Funded by EC-FP7-ICT-2011-8 GN 317562
www.phylaws-ict.org

PIMRC'2016 - Workshop W8
Deployment perspectives of Physical Layer Security into wireless public RATs
2016 September 4 morning

Paper 5: Implantation and experimentation of Physec security schemes into Wifi radio links - Results and relevant standardization perspectives

Nir Shapira (Celeno Communications)
Christiane Kameni Ngassa, François Delaveau, Renaud Molière (Thales Communications

IEEE pimrc'16
27TH ANNUAL IEEE INTERNATIONAL SYMPOSIUM ON PERSONAL, INDOOR AND MOBILE RADIO COMMUNICATIONS
4-7 SEPTEMBER, VALENCIA, SPAIN

Agenda

- **Brief introduction to PHYsical Layer SECurity (PHYSEC):**
  - Studied configuration of wireless links - basic processing architectures
- **Pre-industrial results of Secret Key Generation**
  - Test Bed – Records of Wifi signals – CIR measurements - implantation of SKG analyses in offline analysis
  - Experiments for and Wifi 802.11ac links at 2.4 and 5 GHz.
    - Bi-directional CIR measurement
    - SKG results, impact of channel de-correlation pre-processing
- **Industrial results of Secrecy Coding**
  - Artificial Noise and Bean Forming – principle
  - One particular implantation of Secrecy Coding under radio advantage - Security Analysis from Simulation results.
  - Experiments of Secrecy Coding schemes under real Wifi links
- **Conclusion - Way ahead.**
- **Annex** (References. Acronyms. Causes of the randomness of radio channels, Perspectives of secure pairing. Focus on SKG implantation - principle and algorithm. Implantation details about our secrecy coding scheme. Wi-Fi and LTE-TDD indoor/outdoor environments)

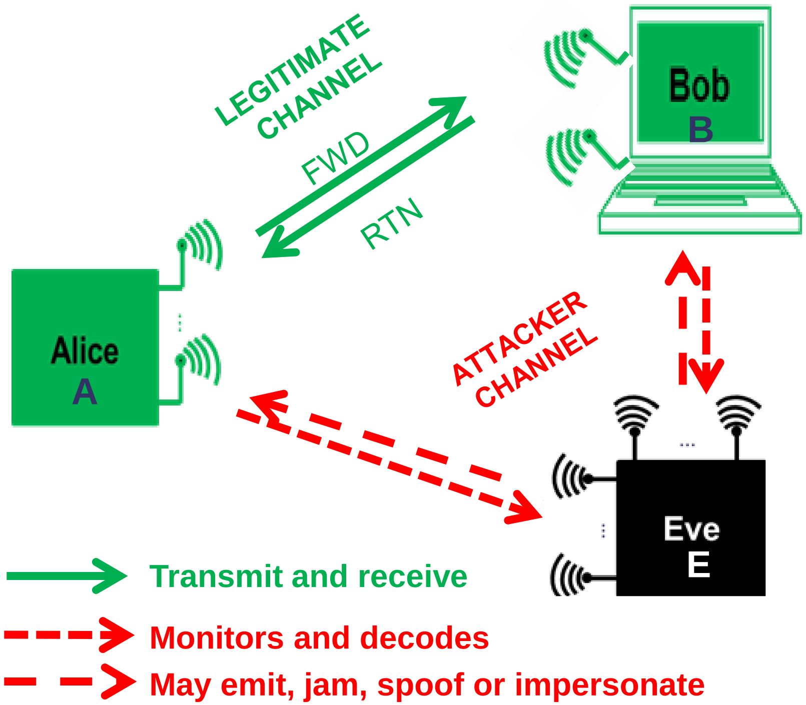
PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Brief introduction to to PHYsical Layer SECurity (PHYSEC)

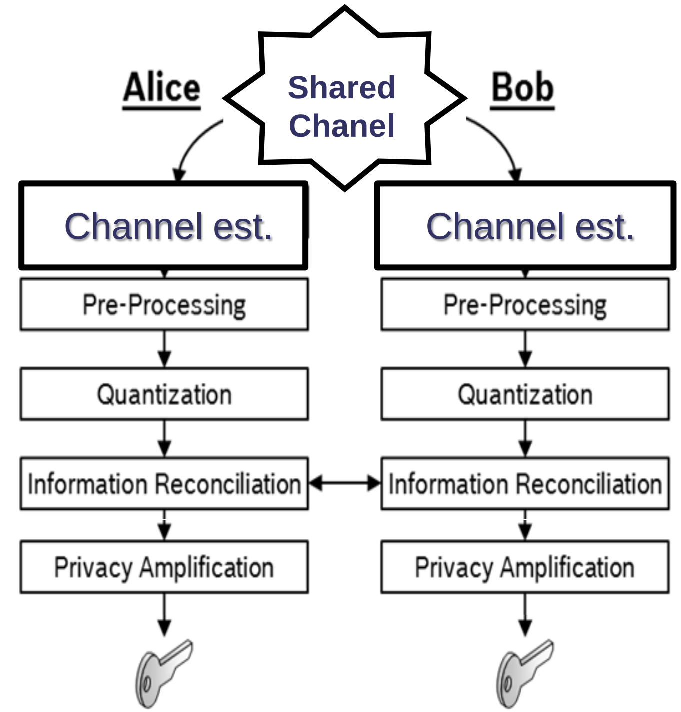
Studied configuration of Wireless links – basic processing architectures

A) wiretap model of legitimate radio transmitters and attacker over the air

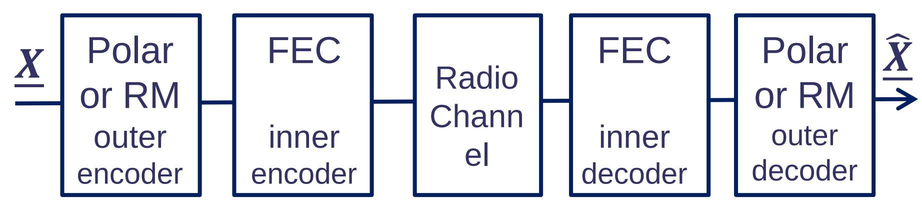
- **LEGITIMATE links are Alice to/from Bob**
- **EAVESDROPPER and RADIO HACKER links are**
  - Alice to Eve…and even (active) Eve to Alice
  - Bob to Eve… and even (active) Eve to Bob
- **THREAT MODELS**
  - Passive
  - Intelligent (protocol aware) jamming,
  - Man in The Middle / Wormhole, etc.



B) Basic Architecture of Secret Key Generation



C) Basic Architecture of Secrecy Coding



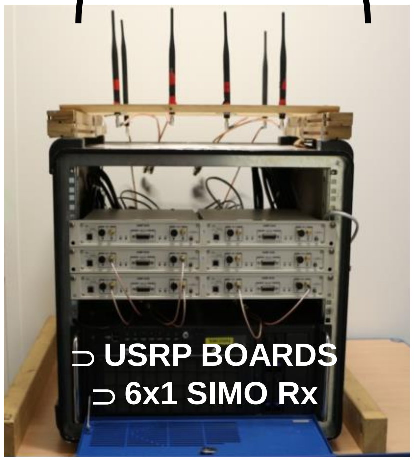
PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

SKG EXPERIMENTS OVER REAL WI-FI AND LTE LINKS

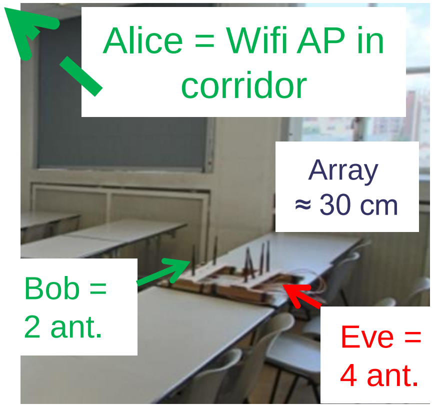
PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

SINGLE SENSE MEASUREMENT AND EVESDROPPING

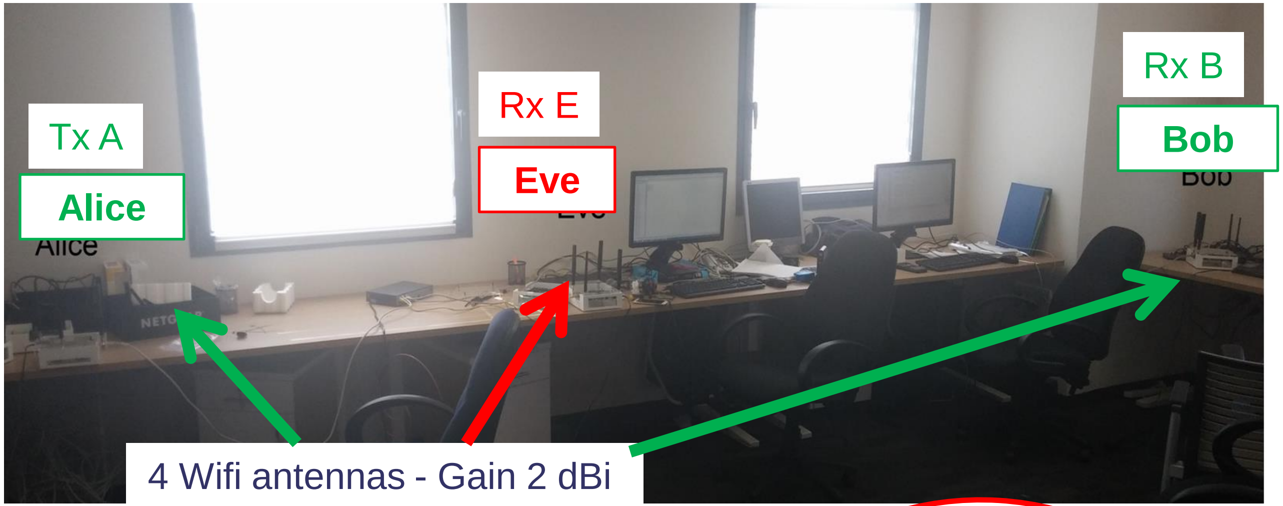
1 to 6 antennas

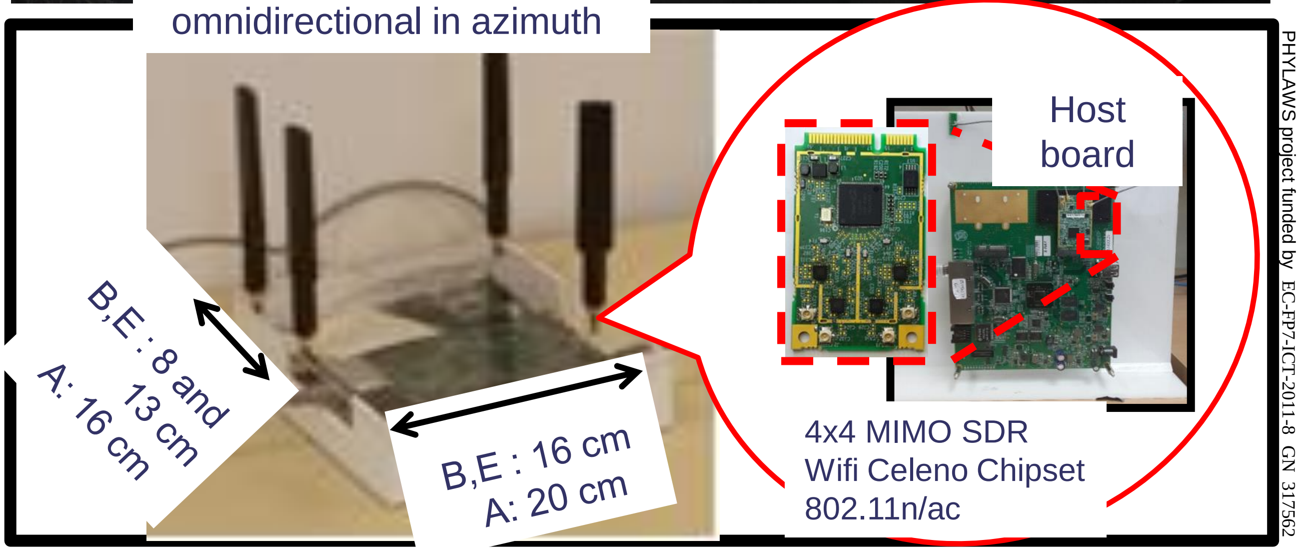


Classroom measurement



BI-DIRECTIONAL LEGITIMATE + EAVESDROPPER LINK



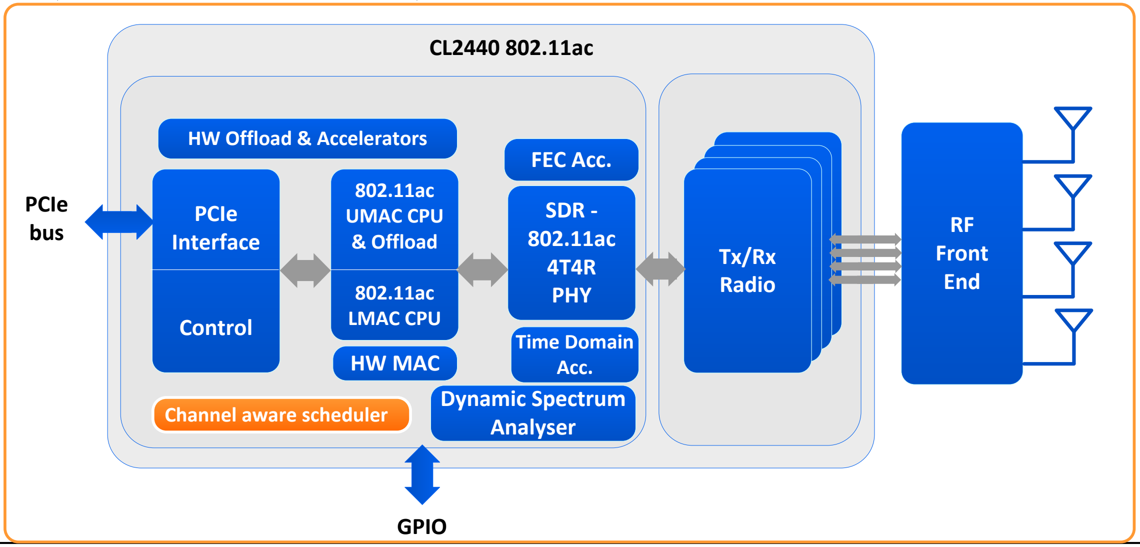


PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

- **Wi-Fi testbed will be based on Celeno's CL2400 4x4 802.11ac W2 chipset**

- **Celeno's CL2400 chipset family is based on an strong SDR architecture**
  - DSP based PHY (OFDM and matrix manipulations engine, including all beamforming operations), using best in class Ceva's XC4210 DSP core (running 64 MACS at 480MHz)
  - Flexible MAC based on 2 processor cores for lower and upper MAC layer

- **Test bed enables establishment of real WiFi links with 3'rd party, commercial client devices**
  - Two chip flavors: CL2440 supporting 5GHz (80MHz channel BW) and CL2442 supporting 2.4GHz (20/40MHz channel BW)

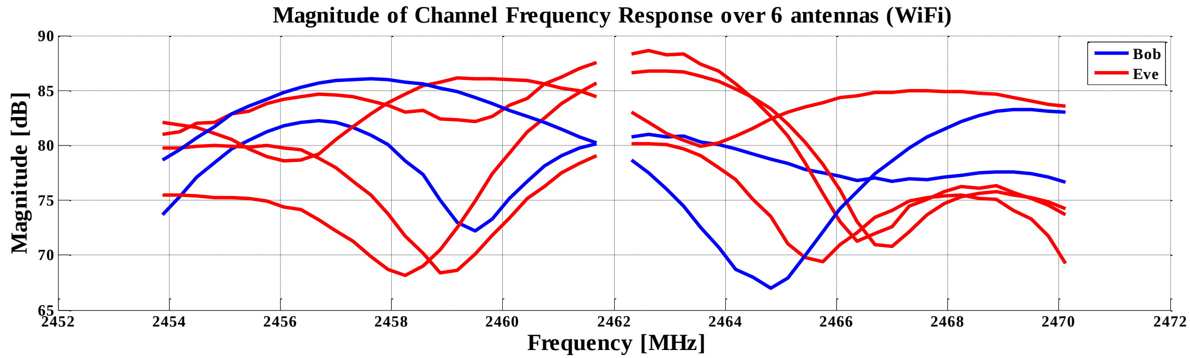


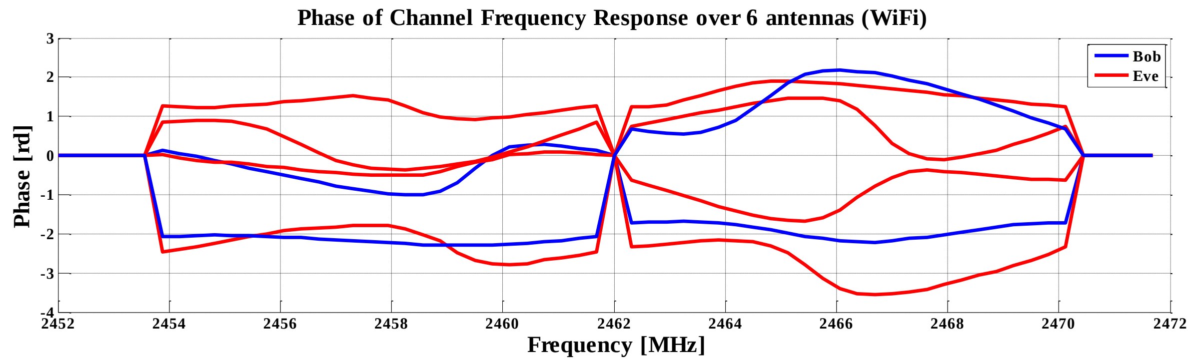
Pre-industrial results of Secret Key Generation

Records of Wifi signals – CIR measurements

SINGLE SENSE MESUREMENT OVER 6 ANTENNAS
INDOOR OFFICE/CLASSROM SLIGHT MOBILITY

Bob (x2) Eve (x 4)





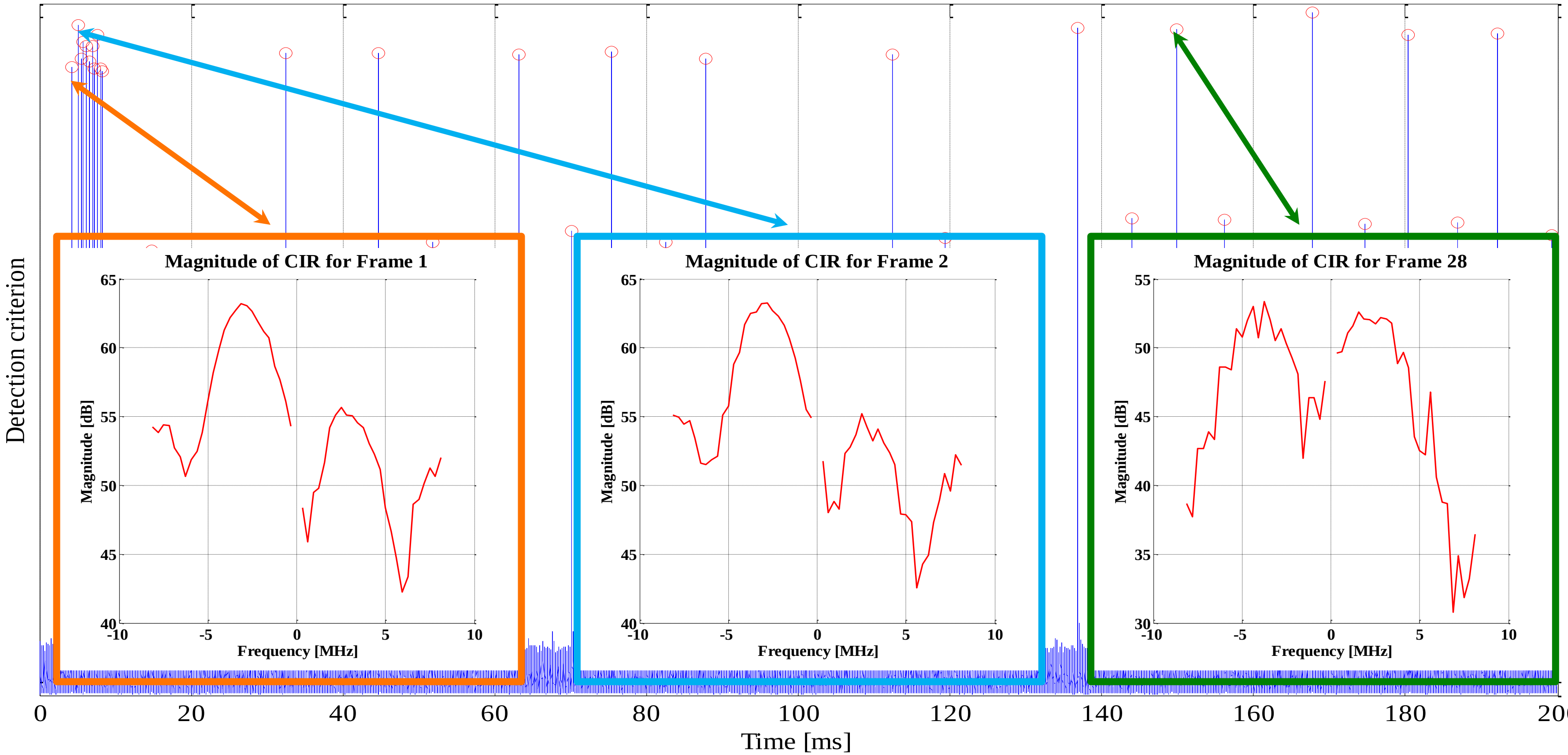
- Very significant space diversity
- Enables computation of “good” secret keys on SIMO/MISO/MIMO Rx
- Ensure security when facing attempts of non-colocated Eve’s for recovering the keys

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Pre-industrial results of Secret Key Generation

Records of Wi-Fi signals – CIR measurements

SINGLE SENSE MESUREMENT AT 1 ANTENNA OVER TIME
INDOOR OFFICE/CLASSROM SLIGHT MOBILITY



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

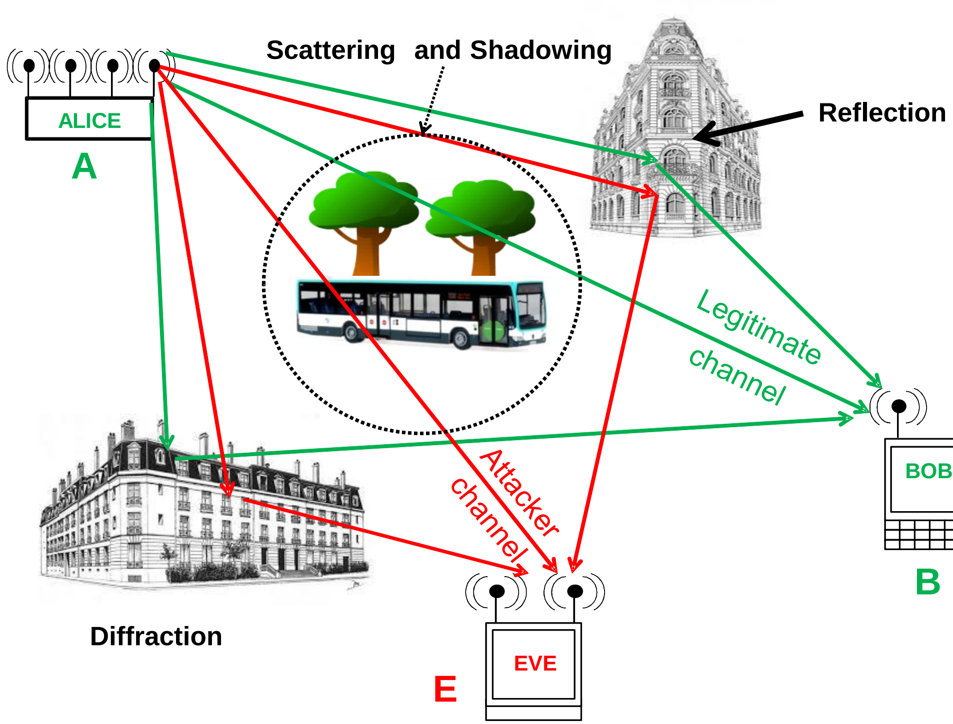
PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Pre-industrial results of Secret Key Generation

Records of Wifi and LTE signals – SKG from CIR measurements

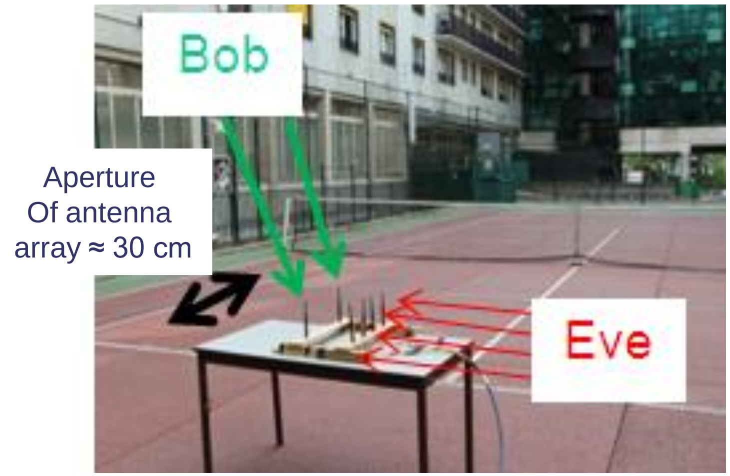
SINGLE SENSE MESUREMENT AT 6 ANTENNAS
COMPARISION OF SLIGHT MOBILE AND FIXED SCENARIOS

a) Propagation of legitimate and attacker radio channel



b) Real field stationary radio configuration in indoor fixed geometry 4G/LTE network empty tennis court and classroom

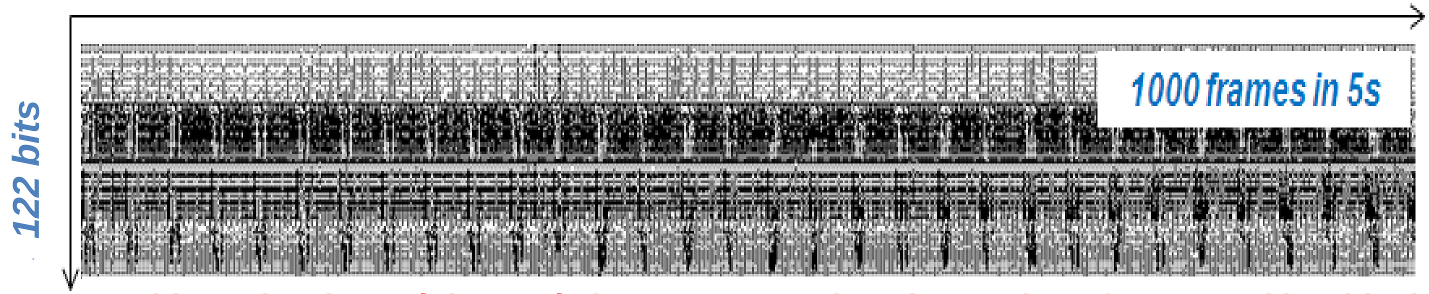
Alice = LTE Node on building roof



PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

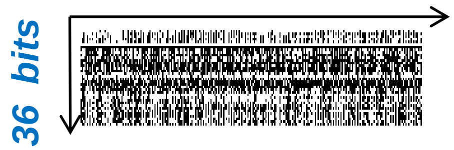
Effect of Channel De-correlation

c) Quantization results in stationary LTE radio environment without channel de-correlation pre-processing



Without the channel decorrelation pre-processing, the number of generated key bits is 1000 x 122 in 5s
=> High time correlation and stationary patterns in the quantized bits that can be exploited by Eve

d) Quantization results in stationary LTE radio environment with channel de-correlation pre-processing



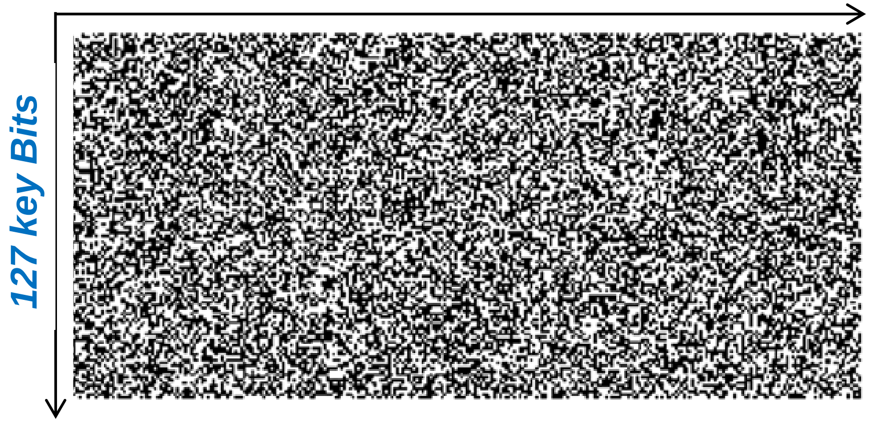
With the channel decorrelation pre-processing, the number of generated key bits decreases to 200x36 in 5s

=> Less stationary pattern in the quantized bits

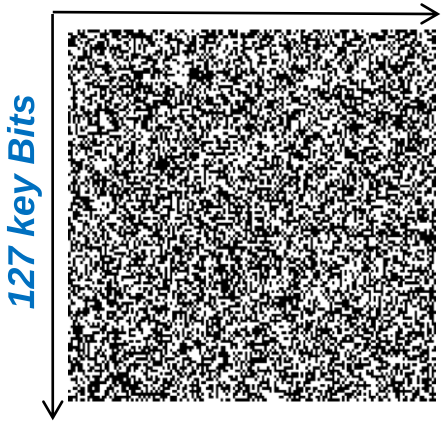
SINGLE SENSE MESUREMENT AT 6 ANTENNAS
COMPARISION OF SLIGHT MOBILE AND FIXED SCENARIOS

e) SKG results in several LTE and WLAN/802/11n radio-environments

LTE outdoor 2.6 GHz
Urban Street NLOS mobile
➔ 284 Keys in 5s



Wifi indoor 2.4 GHz
NLOS Slighly mobile
➔ 152 Keys in 2s



LTE indoor 2.6 GHz
LOS fixed geometry
➔ 49 Keys in 5s

EVEN IN THE MOST DIFFICULT CASE, SKG WORKS WELL.

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

SINGLE SENSE MESUREMENT AT 6 ANTENNAS - INDOOR ENVIRONMENT COMPARISION OF SLIGHT MOBILE AND FIXED SCENARIOS

WIFI indoor NIST Freq. Monobit test	LOS (2.4 GHz)	NLOS (2.4 GHz)
Quantization	87% (132/152)	100% (171/171)
Quant+Reconciliation +Amplification	99% (151/152)	100% (171/171)

LTE - NIST Freq. Monobit test	Indoor (2.6GHz)	Outdoor (2.6GHz)
Quantization only	98% (48/49)	99% (281/284)
Quant+Reconciliation +Amplification	100% (49/49)	100% (284/284)

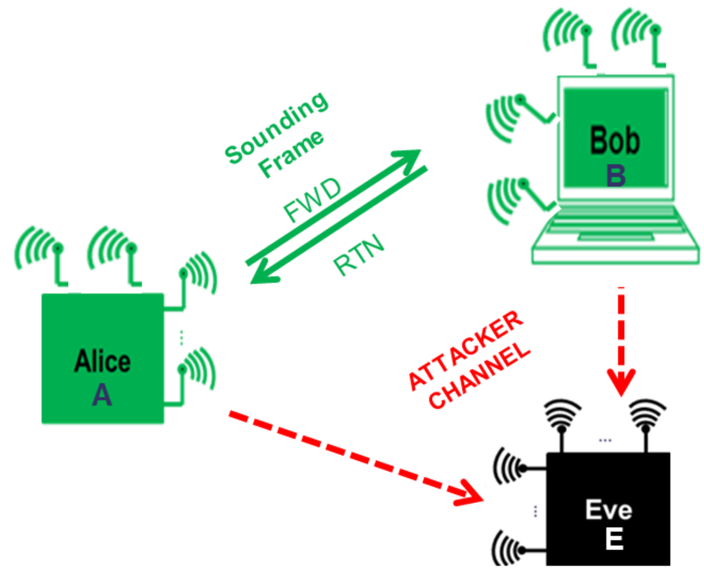
WIFI Indoor NIST Run. test	LOS (2.4 GHz)	NLOS (2.4 GHz)
Quantization only	84% (128/152)	99% (169/171)
Quant.+Reconciliation +Amplification	98% (149/152)	99% (170/171)

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

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

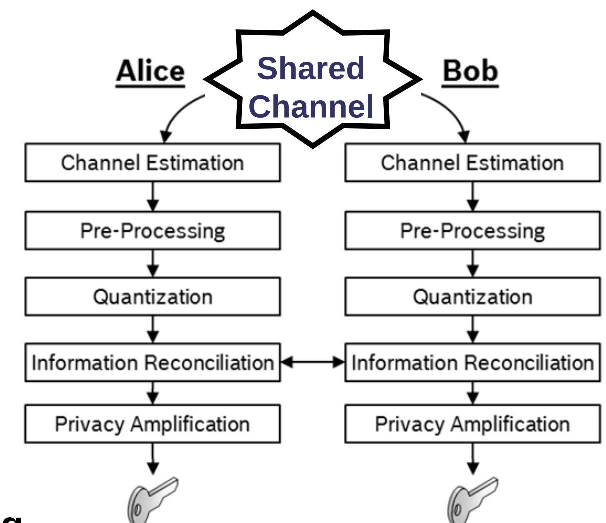
Bi-Directional Channel Sounding

- Alice, Bob and Eve are 4-antenna devices (all using CL2400 4x4 chipset)
- Alice and Bob exchange NDP sounding frames (spaced 20µS in time), both are captured by Eve
- Each node estimates channel independently



Reciprocity Restoration

- Channel reciprocity issues
  - TX to RX analog/RF gain/phase mismatch
  - Mixer phase ambiguity between antennas – 180 degrees
  - AGC gain mismatch between Alice and Bob
  - OFDM symbol timing mismatch (Alice and Bob has tolerance of 0.8µS Cyclic Prefix Guard Interval !)
- Reciprocity restoration - Each channel element (out of 4x4 channel matrix) is normalized and compensated independently



Secret Key Generation

- Reciprocity restoration, de-correlation, Quantization, Reconciliation and Amplification are done in offline processing

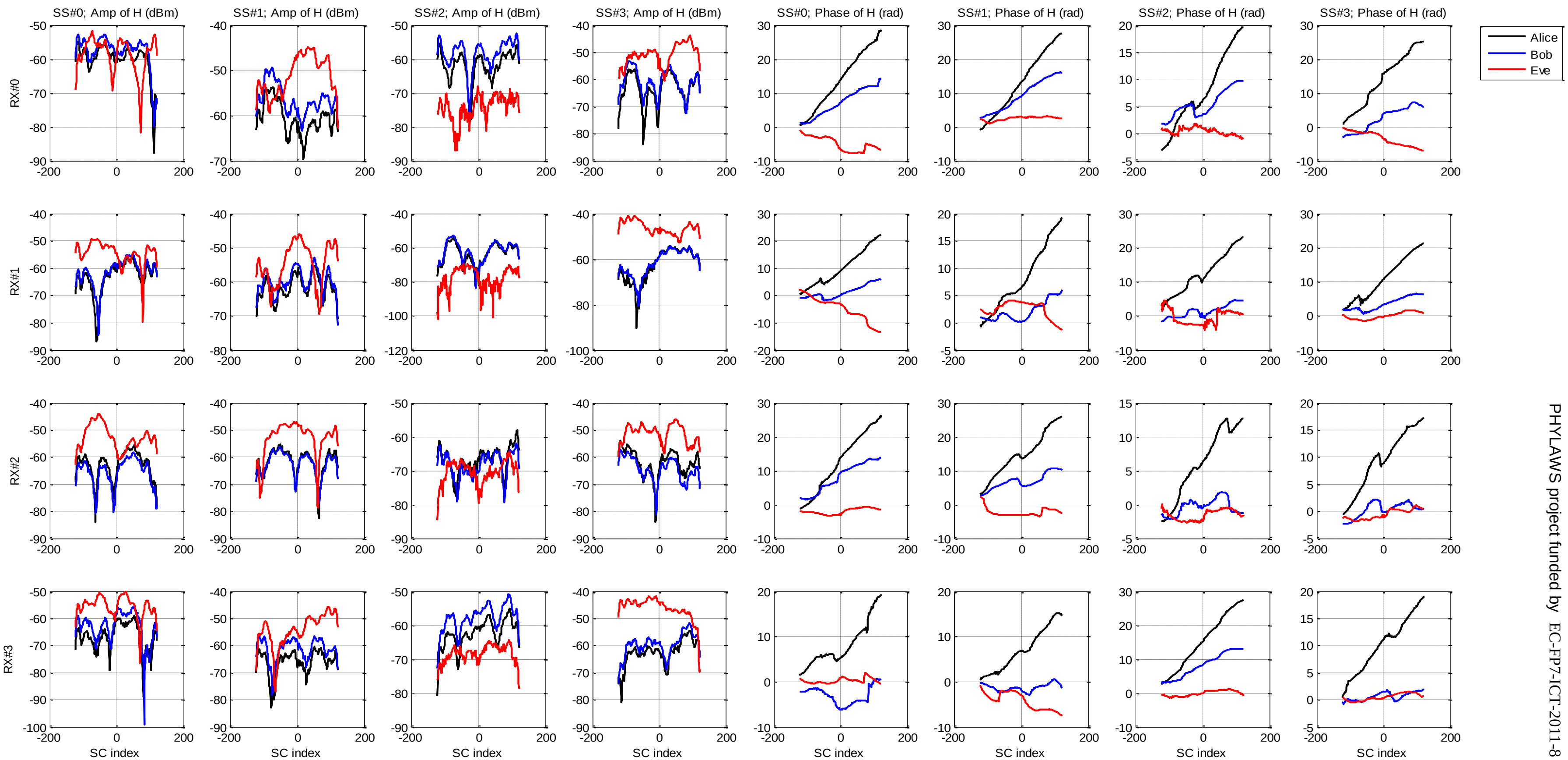
PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Pre-industrial results of Secret Key Generation

Experiments for and Wifi 802.11ac 2.4 and 5 GHz links

DUAL SENSE LEGITIMATE + EAVESDROPPER LINK

Initial CSI extraction



Amplitude **Phase**

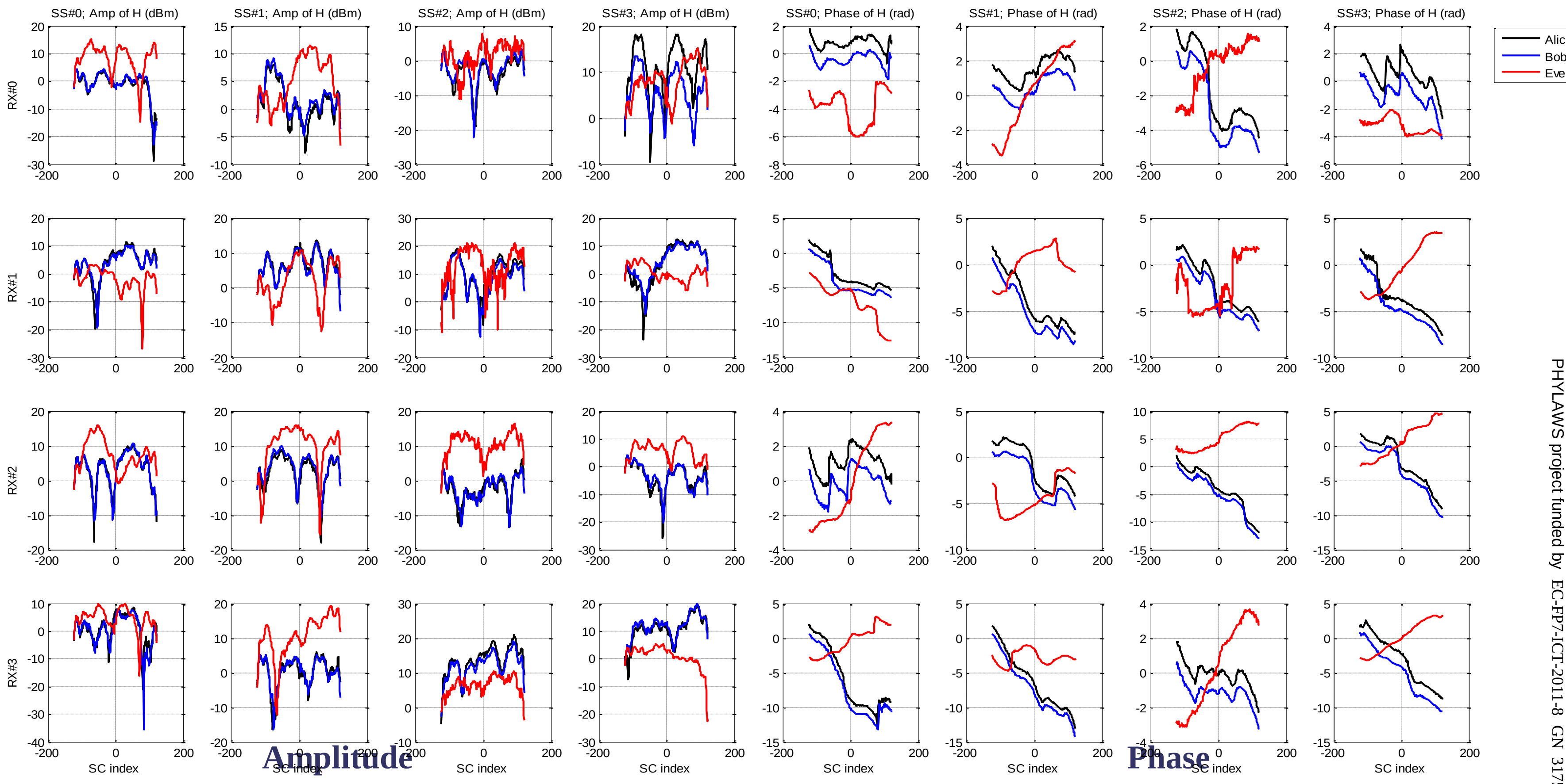
PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Pre-industrial results of Secret Key Generation

Experiments for and Wifi 802.11ac 2.4 and 5 GHz links

DUAL SENSE LEGITIMATE + EAVESDROPPER LINK

Processing stage I+II:
average gain/phase normalization and linear phase estimation and removal



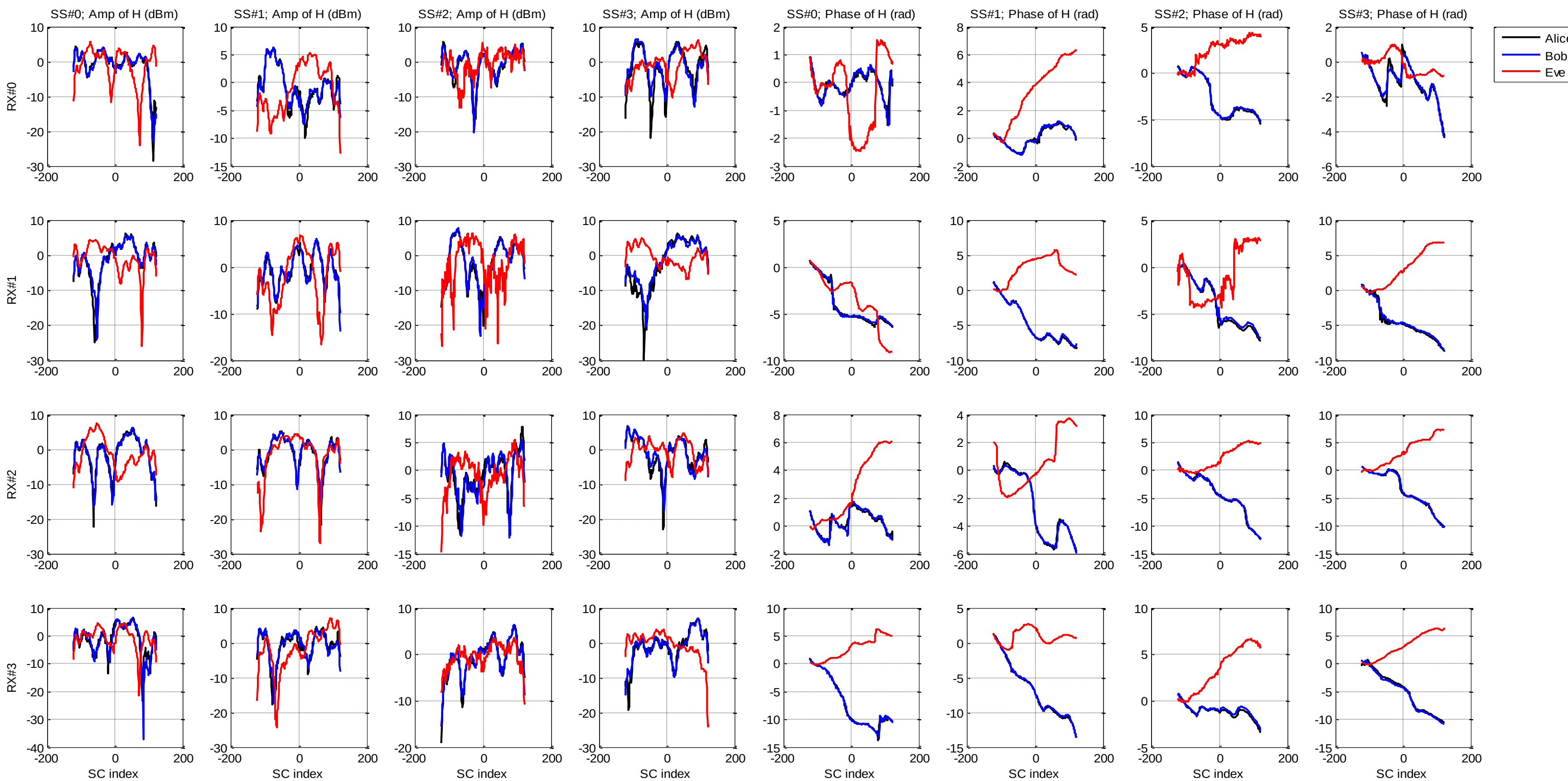
PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Pre-industrial results of Secret Key Generation

Experiments for and Wifi 802.11ac 2.4 and 5 GHz links

DUAL SENSE LEGITIMATE + EAVESDROPPER LINK

Processing stage III: 2nd normalization stage



Amplitude **Phase**

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Pre-industrial results of Secret Key Generation

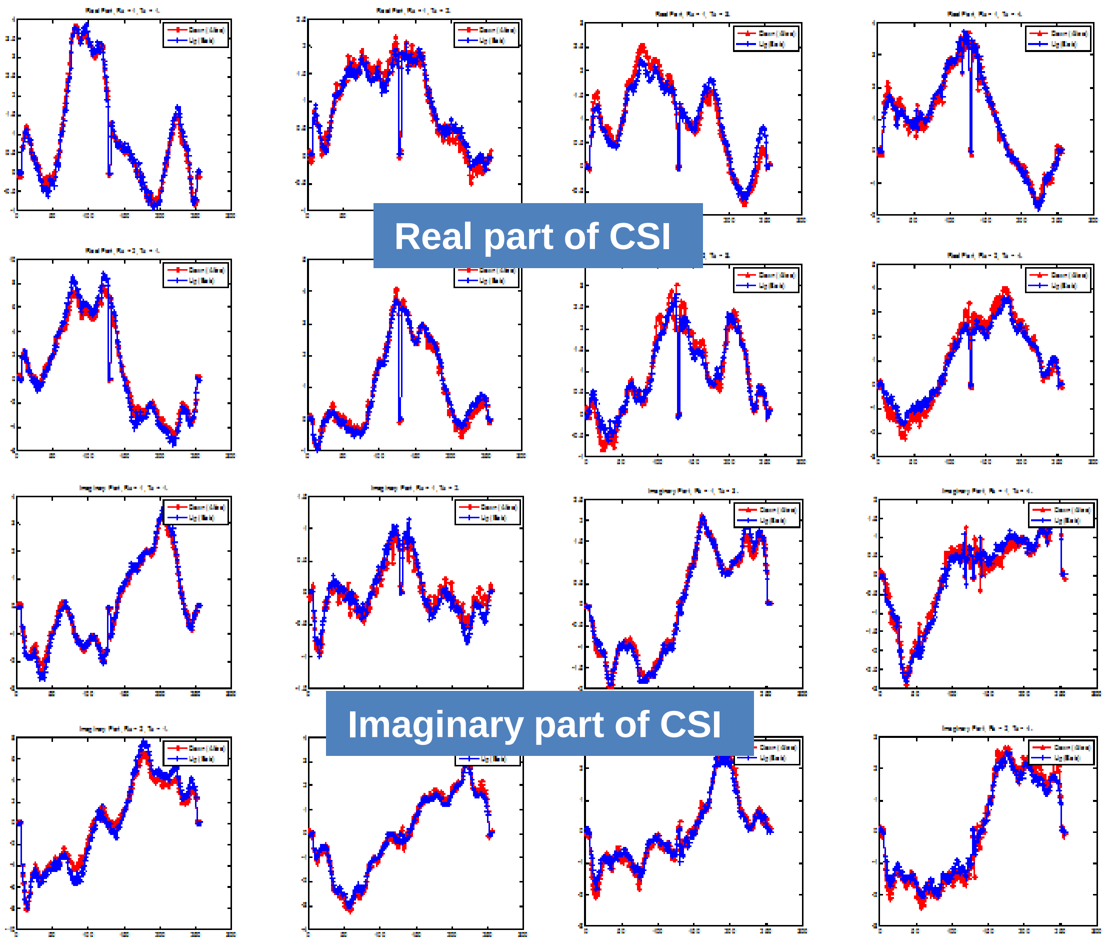
Experiments for and Wifi 802.11ac 2.4 and 5 GHz links

SKG scheme dual sense, without channel de-correlation

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

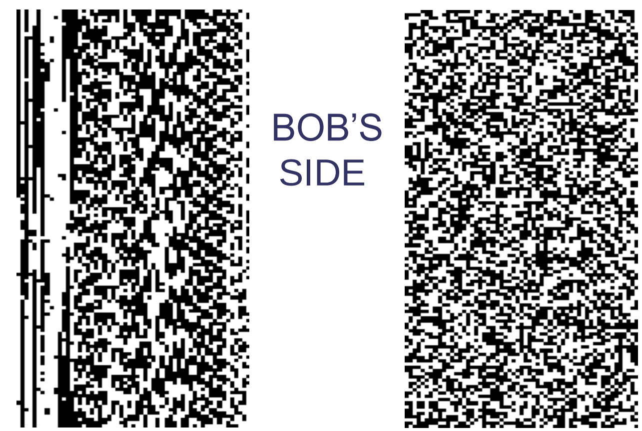
Use of dual sense CSIs: B2 Alice -> Bob and Bob -> Alice

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



Test of key quality

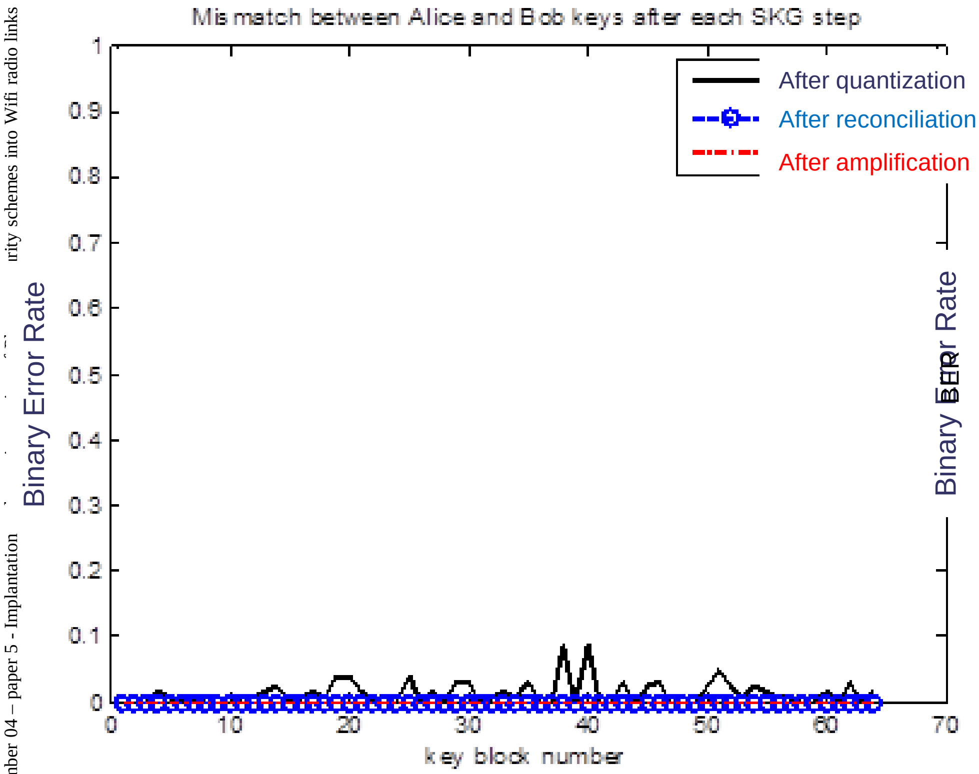
NIST test	Freq. Monobit	Runs
After Quantization	31/57	22/57
After Amplification	57/57	57/57
Concatenation of all keys after quantization	Pass	Fail

PIMRC W8 – 2016 September 04 – paper 5 - Implantation and experimentation of Physec security schemes into Wifi radio links

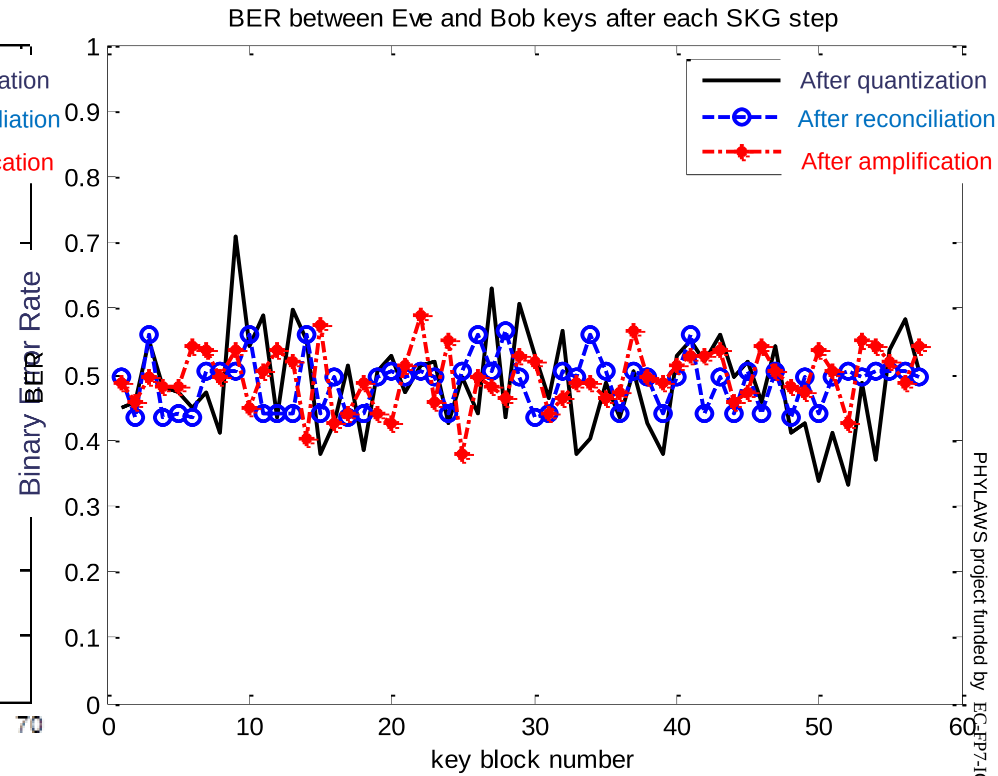
PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

SKG scheme dual sense, without channel de-correlation (following)

Test of Key agreement between Alice and Bob



Test of Information leakage towards Eve



AT BOB'S SIDE: Near 0 BER

⇒ **Reconciliation + key vérification are OK at Alice and Bob**

AT EVE'S SIDE: Near 0.5 BER

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

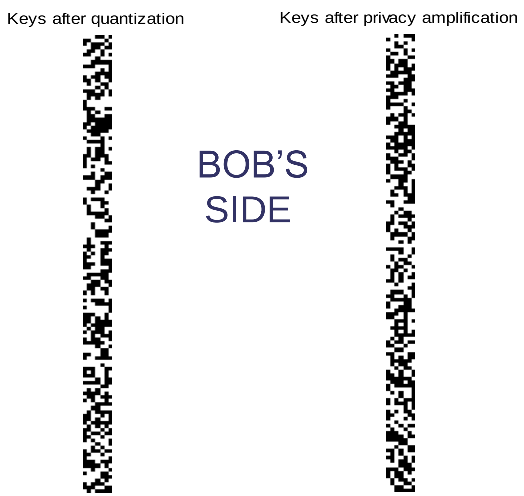
Pre-industrial results of Secret Key Generation

Experiments for and Wifi 802.11ac 2.4 and 5 GHz links

SKG scheme dual sense with channel de-correlation

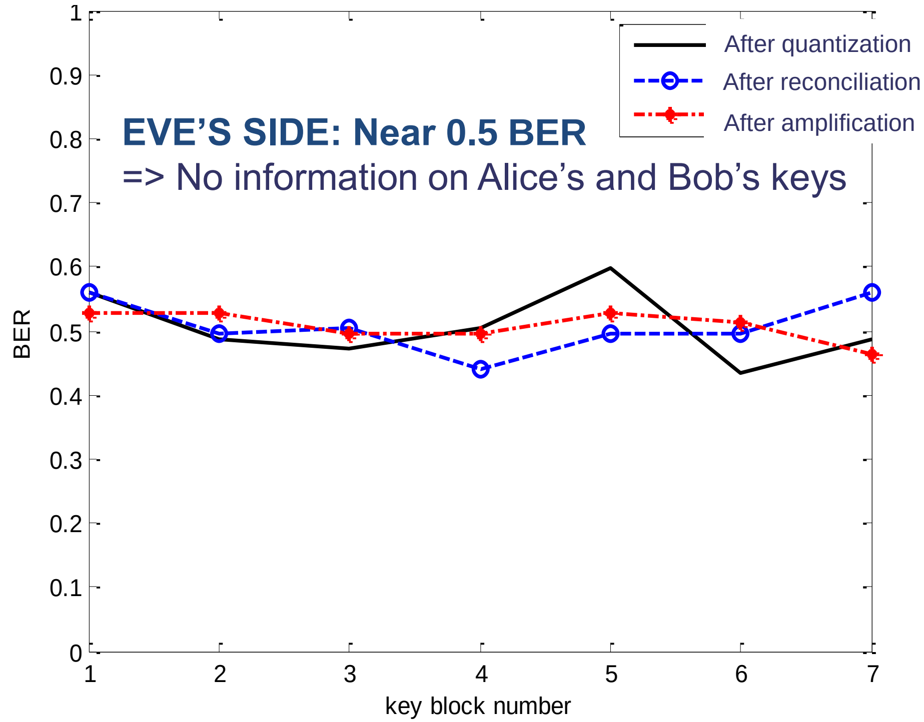
Time and Freq. de-correlation.
Reconciliation FEC=BCH(15,127),
Amplification with 2-Universal Hash

Generation of 128 bits keys from CSI samples computed from one WiFi frame



NIST test	Freq. Monobit	Runs
After Quantization	7/7	7/7
After Amplification	7/7	7/7
Concatenation of all keys after quantization	**Pass**	**Pass**

Test of information leakage towards Eve



Test of Key agreement between Alice and Bob

BOBS'S SIDE: near 0.5 BER

=> Reconciliation + key vérification are still OK at Alice and Bob

PHYLAWS project funded by EC-FP7- -8 GN 317562

WI-FI TESTBED IMPLEMENTATION OF ARTIFICIAL NOISE PLUS BEAMFORMING

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

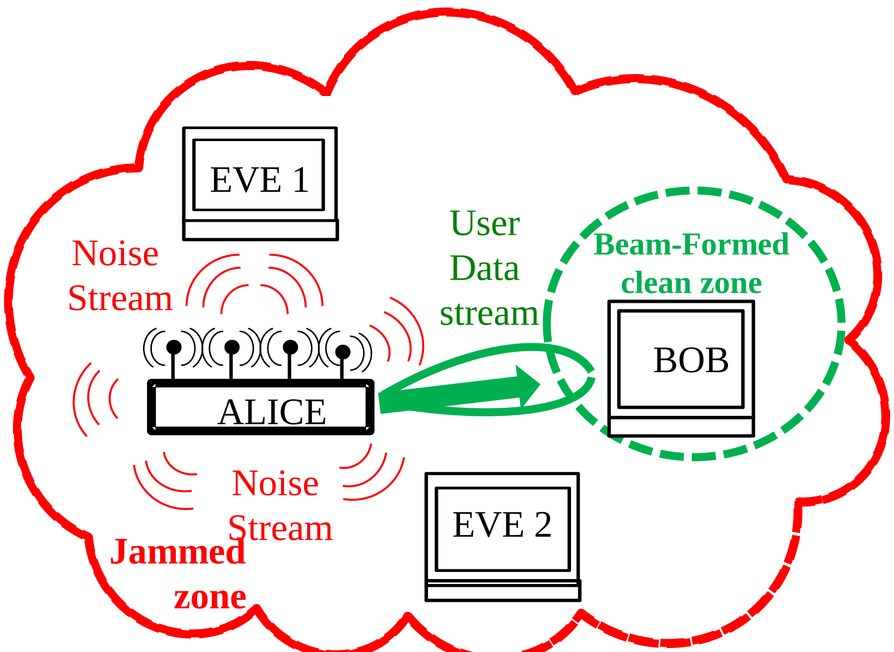
Artificial Noise and – Beam Forming – principle and simulation

General principle in MIMO Tx

1/ Extract the Alice-Bob Channel matrix (CIR) and its orthogonal directions

2/ Transmit noise streams on orthogonal directions. Eve cannot estimate the legitimate CIR, she is thus forced into low Signal to Noise Ratio (SNR).

3/ Beam-form of the Alice-Bob data stream for Bob to maximize link budget.

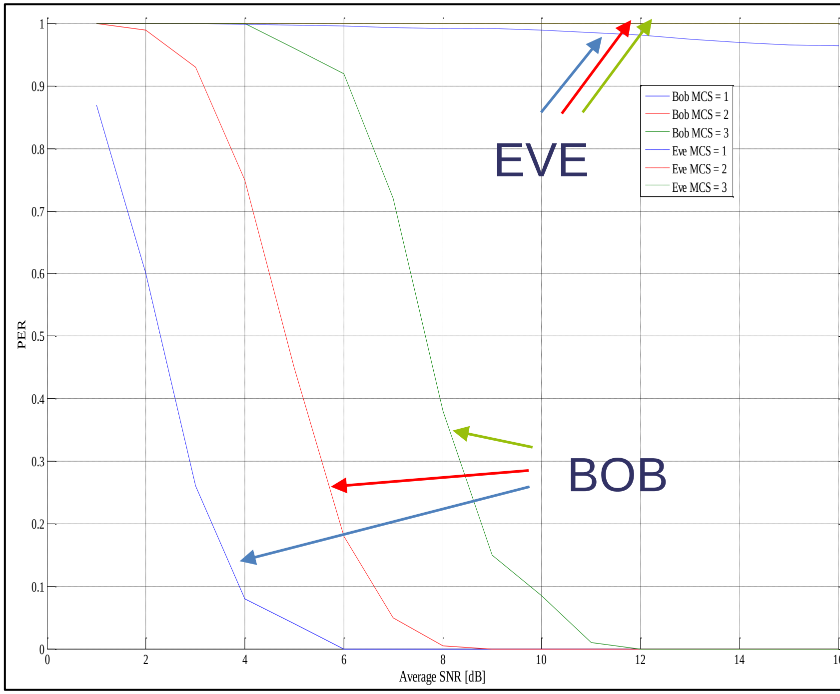


Wifi simulations (Packet error rate)

1/ Alice has four antennas and emits one 802.11n data stream and three noise streams

2/ Bob and Eve have respectively 2 and 4 antennas, with the same receiving capabilities

- Dash line: Packet Error Rate of Eve vs SNR
- Solid line: Packet Error Rate of Bob vs SNR
- Color: Modulation and coding Scheme (MCS)



PIMRC W8 – 2016 September 04 – paper 5 - Implantation and experimentation of Physec security schemes into Wifi radio links

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Pre-industrial results of Secrecy coding

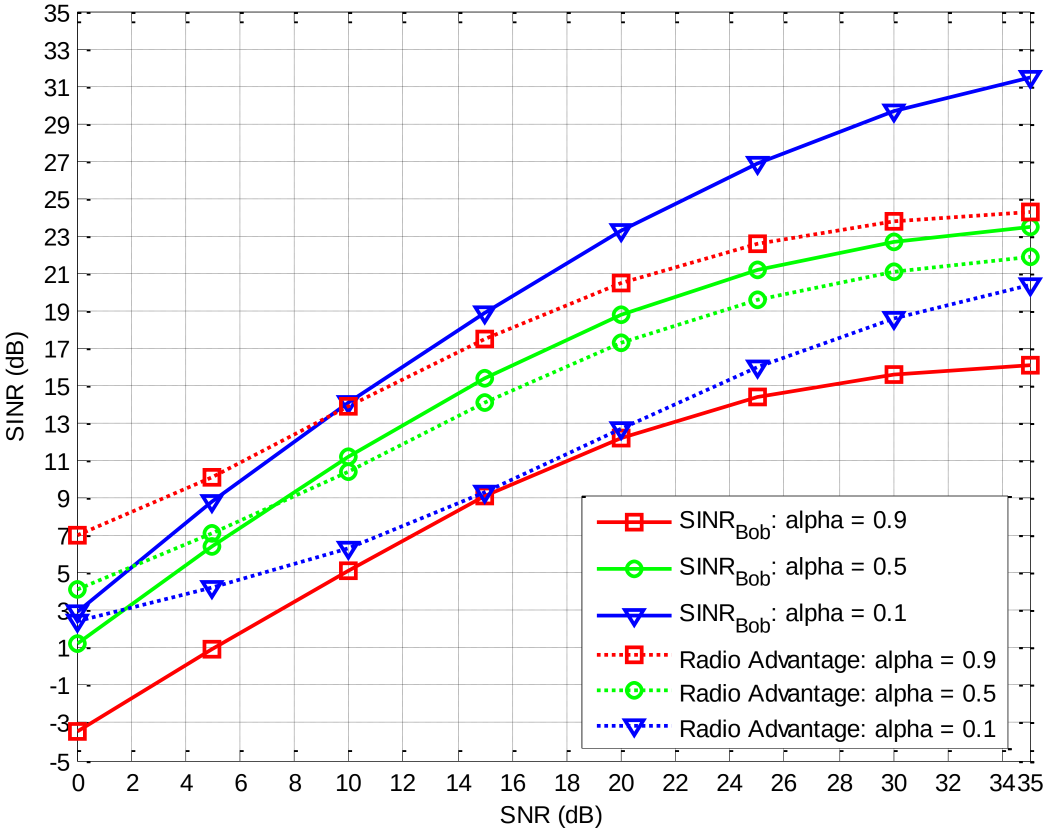
- Simulation Results of AN+BF

Radio Advantage Simulation Results

Wifi simulations (Radio advantage)

- Alice has four TX antennas and emits one 802.11ac data stream and three noise streams
- Bob is a single antenna device
- Radio advantage is normalized to a single antenna Eve
- AN is applied on data portion of frame only
  - AN applied on MAC header (not protected by WPA/WEP) => privacy protection and defense from MAC spoofing
- Simulations are based on fixed point model of the Testbed, and includes all protocol and implementation losses

(**alpha** factor is noise percentage out of total power)



PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

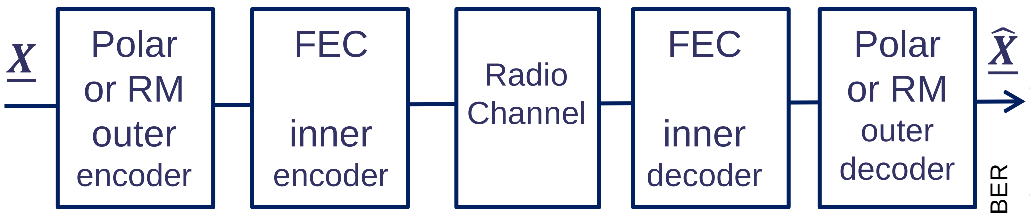
Pre-industrial results of Secrecy coding

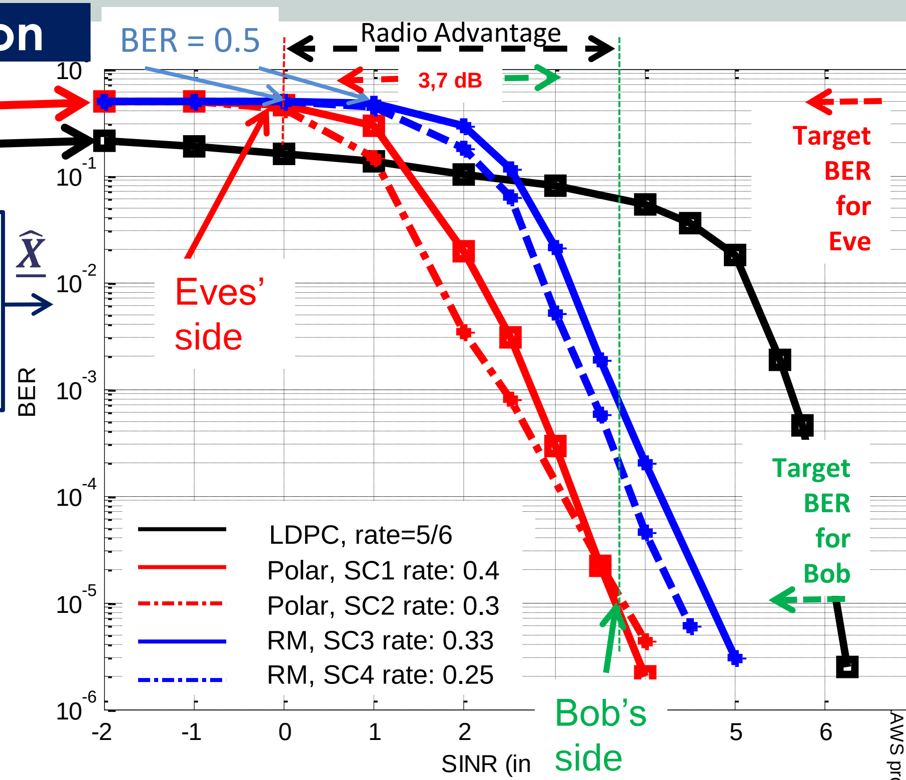
- Analysis of simulation results

From SC principle to practical implantation

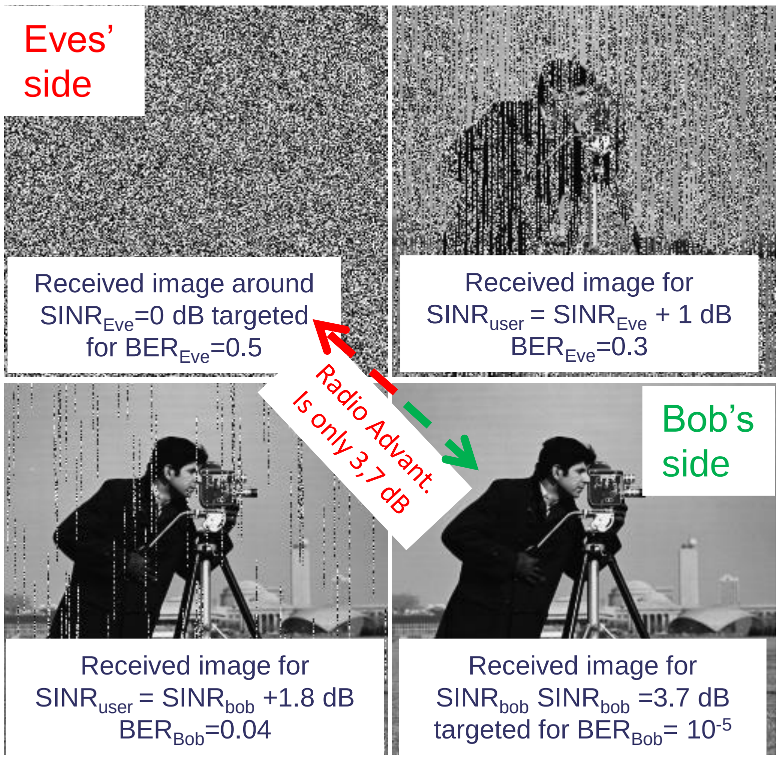
Low $SINR_{Eve}$ ➔ BER = 0.5: no more information leakage

Low $SINR_{Eve}$ ➔ BER = 0.2: information leakage





Example with SC 2



Received image around $SINR_{Eve}$=0 dB targeted for BER_{Eve}=0.5

Received image for $SINR_{user}$ = $SINR_{Eve}$ + 1 dB BER_{Eve}=0.3

Received image for $SINR_{user}$ = $SINR_{bob}$ +1.8 dB BER_{Bob}=0.04

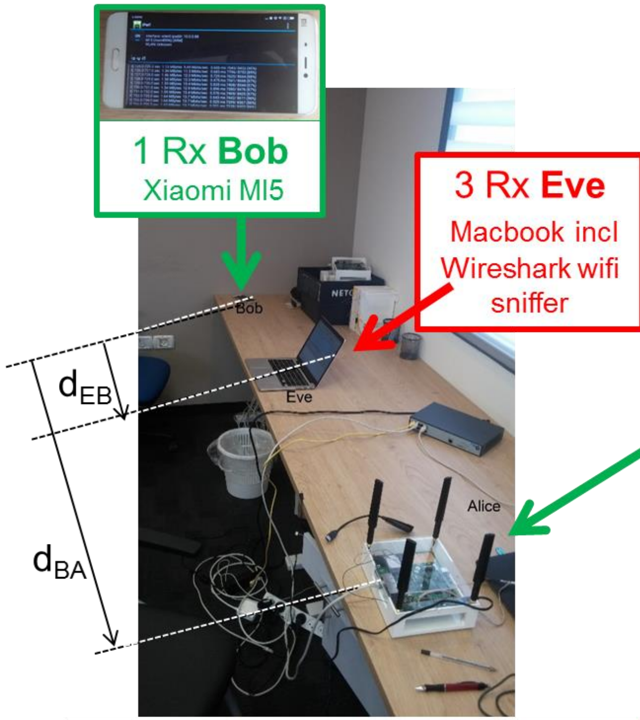
Received image for $SINR_{bob}$ $SINR_{bob}$ =3.7 dB targeted for BER_{Bob}= 10^{-5}

Coding schemes	SC 1	SC 2	SC 3	SC 4
Inner code	LDPC code of length 1296 and rate 5/6 defined in the 802.11 standard			
Outer code	PC	PC	RMC	RMC
Eves's target rate	0.05	0.13	0.05	0.05
Bob's target rate	0.55	0.52	0.5	0.4
R bits, UD bits, P bits	51, 512, 461	133, 399, 492	56, 430, 538	56, 330, 638
Secret Bits Rate	0.4	0.3	0.33	0.25

AWS project funded by EC-FP7-ICT-2011-8 GN 317562

Pre-industrial results of Secrecy coding

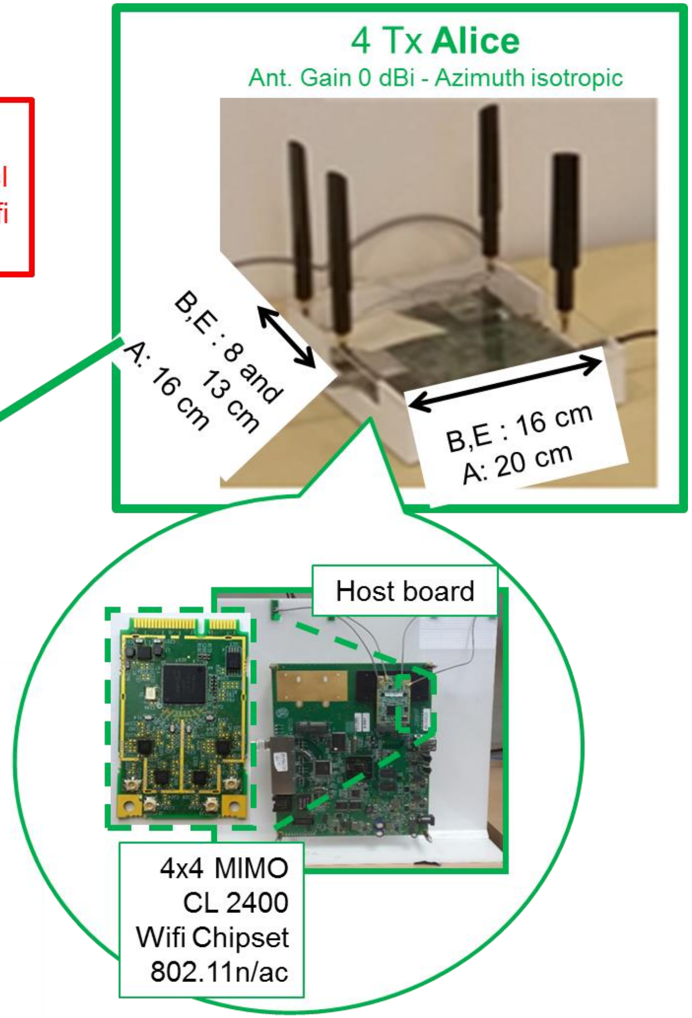
Experiments of Secrecy coding under Wifi links



a/ Geometry of experiments

Indoor Line of Sight configuration
Frequency = 5.2 GHz
Wavelength = 5.8 cm
Distance Alice – Bob: d_{BA} = 2 m
Distance Eve – Bob:
- Near Eve : d_{EB} = -20 cm
- Middle Eve : d_{EB} = 50 cm
- Far Eve : d_{EB} = 5 m

b/ Components for AN-BF and SC implantations



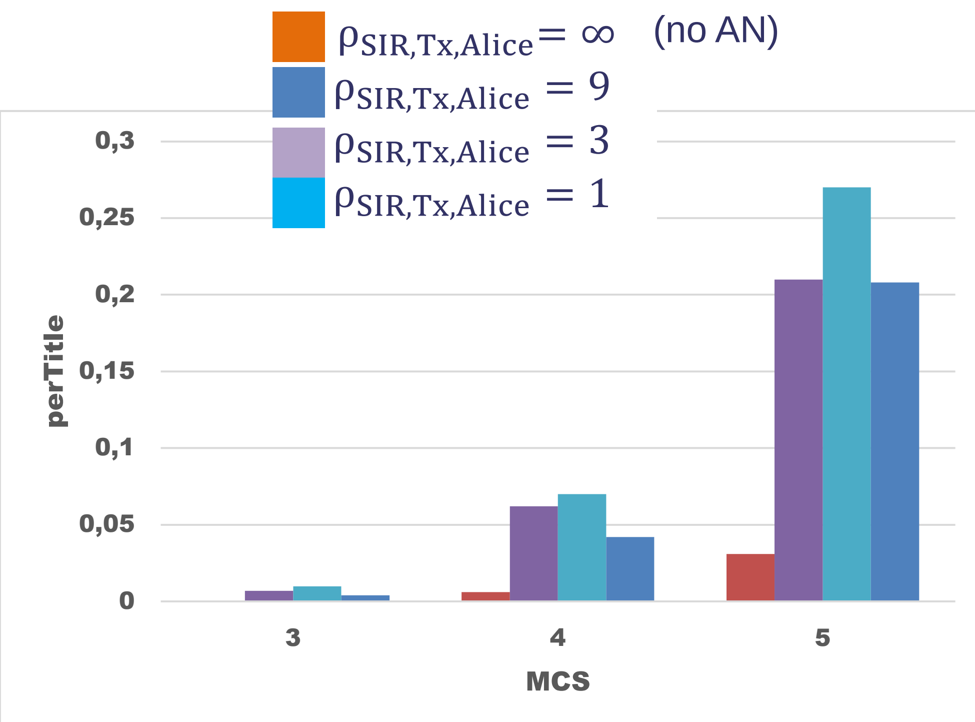
Sounding frequency = 100ms
Thales Communications

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Pre-industrial results of Secrecy coding

- Experiments of Secrecy coding under Wifi links

Values of power ratio and Bob's PER (Packet Error Rate) at different MCSs



Tx/Rx radio parameters

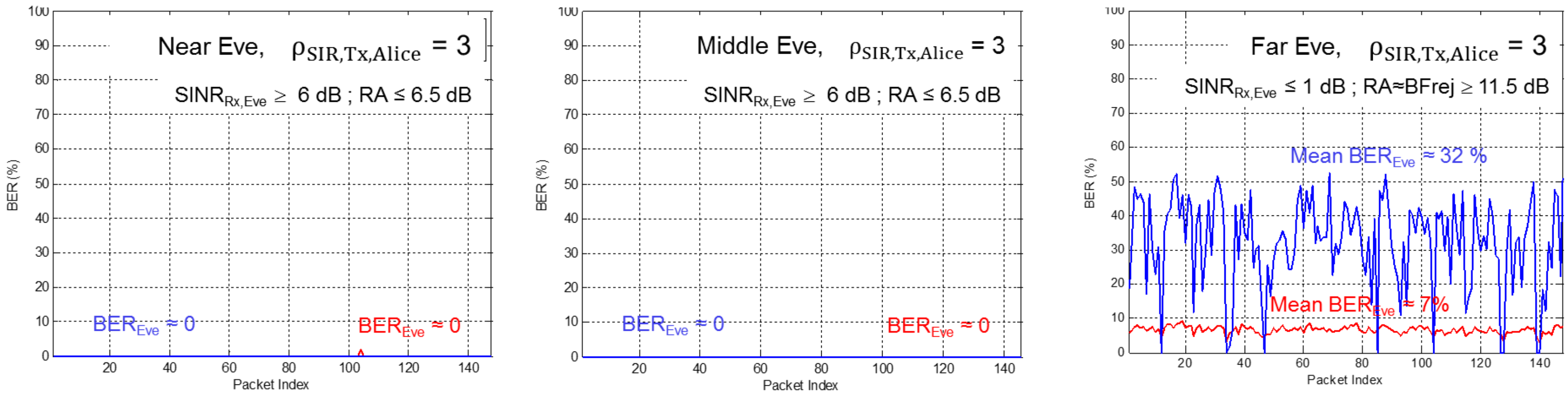
1 user and 3 noise spatial streams among 4
AN is uniformly distributed over the antennas

Table of Rx Modulation and coding scheme

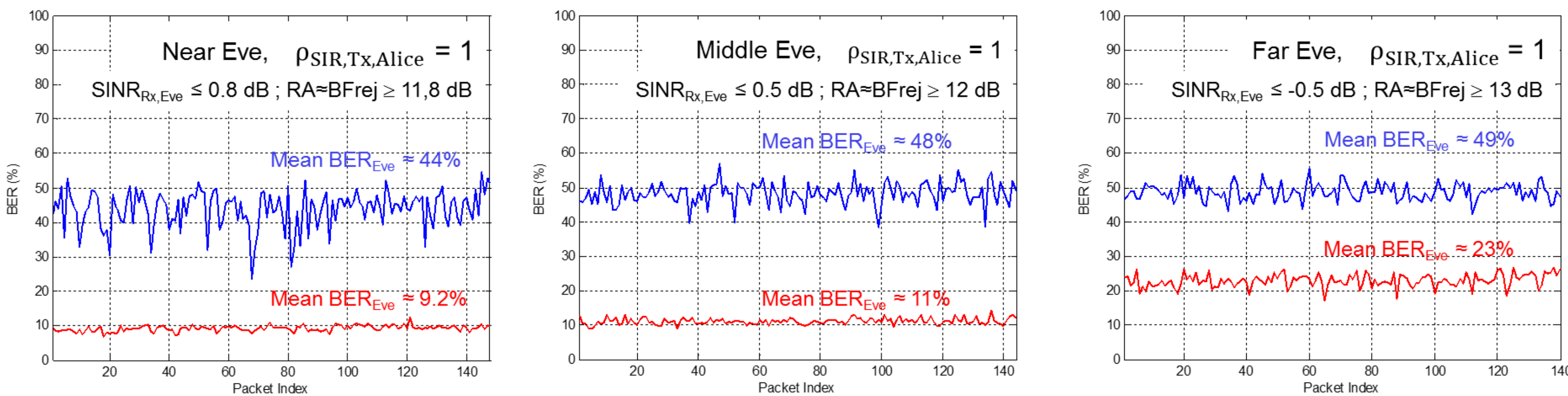
MCS	BW MHz	Rate Mbps	CarrierNb	Modulation coding	SNR Thresh dB
2	20	19.5	52 + 4	QPSK ¾	5,5
3	20	26	52 + 4	16QAM ½	8,5
4	20	39	52 + 4	16QAM ¾	12,5
5	20	52	52 + 4	64QAM 2/3	16,5
> 5	20	≥ 58	52 + 4	≥64QAM ≥¾	≥17.5

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

a/ When AN power is low (25% of the total power, $\rho_{SIR,Tx,Alice} = 3$) => poor secrecy



b/ When AN power is medium (50% of the total power, $\rho_{SIR,Tx,Alice} = 1$) => high secrecy is achieved



Bob's decoder is MCS4 with $PER_{Bob} \approx 0$; $SINR_{Rx,Bob} \geq 12.5$ dB
Eve's decoder is MCS2 with variable PER_{Eve}
SC is Polar, (R,I,F) = (102, 409, 513)

BER_{Eve} when AN-BF only occur (red line)
BER_{Eve} when AN-BF + SC occur (blue line)

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

1/ Secret Key Generation from CSI is feasible

Can be implemented on top of industrial WiFi chipsets at application level – no need for silicon changes (provided full access available to CSI)

More work needed to fully commercialize all required calibrations

2/ Artificial Noise and Beam-Forming is mature

Now made feasible with increasing support for Beamforming in 802.11ac standard

Radio advantage is adequate as basis for link security

More work needed to optimize signal and noise power allocation

2b/ Secrecy Coding feasibility proof is achieved !!

First SC schemes for realistic radio communications are proposed and tested

Zero information leakage between Alice and Eve demonstrated

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Thank you for your attention

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

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Annex

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Tag Signals (TS) – building and processing

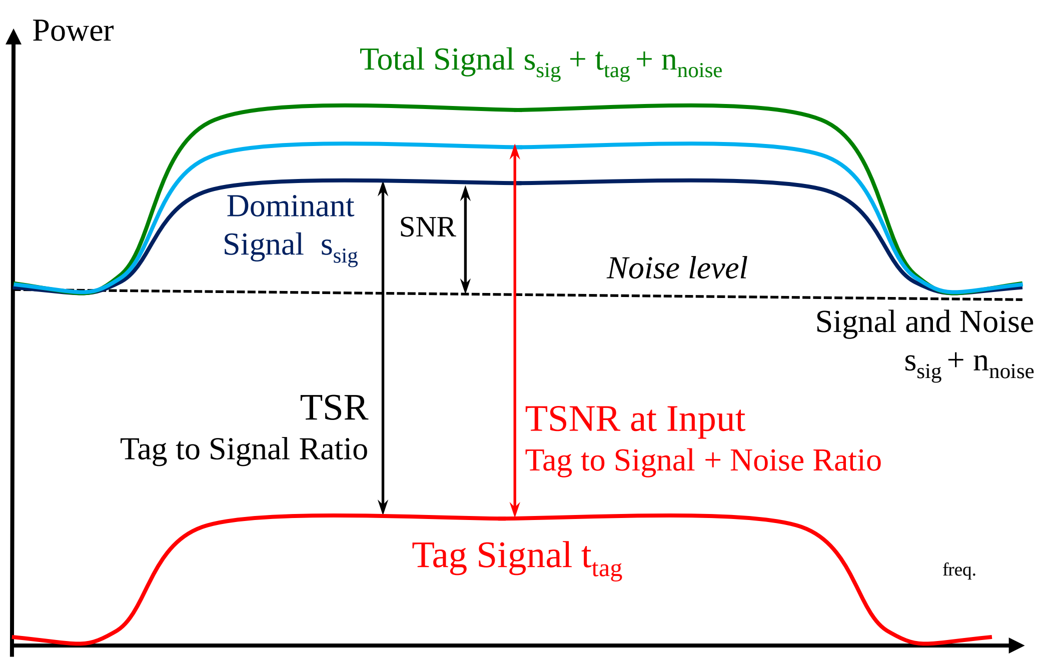
Built with wide band low DSP Direct Spread Sequences signals (DSSS)

FWD and RTN Under beacon frequencies/msgs S_{sig} => Self interfered

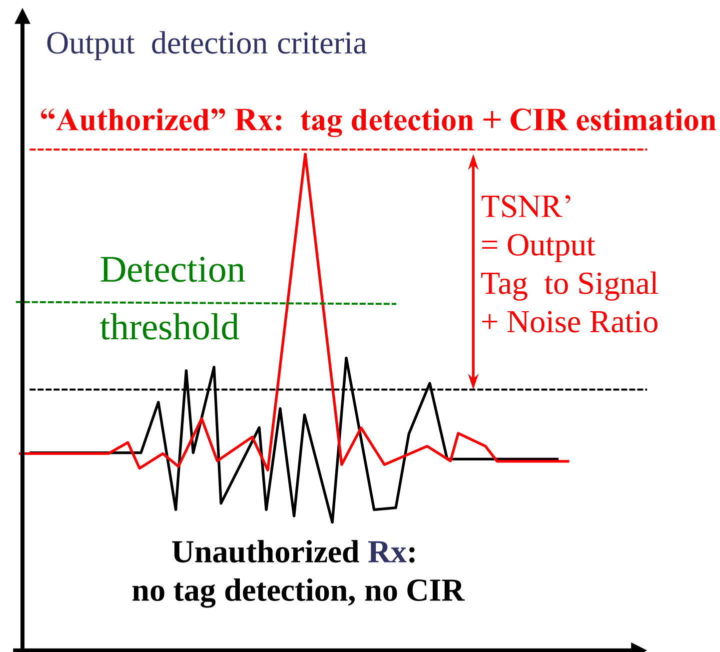
=> negative « tag to Signal + noise » ratio

Optimal time resolution for accurate CIR estimation

DSSS codes change fast and the chose is made adaptively dependent on channel measurement



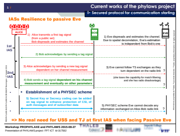
A- Building – Relevant Radio parameters



B- Processing = Matched filtering
CIR est. No RAKE

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Interrogation and Acknowledgement Sequences (IAS) – principle & resilience analysis



I- SECURE PAIRING TROUGH CIR ESTIMATION WITH TAG SIGNALS

1st IAS

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

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

ALICE

BOB

2nd IAS

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

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

II- ESTABLISHMENT OF PHYSEC SCHEME

ALICE

Forward and return Secret Keys and Secrecy Codes / Artificial Noise

BOB

PIMRC W8 – 2016 September 04 – paper 5 - Implantation and experimentation of Physec security schemes into Wifi radio links

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

(Mobile) obstacles between users:

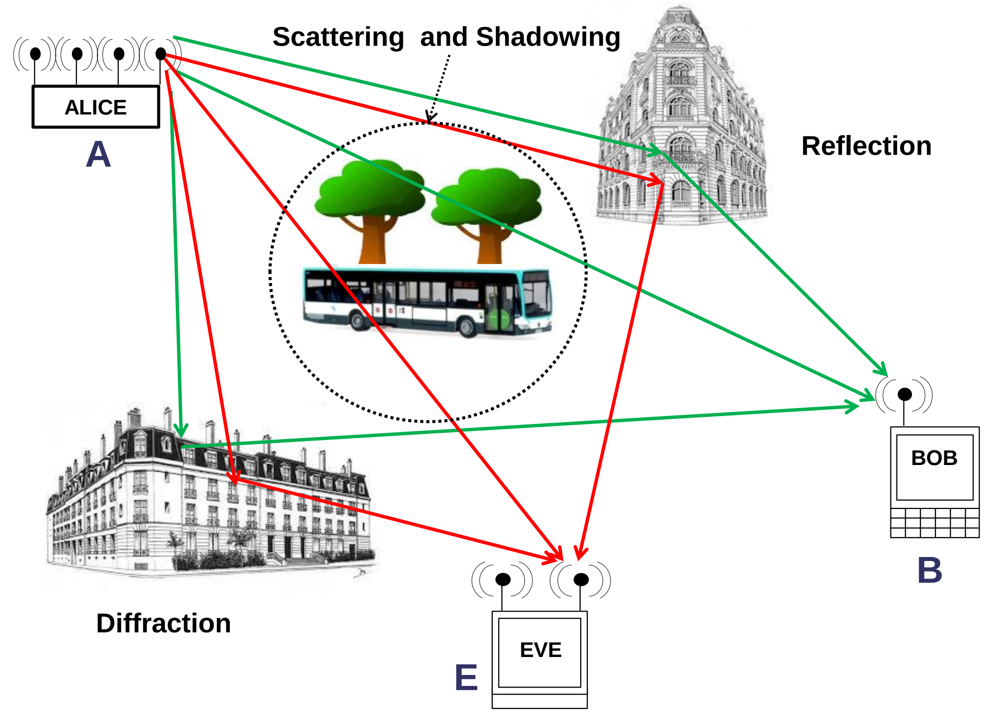
- Multiple paths to reach Bob or Eve
  Reflection, Diffraction, Scattering, Shadowing
- Waveforms received by Bob and Eve have been altered differently
- Apply either to outdoor and indoor

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



Additional "radio" random for disturbing Eve:

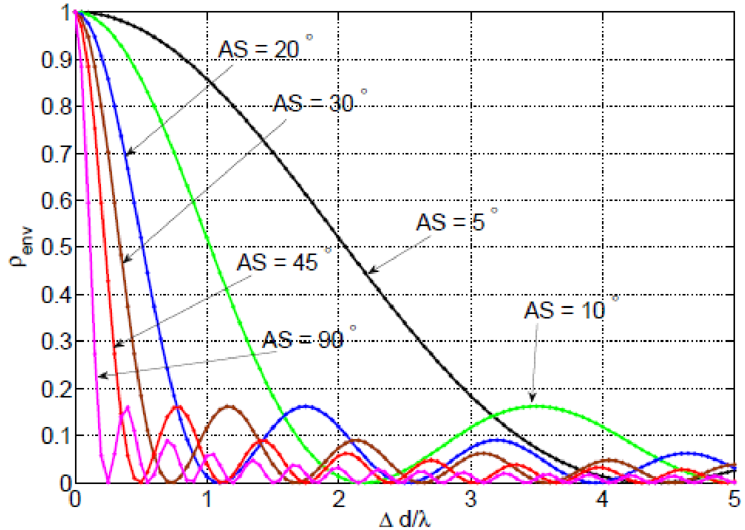
- **Alice and Bob Antennas: patterns and orientations**
- **Artificial noise and Beamforming : SNR advantage to A and B.**

ct funded by EC-FP7-ICT-2011-8 GN 317562

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)

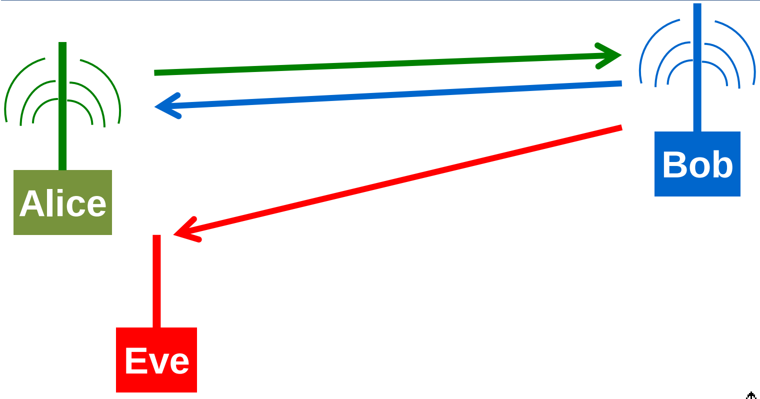
Provisory Conclusion

- **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 !

RSSI example
Source = project Prophylaxe

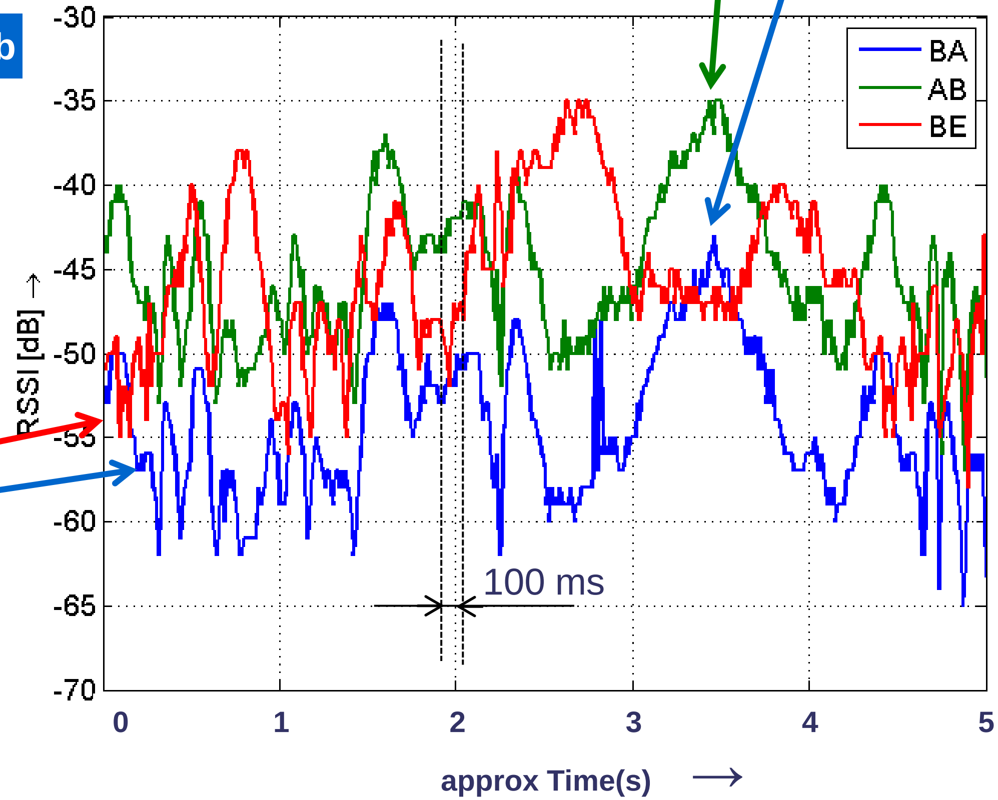


Same RSSI figure (after normalisation)
In forward sens Alice -> Bob
In sense Bob -> Alice

⇒ **Channel Reciprocity**

Different RSSI figure
In sense Bob -> Eve
In sense Bob -> Alice

⇒ **Channel spatial decorrelation**



Example of RSSI measurement over time - Source = project Prophylaxe
Signal is IEEE 802.11n, 2.4 GHz, BW=20 MHz E is located ~ 15cm next to Alice.
Slight mobility of Scatterers.

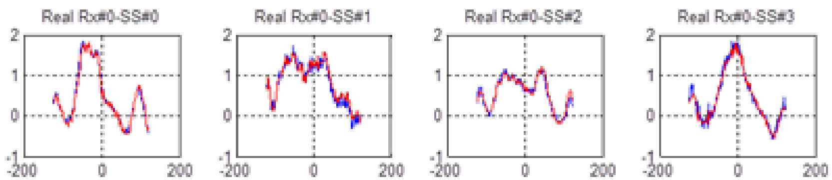
<u>In addition:</u>
Indoor time coherence is 50 to 100 ms

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

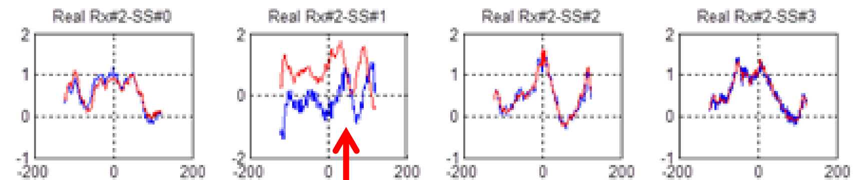
A/ CIR measurements - Need for Tx/Rx calibration

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

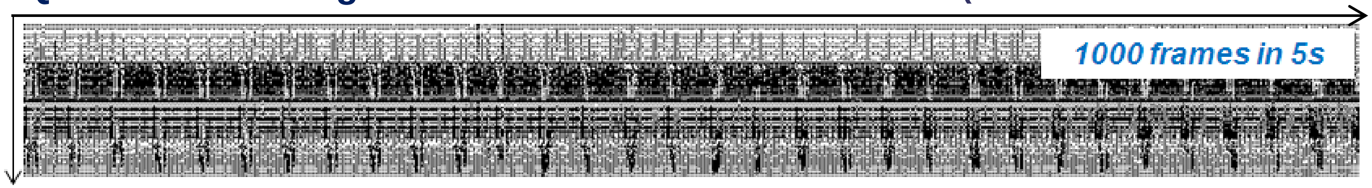


Mismatch to calibrate

B/ Need for Channel de-correlation → channel pre-processing techniques

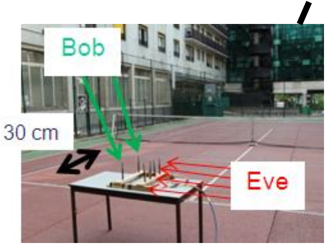
Quantization using all available Channel coefficients (case LTE 2.6 GHz - PSS BW 1.4 MHz - indoor LOS)

122 bits



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

LTE Node Alice



Resulting Quantization after removing highly correlated frames

36 bits

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

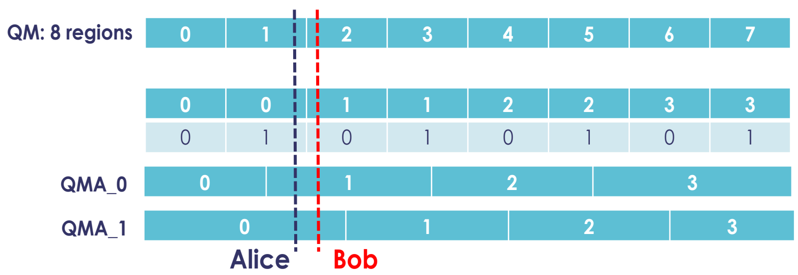
PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

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)

RSSI quantization schemes
Robust but low richness random extraction

Case of CSI CQA algorithm: (Wallace2010)
+ High richness random extraction
+ Bit disagreement reduction
(CSI based, 2 alternate quant. maps + geom. criterion)
Alice and Bob compute Quantization maps
Then Alice choses symbol 0 & informs Bob about her map (QMA_1)
Thus Bob choses symbol 0 on ma QMA_1



. Reduces mismatch risks between Alice and Bob (esp. low SNR)
. No information leakage (map index is transmitted, symbol not)

D- Reconciliation

- Objective: correct key bit mismatches between Alice and Bob
- Based on sketch exchanges between Alice an Bob and Error Correction (basic FEC)
- Well known and similar to error basic decoding applied to keys

E- privacy amplification + key test

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

A- Preliminary Radio advantage

- Objective: provide at better capacity at Bob's side than at Eve's side
  - Simple cause of single path channel + Gaussian additive noise:

at Bob's Rx — at Eve's Rx

Radio advantage: $(SNR)_{B,dB} - (SNR)_{E,dB}$

Secrecy capacity: C_{SEC}=

$$C_{SEC} = \log_2[[1+10^{((SNR)B,dB)/10}]/[1+10^{((SNR)E,dB)/10}]$$

at Bob's Rx — at Eve's Rx

- One practical mean for achieving the radio advantage is Artificial Noise and Beam Forming
  - See the previous slide
  - Eve is forced into low SNR radio because of interference from Alice
  - Thanks for the Beam-Forming Bob keeps a high SNR radio

B- Objective of the secrecy codes

- correct bit errors between Alice and Bob
- warranty null information leakage towards Eve
- Condition: rate less than C_{SEC}.

C- Practical secrecy coding scheme developed in Phylaws WP4

- Concatenation of two codes
  - A usual Inner FEC Code: able to provide sufficient error correction capability when facing any kind of realistic radio channel
  - An added Outer code (polar or Reed Muller) able to provide secrecy
- The result is a sub-optimal scheme which is close to the optimum

IEEE pimrc'16 27TH ANNUAL IEEE INTERNATIONAL SYMPOSIUM ON PERSONAL, INDOOR AND MOBILE RADIO COMMUNICATIONS 4-7 SEPTEMBER, VALENCIA, SPAIN

IEEE COMMUNICATIONS SOCIETY

THALES Celeno TELECOM ParisTech PHYLAWS Imperial College London VTT