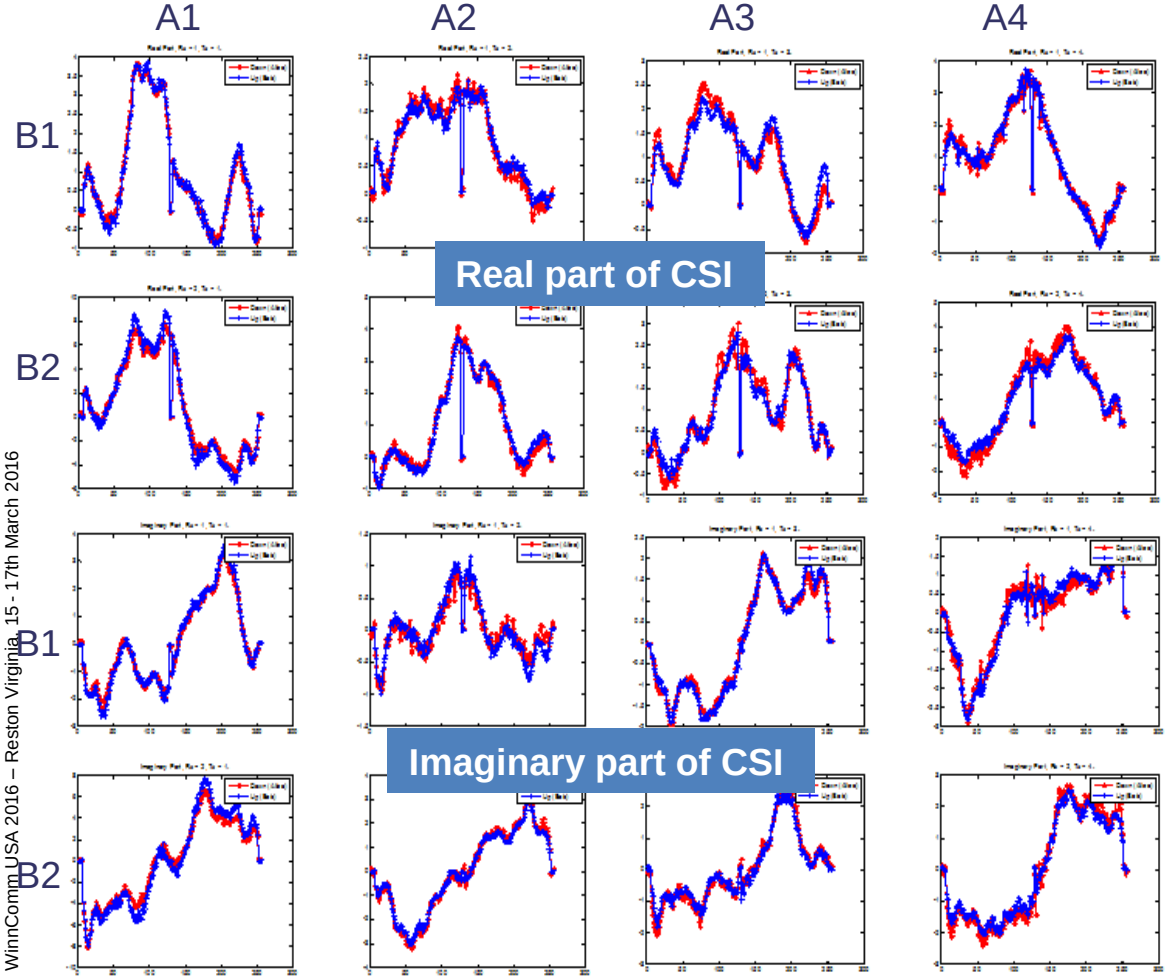
RECENT NEW RESULTS

SKG scheme dual sense, algo. without pre-processing

No Space de-correlation,
No Time neither Freq. de-corr.
Reconciliation with FEC=BCH(15,127),
Amplification with 2-Universal Hash

Use of dual sense CSIs: B2 Alice -> Bob and Bob -> Alice

Alice is 4 Tx/Rx antennas A1 to A4 ; Bob is 2 Antennas B1 and B2



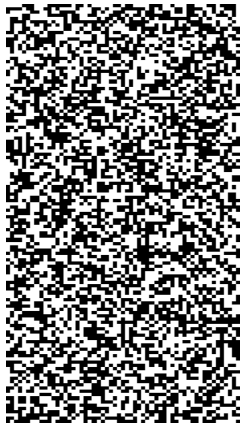
Generation of 128 bits keys

samples computed from one WiFi frame

Keys after Quantization

BOB'S SIDE

Keys after amplification



Test of key quality

NIST test	Freq. Monobit	Runs
After Quantization	31/57	22/57
After Amplification	57/57	57/57
Use of all generated bits after Q/after A	Pass / Pass	Fail / Pass

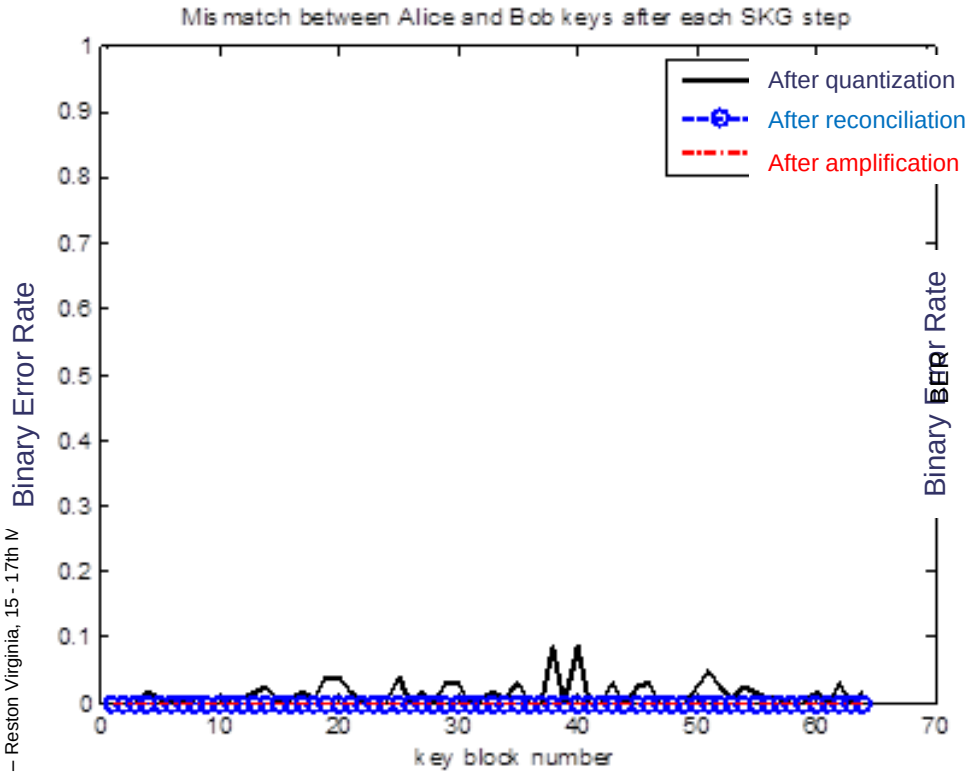
Pre-industrial results of Secret Key Generation

Dual sense SKG on Wifi 802.11ac indoor CIRs (5.2 GHz - BW 40 MHz)

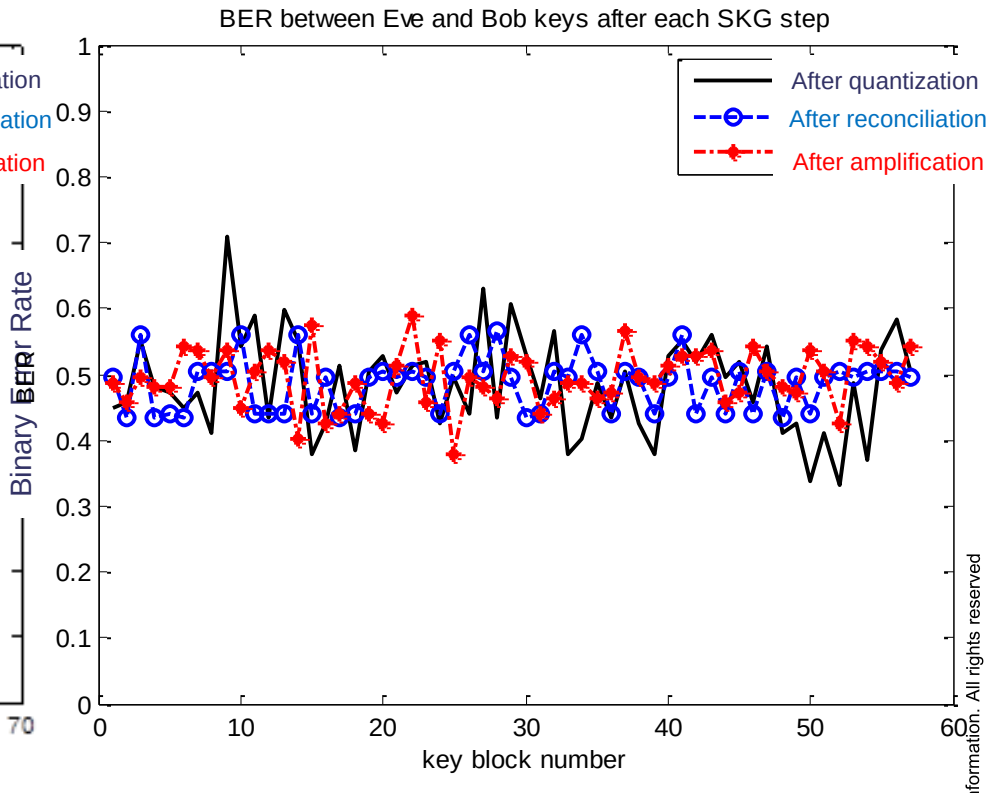
RECENT NEW RESULTS

SKG scheme dual sense, without pre-processing (following)

Test of Key agreement between Alice and Bob



Test of Information leakage towards Eve



AT BOB'S SIDE:

=> BER is null after reconciliation

⇒ Reconciliation + key vérification are OK at Alice and Bob

AT EVE'S SIDE: Near 0.5 BER

⇒ No/low information of Eve on Alice's and Bob's keys

Thank you for your attention

Find more information on our website
www.phylaws-ict.org

ANNEX

Some references

- ZEIT, “Wie Merkels Handy abgehört werden konnte,” 18 12 2014. [Online]. Available: http://www.zeit.de/digital/datenschutz/2014-12/umts-verschluesselung-umgehen-angela-merkel-handy
- Metronews, “Une énorme faille de sécurité permet d'écouter vos appels et de lire vos SMS,” [Online]. Available: http://www.metronews.fr/high-tech/une-enorme-faille-de-securite-permet-d-ecouter-vos-appels-et-de-lire-vos-sms/mnlv!YngDbOgrtHFYk/
- http://media.ccc.de/browse/congress/2014/31c3_-_6531_-_en_-_saal_6_-_201412272300_-_ss7map_mapping_vulnerability_of_the_international_mobile_roaming_infrastructure_-_laurent_ghigonis_-_alexandre_de_oliveira.html
- https://firstlook.org/theintercept/2015/02/19/great-sim-heist/
- M. Bloch and J. Barros, Physical-Layer Security, Cambridge University Press, 2011.
- J.-C. Belfiore, C. Ling and L. Luzzi, “Lattice codes achieving strong secrecy over the mod-Λ Gaussian channel,” in IEEE International Symposium on Information Theory Proceedings, Cambridge, USA, 2012
- J. W. Wallace and R. K. Sharma, “Automatic secret keys from reciprocal MIMO Wireless channels: measurement and analysis,” *IEEE Transactions on information forensics and security,* vol. 5, no. 3, pp. 381-392, September 2010.
- F. Delaveau, A. Evestti, A. Kotelba, R. Savola and N. Shapira, “Active and passive eavesdropper threats within public and private cililian networks - Existing and potential future countermeasures - An overview,” in Winncomm, Munich, Germany, 2013.
- F. Delaveau, C. Ling, E. Garrido, J.-C. Belfiore and A. Sibile, “Physec concepts for wireless public networks - Intoduction, state of the art, perspectives,” in Winncomm, Munich, Germany, 2013.
- T. Mazloum, F. Mani and A. Sibille, "Analysis of secret key robustness in indoor radio channel measurements," in *IEEE Vehicular Tech. Conf.*, Glasgow, Scotland, 2015.
- X. He, H. Dai, “Is link signature dependable for Wireless Security?” in proceeding IEEE INFOCOM 2013
- Web site of the project Phylaws (Funded by EC-FP7-ICT-2011-8 GN 317562): www.phylaws-ict.org
- Web site of the project Prophylaxe (funded by German BMBF GN 16KIS0005K): www.ict-prophylaxe.de

ANNEX
Acronyms

AN - BF	Artificial Noise – Beam Forming
BCH	Bose Ray-Chaudhuri Hocquenghem
BER	Bit Error Rate
BTS	Base Transceiver Station
CIR	Channel Impulse Response
CFR	Channel Frequency Response
CQA	Channel Quantization Algorithm
COMSEC	Communication Security
CRS	Cell-specific Reference Signal
FDD	Frequency Division Duplex
FEC	Forward Error Correction
FuDu	Full Duplex
GSM	Global System for Mobile communications
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
LDPC	Low Density Parity Check
LOS	Line Of Sight
LTE	Long Term Evolution
MAC	Media Access Control
MISO/MIMO	Multiple Input Single Output / Multiple Input Multiple Output
NIST	National Instrument of Standards and Technology
NETSEC	Network Transmission Security
NLOS	Non Line Of Sight
PHYSEC	Physical Layer Security
OoM	Order of Magnitude
PSS / SSS	Primary Synchr. Sequence / Secondary Synchr. Seq. (LTE)
RAT	Radio Access Technology
Rx	Receiver
SIM	Subscriber Identity Module – Self Interference Mitigation
SISO/SIMO	Single Input Single Output / Single Input Multiple Output
SKG,SC,SP	Secret Key Generation , Secrecy Coding, Secure Pairing
SNR, SINR	Signal to Noise Ratio, Signal to Noise + Interference Ratio
SS7	Signaling System No.7
STF, LTF	Short Training Field, Long Training Field (Wifi)
TBD - TBS	To Be Defined - To Be Studied
TDD	Time Division Duplex
TMSI	Temporary Mobile Subscriber Identity
TRANSEC	Transmission Security
Tx	Transmitter
UIM	User Identity Module
UMTS	Universal Mobile Telecommunications System