



EUROPEAN
COMMISSION

Community Research



PHYSical Layer Wireless Security



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

**WinnComm Europe 2015
Erlangen – 10/07/2015**

Renaud Molière
renaud.molier@thalesgroup.com

- **INTRODUCTION**
- **INTEREST OF PHYSEC**
- **SECRET KEY GENERATION**
- **ARTIFICIAL NOISE**
- **SECRECY CODING**
- **CONCLUSION**

■ LACKS OF SECURITY IN EXISTING WIDESPREAD WIRELESS NETWORKS

• Mobile Telephony

Using failures of the SS7 and international roaming protocols to get Ki keys

- Monitoring of VIP's smartphone during years
- Security of subscribers can be decreased by networks protocol weaknesses

SIM card providers may be hacked

- Hacking of SIM manufacturers by security agencies to obtain Ki Keys
- Subscribers' keys may not be secret in practice

• WiFi

Where's security in WiFi ? An Argument for Industry Awareness

- Use of WEP keys
- WPS enables to crack WPA-2

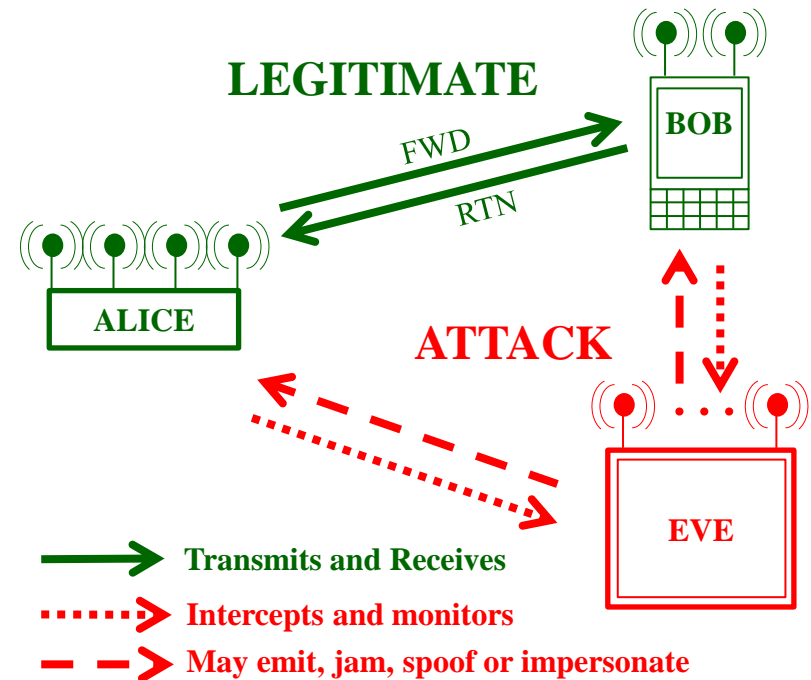
• Internet of Things

FBI: "Internet of Things poses opportunities for cyber crime"

- Weak security control
- Vulnerability of the air interface

■ COMMUNICATION SCENARIO

- **LEGITIMATE** links are Alice to/from Bob
- **EAVESDROPPER** links are
 - Alice to Eve...and even (active) Eve to Alice
 - Bob to Eve... and even (active) Eve to Bob
- Most usual academic hypothesis are:
 - complete information of Eve about legitimate RATs/waveforms
 - no Information of Eve about legitimate Keys (e.g. Ki Keys on SIM cards)
 - No more valid nowadays in public RATs



■ CLASSIC SECURITY COUNTERMEASURES

- **TRANSEC** (Transmission Security) is the protection of the transmitted signals face to interception and intrusion attempts (and even jamming and direction finding)
- **NETSEC** (Network Transmission Security) is the protection of signalling and access messages. Usual solutions are authentication and integrity control (or ciphering of signalling in military networks)
- **COMSEC** (Communication Security) is the protection of data messages (voice, sms, mms, high speed data). Most of solutions are based on ciphering and integrity control schemes

■ NEW ADD-ON SECURITY SCHEMES SHALL

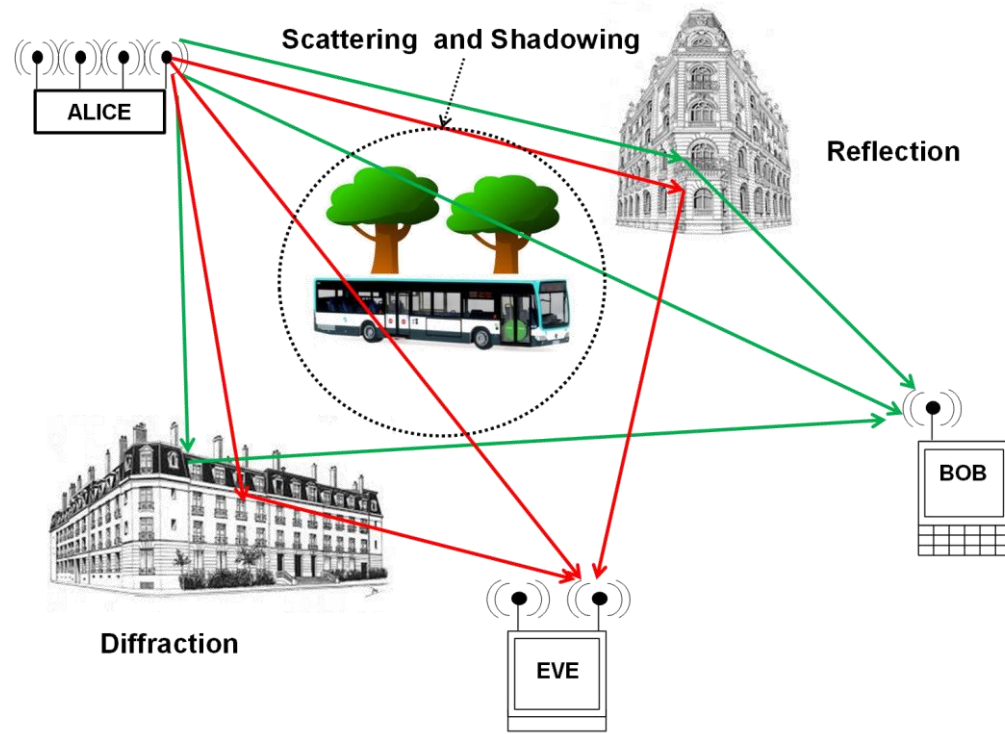
- Not rely on pre-distribution of keys
- Be compatible with a large numbers of subscribers
- Be easy to implement and standard compliant
- Be efficient against any kind of attack

■ EMERGENCE OF A NEW SECURITY TECHNIQUE: “PHYSICAL LAYER SECURITY”

- PHYSEC
- **Key-less security technique exploiting propagation randomness to establish secrecy between legitimate users**
- Theories are well developed and results are promising
- Practical implementations are thriving
- Various techniques for different kinds of protection
- Adaptive techniques

■ EXPLOITING THE RANDOM PROPAGATION OF WIRELESS RADIO CHANNEL

- **Obstacles between users**
 - Multiple paths to reach Bob or Eve
 - Reflection, Diffraction, Scattering, Shadowing
 - Waveforms received by Bob and Eve are differently altered
 - Apply both to outdoor and indoor
- **Complex propagation and unpredictable scattering objects**
 - Channel randomness
 - Received waveforms cannot be recovered by computation
- **At fixed carrier, same angles on obstacles for Alice \rightarrow Bob and Bob \rightarrow Alice**
 - Channel reciprocity (in TDD)
 - Same randomness for Alice and Bob
- **Additional “radio” randomness**
 - Alice and Bob Antennas: patterns and orientations



PHYSEC: Key-less security technique exploiting propagation randomness to establish secrecy

■ 2 MAIN APPROACHES FOR PHYSEC

- **Secret Key Generation (SKG):** Secret Keys are computed from channel measurements
 - Channels between legitimate nodes are reciprocal and uncorrelated elsewhere
 - Propagation randomness ensures the uniqueness of the computed key

Channel quantization algorithms target low mismatches between legitimate links

Existing SKG strategies ensure few information leakage to third parties

- *Y. El Hajj et al., "Towards robust key extraction from multipath wireless channels", IEEE Journal of Comm. and Net., vol.14, no.4, 2012*
- www-phylaws.ict.org, deliverable D4.1

- **Secrecy codes: channel codes (FEC) are augmented with secrecy capabilities**
 - Require better radio link (SNR) between Alice and Bob than between Alice and Eve
 - Approach Shannon capacity for legitimate link
 - Mitigate information leakage at "any" other location

Theoretical feasibility is established but explicit design remains an active research domain

Expected results from Phylaws project in 2016

- *Bloch and Barros, "Physical Layer security", Cambridge University Press, 2011*

■ AUTHENTICATION OF THE RADIO LINK

- Tag Signals and Interrogation and Acknowledgement Sequences
- See previous presentation at WinnComm 2015 (San Diego)



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

SDR'15 Winncomm, session 1, San Diego, 26 March 2015

Eric Nicolle

François Delaveau, Renaud Molière, Christiane Kameni Ngassa, Claude Lemenager
Thales Communications & Security, Gennevilliers, France

Taghrid Mazloun, Alain Sibille
Telecom ParisTech, Paris, France

Contacts: francois.delaveau@thalesgroup.com

Supported by PHYLAWS project FP7 ICT Id-317562

THALES
Celeno

TELECOM
ParisTech

PHYLAWS

Imperial College
London

VTT

■ PROVIDING A RADIO-ADVANTAGE FOR THE LEGITIMATE LINK

- Artificial Noise (AN): Beamforming for legitimate data stream
 - Extraction of orthogonal directions to the legitimate link and transmission of noise streams
 - Maximization of the legitimate link budget providing a radio advantage for the legitimate link

Theories and implementations are numerous, practical performance is proven for WiFi

- S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise", *IEEE Transaction on Wireless Communications*, vol.7, no.6, June 2008
- www-phylaws.ict.org, deliverable D2.4

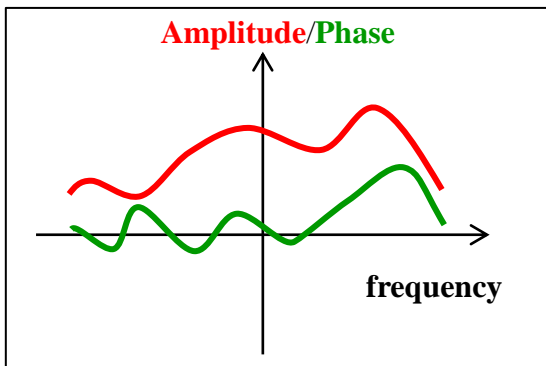
- Tag signals and Interrogation and Acknowledgement Sequences

■ PRINCIPLE OF SECRET KEY GENERATION

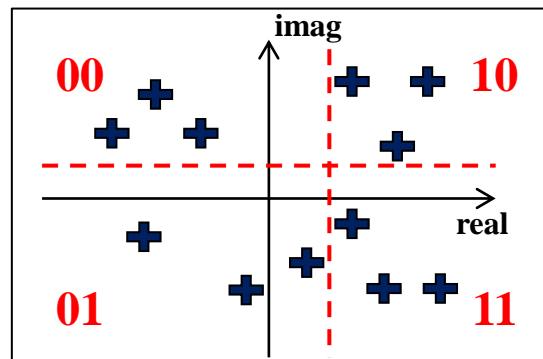
- The goal is to use channel randomness to extract secret keys
- Keys computed by legitimate users should be exactly the same
- Keys computed by eavesdroppers should be independent from the secret key

■ SIMPLIFIED GENERATION PROCESS OF SECRET KEYS

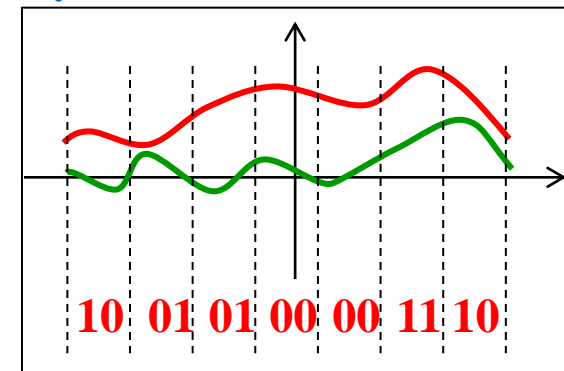
- Step 1: Estimation of the Channel Frequency Response (CFR)
 - Study of the correlation of the CFR
- Step 2: Quantization
 - channel coefficients are quantized according to a defined and public algorithm
- Step 3: Information reconciliation
 - Alice and Bob use error-correcting code (BCH) on the obtained key to suppress mismatch
- Step 4: Privacy amplification
 - Alice and Bob use hash functions to strengthen the quality of their key



- Estimation of the Channel Frequency Response (CFR)



- Quantization and study of repartition of the points



- Each quantized point is then translated into bits

■ FIRST CHALLENGE: CHANNEL CORRELATION

- Occurs in environment with low mobility, resulting in:
 - Stability in channel response, longer coherence time and not enough randomness in secret keys
- How to reduce channel correlation before quantization to improve quality of the keys?

■ STRAIGHTFORWARD METHOD TO REMOVE TEMPORAL CORRELATION

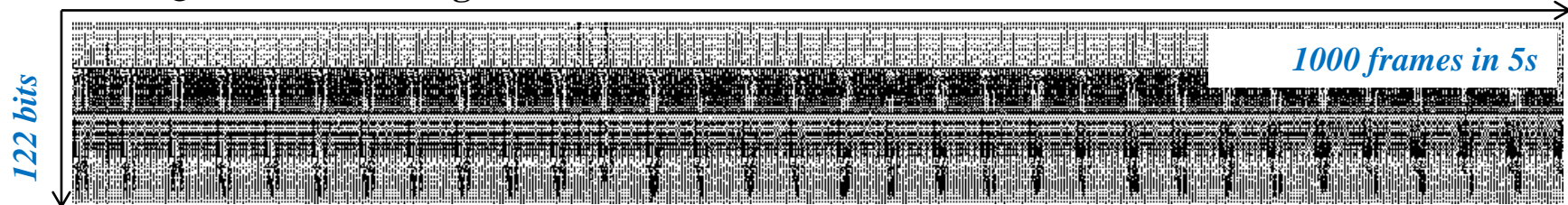
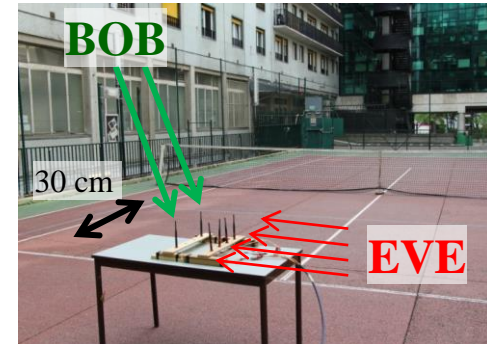
- Use of the eigenvector of the full covariance matrix of the channel response. However:
 - High complexity and Bob has to send the eigenvectors to Alice over the public channel
- Chan Chen; Jensen, M.A., "Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients," Mobile Computing, IEEE Transactions on , vol.10, no.2, pp.205,215, Feb. 2011

■ TOWARDS A LESS COMPLEX SOLUTION: A FIRST APPROACH

- Remove time correlation between frames
 - Compute cross-correlation coefficient between two consecutive frames
 - Select only frames for which the cross-correlation coefficient is above a given threshold T_t
- Remove correlation between frequency carriers
 - Compute cross-correlation between two consecutive frames
 - Select only frequencies for which the cross-correlation coefficient is above a given threshold T_f
- Bob has to send the position of the selected channel coefficients to Alice
 - Does not leak any information about the key to Eve

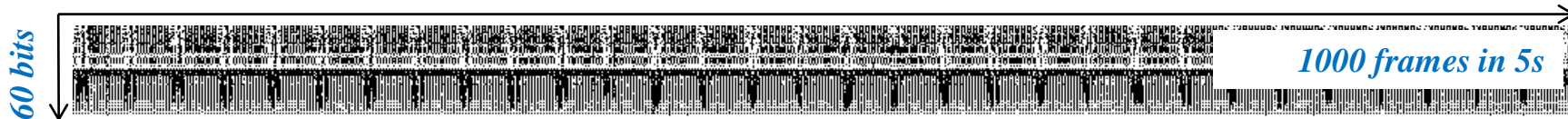
■ IMPACT OF CHANNEL DECORRELATION

- Worst case = LTE measurements in a stationary environment
 - Frequency: 2627.5MHz , Bandwidth: 10 MHz
 - Acquisition duration: 5 seconds
 - 6 antennas : 2 for Bob, 4 for Eve
- Quantization using all available channel coefficients



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

- Resulting keys after using the eigenvectors of the channel covariance matrix



The correlation problem persists

- Resulting keys after removing highly correlated frames with the low complex method

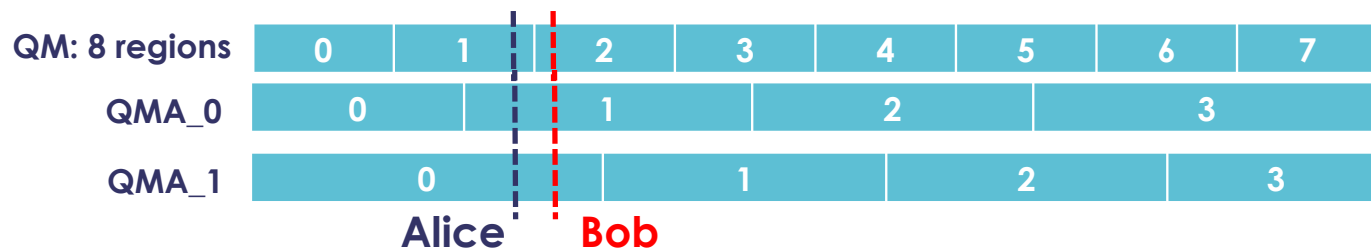


No obvious pattern is repeated in the keys

Selected Method in the following

■ QUANTIZATION

- **Objective:** generate binary symbols from channel measurements
- **Possibility to quantize RSSI or Channel State Information (CSI)**
- **Quantization algorithm:** CQA (CSI based, Wallace2010)
- **Advantage of CQA:** reduce mismatch between Alice and Bob keys



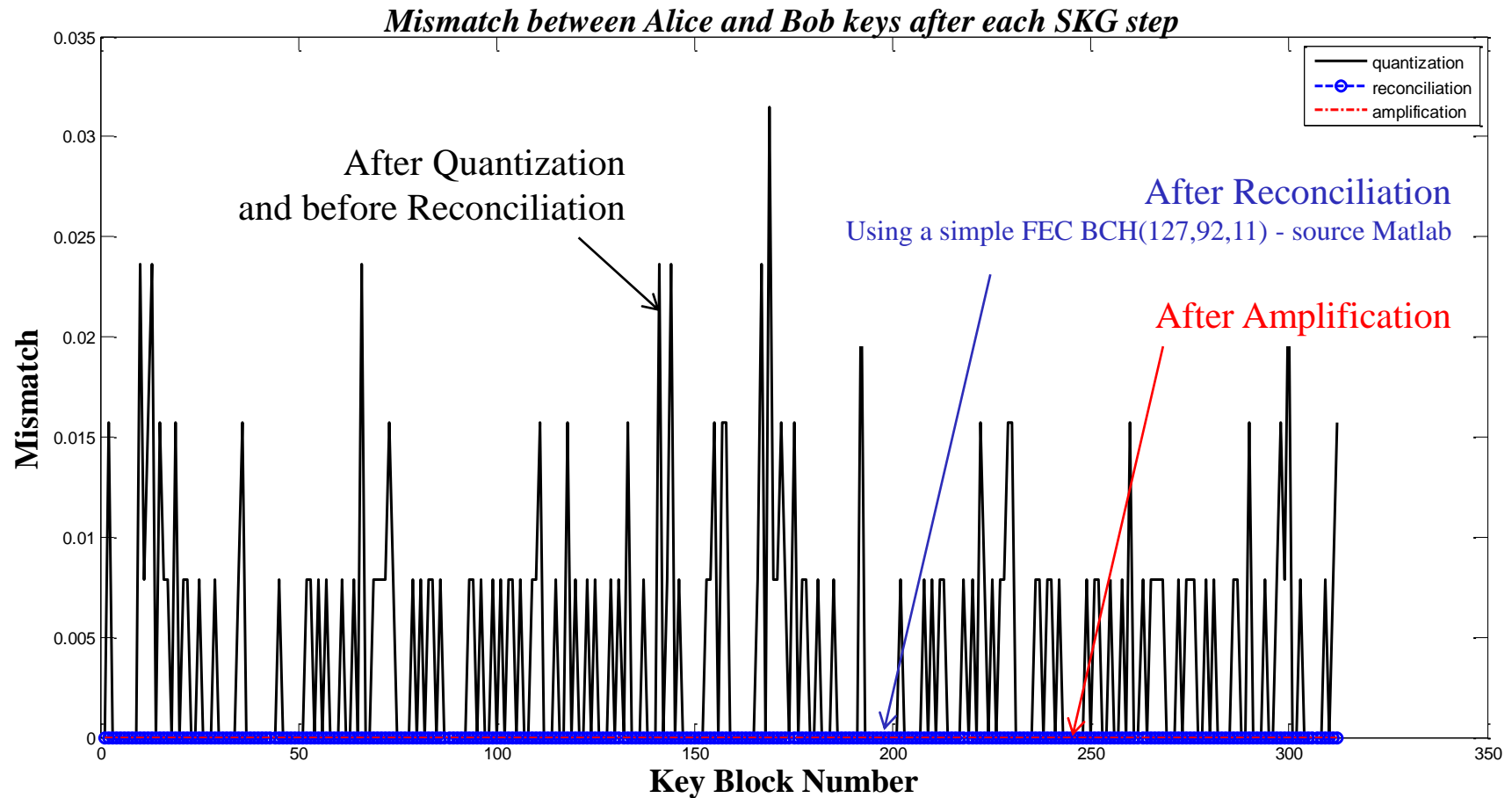
■ CQA ALGORITHM

- The total space of observable channel measurements is divided into regions
- Region boundaries can cause mismatch between Alice and Bob keys
- Two Maps are created and alternated to avoid this
- In CQA, Alice chooses one map (here QMA_1), evaluates the quantization symbol (0) and sends the number of the quantization map to Bob (1)
- Bob evaluate his quantization symbol using the map indicated by Alice (He also finds 0 using QMA_1)

- 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

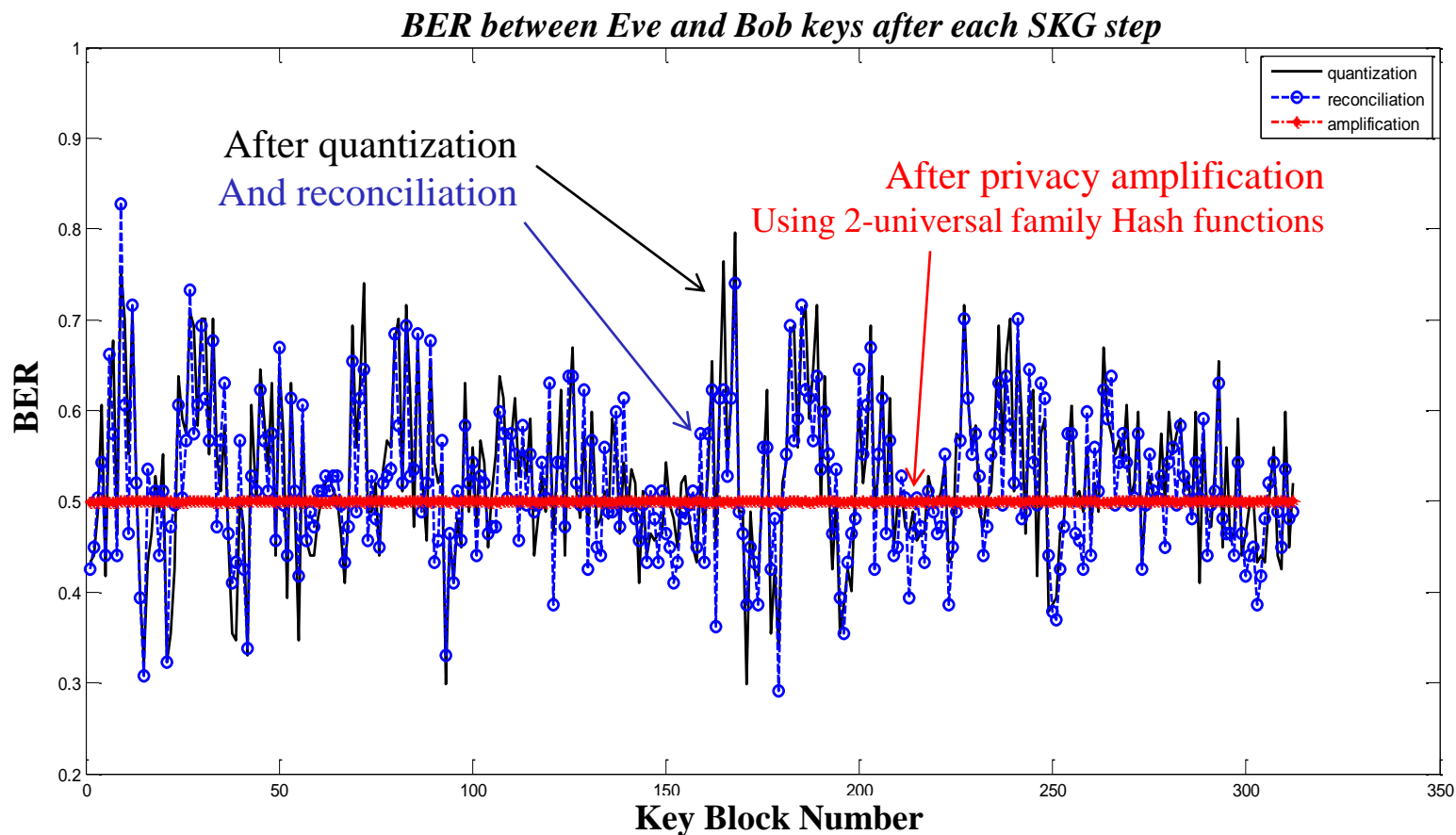
▪ SECOND CHALLENGE: CORRECT MISMATCH BETWEEN COMPUTED KEYS

- Mismatch can occur after quantization between keys computed by Alice and Bob
- Reconciliation through FEC is necessary to achieve a perfect equality of the keys



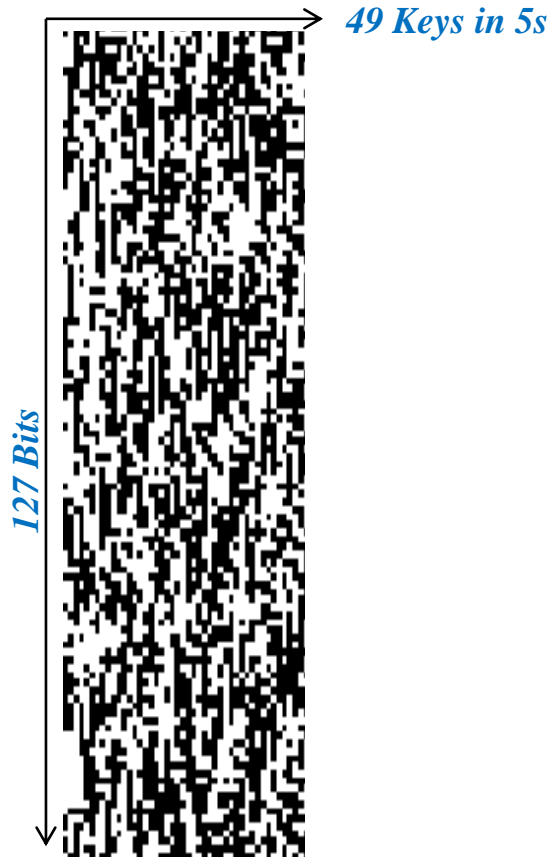
■ THIRD CHALLENGE: ENSURING LOW INFORMATION LEAKAGE TO EVE

- First criteria is a key Bit Error Rate
 - BER ~ 0.5 at Eve's side
- Amplification deletes information on Bob's key by ensuring a BER of 0.5
- Eve has no information on Bob's key

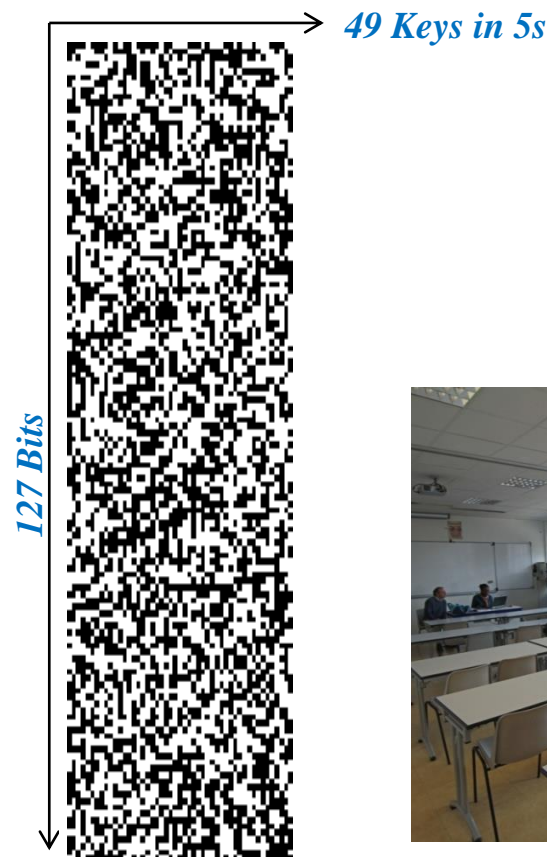


■ FOURTH CHALLENGE: RANDOMNESS OF THE KEY IMPACT OF AMPLIFICATION STEP

- **LTE – Indoor (Classroom)**
- Keys are generated from Channel Frequency Response measured on the PSS
 - Frequency: 2627.5MHz
 - Bandwidth: 10 MHz



- LTE Classroom after quantization



- LTE Classroom after amplification



■ FOURTH CHALLENGE: RANDOMNESS OF THE KEY IMPACT OF AMPLIFICATION STEP

- **LTE – Outdoor (street in Paris)**
- Keys are generated from Channel Frequency Response measured on the PSS
 - Frequency: 2645MHz
 - Bandwidth: 10 MHz

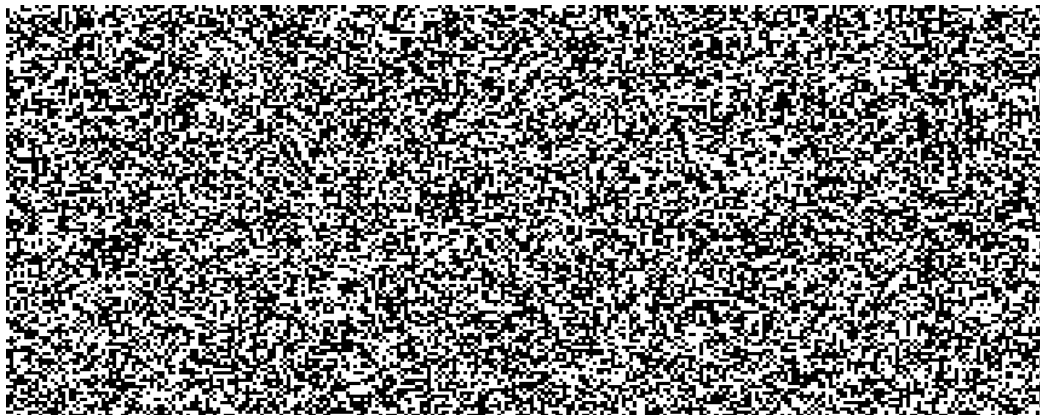
After
quantization



284 Keys in 5s

**More keys are
generated due to
higher mobility and
more scatterers in the
environment**

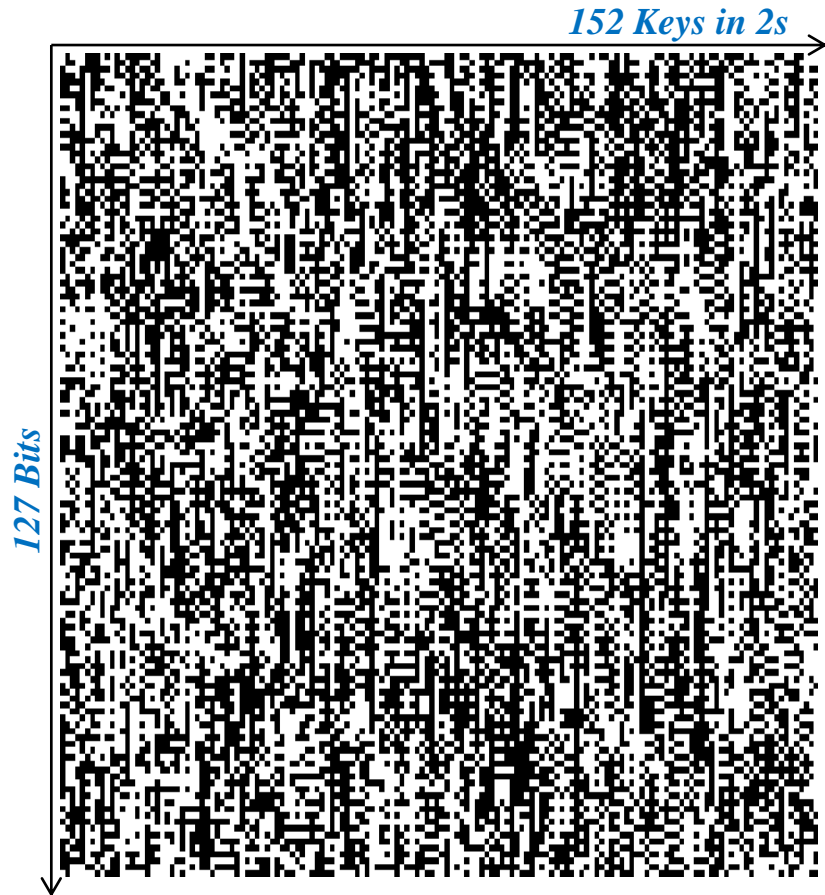
After
amplification



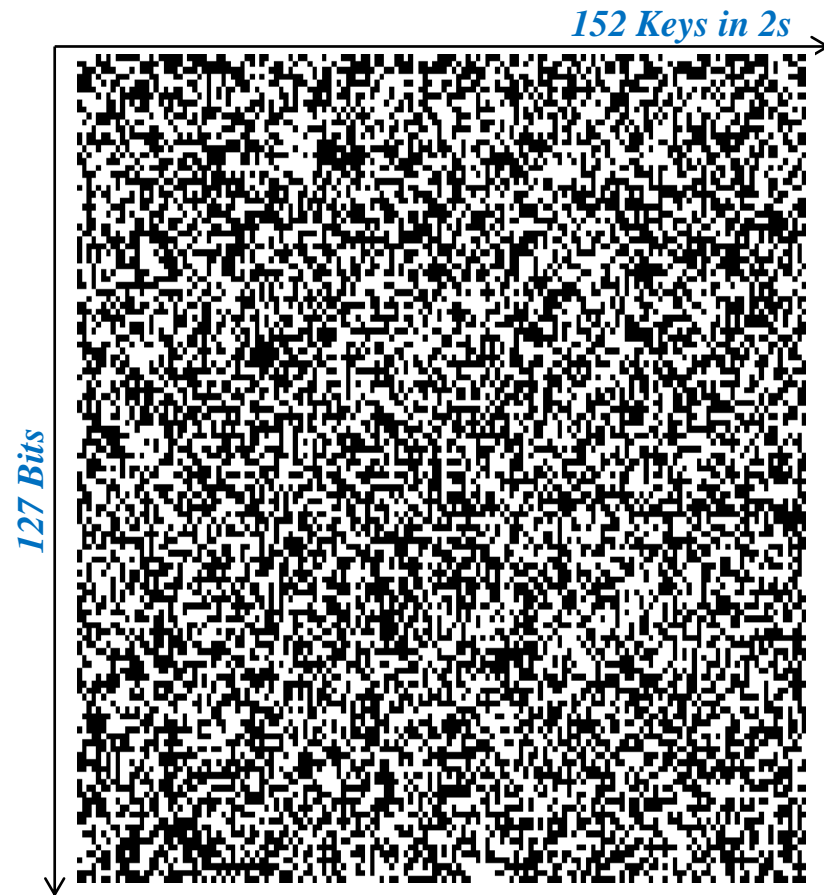
Thales proprietary information. All rights reserved

■ FOURTH CHALLENGE: RANDOMNES OF THE KEY IMPACT OF AMPLIFICATION STEP

- **WIFI – LOS (Indoor)**
- Keys are generated from Channel Frequency Response measured on the LTF
 - Frequency: 2462MHz
 - Bandwidth: 20 MHz



- WiFi LOS After quantization



- WiFi LOS After amplification

■ FOURTH CHALLENGE: RANDOMNES OF THE KEY - NIST CRITERIA

- 2 NIST tests are carried out to evaluate the quality of the keys
 - **Frequency monobit test**
 - Determines whether the numbers of 0s and 1s in the key are approximately the same as would be expected for a truly random sequence.
 - **Runs test**
 - Determines whether the oscillation between 0s and 1s is too fast or too slow

• NIST frequency monobit tests

LTE	Indoor (2.6GHz)	Outdoor (2.6GHz)
Quantization	98% (48/49)	99% (281/284)
Amplification	100% (49/49)	100% (284/284)

• Runs tests

LTE	Indoor (2.6GHz)	Outdoor (2.6GHz)
Quantization	27% (13/49)	80% (228/284)
Amplification	100% (49/49)	100% (284/284)

WIFI	LOS (2.4 GHz)	NLOS (2.4 GHz)
Quantization	87% (132/152)	100% (171/171)
Amplification	99% (151/152)	100% (171/171)

WIFI	LOS (2.4 GHz)	NLOS (2.4 GHz)
Quantization	84% (128/152)	99% (169/171)
Amplification	98% (149/152)	99% (170/171)

■ TEMPORARY CONCLUSION ON SECRET KEY GENERATION

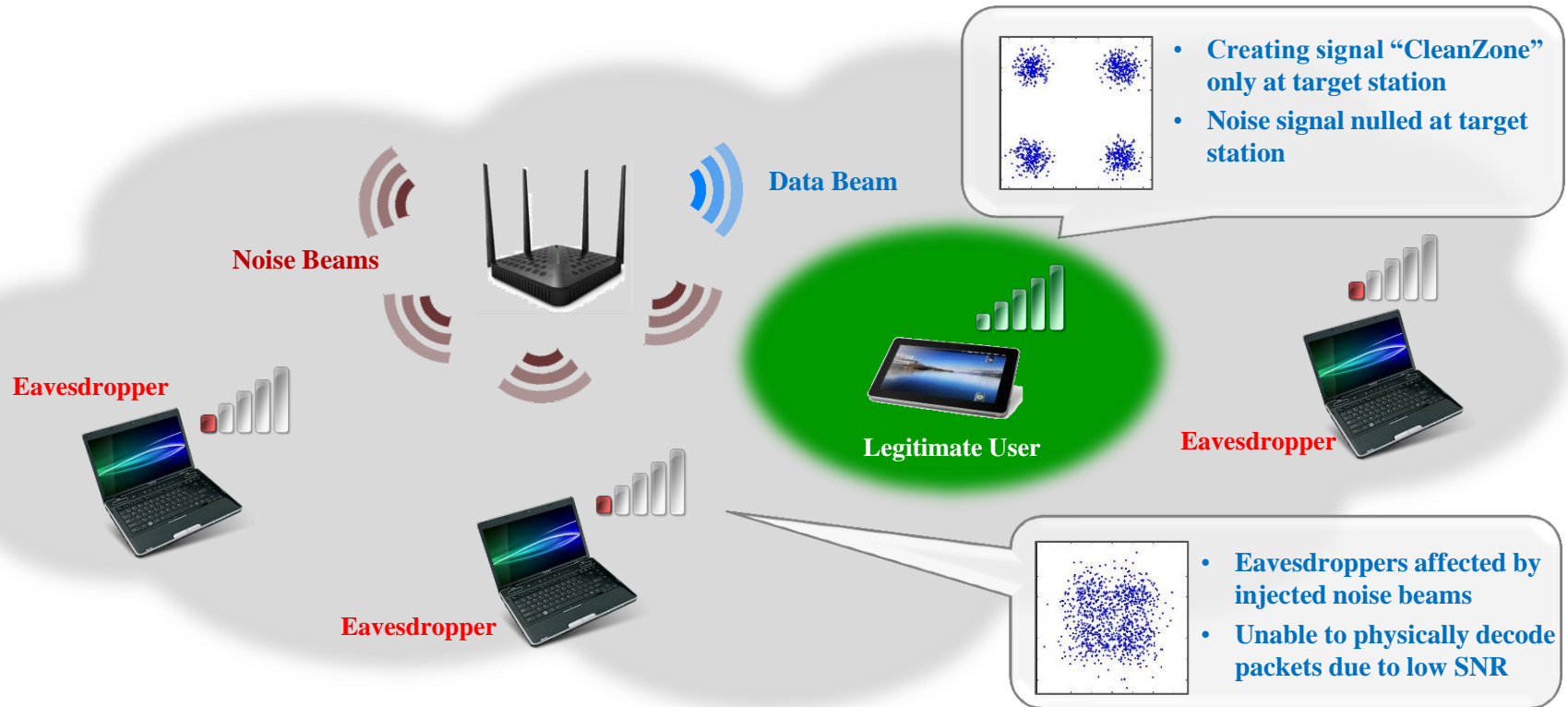
- Easy implementation
 - Low Complexity
 - Compliant with all modern digital standards
- Does not require better SNR for legitimate link than eavesdropper link
- Process provides good quality key (most often in short amount of time)
- Can take great advantage of TDD, Massive MIMO and Full-Duplex technologies
- However, provides limited results in stationary environment

■ EXPECTED UPGRADES IN VERY SHORT TERM

- Quality, length and rate of the key depends on the environment
 - Low diversity in some LOS environment
 - Longer time required to extract enough entropy to obtain good keys
 - Otherwise, Eve may recover the key in stationary and very low diversity case
 - New algorithms are expected to remove all the predictable components of the CFR
- For low SNR, reconciliation between Alice and Bob can be increased
 - Higher correction capacity of the codes uses by Alice and Bob for reconciliation
- Trade-off between algorithm complexity and
 - Mismatch between Alice and Bob
 - Information leakage
 - Quality of the key

■ PRINCIPLE ON MISO OR MIMO RATS

- PHY level security based on beamforming and directional artificial noise (AN) jamming
- Transmission of orthogonal noise beams that force very low SNR anywhere in space other than in a small sphere surrounding the legitimate user
- The result is high SNR at the legitimate user spatial location and very low SNR elsewhere
- Unlike standard encryption, e.g. WPA2, AN is “unbreakable” and is immune to offline processing attacks. Eavesdropper cannot even recover the bits by offline processing



■ IMPLEMENTATION OF ARTIFICIAL NOISE (AN)

- The 802.11ac/n frame has two parts to the preamble
 - Legacy part: used for initial synchronization
 - VHT part: used for channel estimation.
 - Beamforming mode is applied from VHT part onwards
- AN can be added from
 - The legacy part

Pro: can disrupt Eve synchronization

Con: gives Eve more time to estimate (and suppress) spatial noise

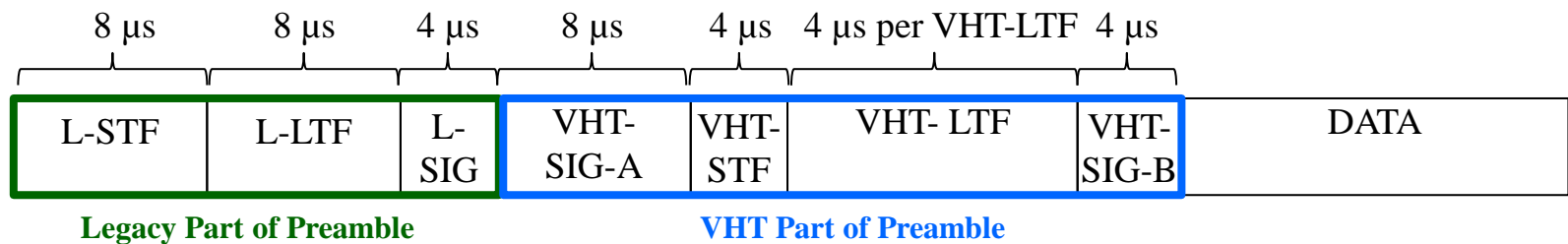
- The VHT part of preamble

Pro: Bob can estimate residual noise

Con: degrades channel estimate for Bob. Still allows Eve to estimate direction of spatial noise

- Data

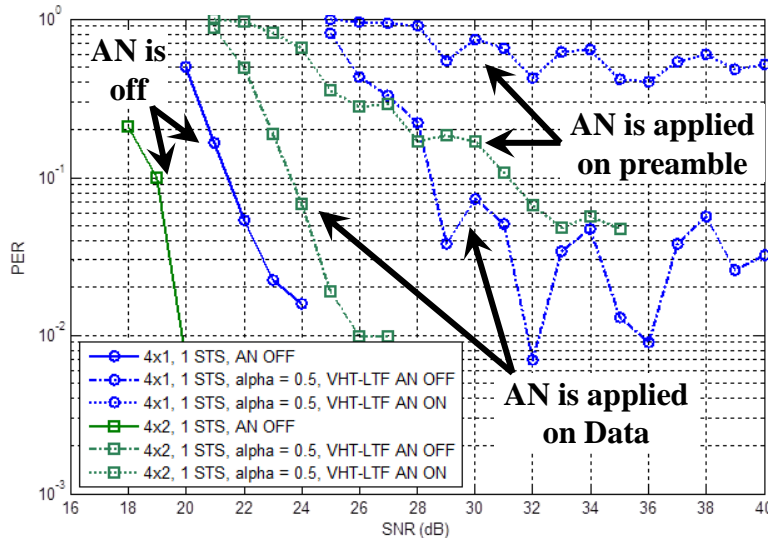
Pros: Bob has clean channel estimate. Eve cannot estimate noise from known preamble.



■ SIMULATIONS PARAMETERS

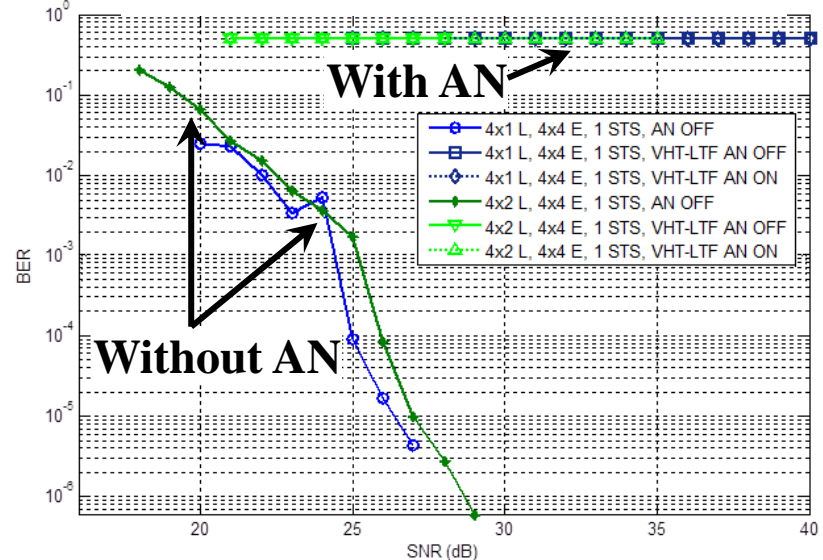
- Power allocation to noise is 50%
- Simulation includes effect of CSI quantization
- Communication scenario
 - 4xTX Alice
 - Number of spatial stream: 1
 - Constellation: 64-QAM
 - Rate: 5/6
 - 1xRX Bob (addition of 3 noise streams)/ 2xRX Bob (addition of 2 noise streams)
 - 4xRX Eve. Eve was modeled as a “standard” receiver

PER for Bob in different AN schemes



- Performance loss for single antenna Bob is 7dB when AN applied from Data portion
- Application of AN on preamble significantly increases noise

BER for different AN schemes



- BER for Eve is 50% for every cases

■ CONCLUSION ON ARTIFICIAL NOISE

- **Easy implementation**
 - Low Complexity
 - Compliant with all modern digital standards
 - Take advantage of space time block coding for security purposes
- **Provide radio advantage for legitimate link**
 - Even if Eve has more antennas than Bob
 - Independent on the Modulation Coding Scheme (MCS)
 - Resilience against offline processing
- **Provides suitable conditions for secrecy coding**

■ LIMITS

- **CSI must be protected from Eve**
 - Protection can be decreased if channel matrix is revealed
 - Necessity to protect of sounding frame
- **What if Eve has more antennas capabilities ?**

■ OBJECTIVE OF SECRECY CODING

- **Designing error correcting codes with secrecy capacity**
- **Providing reliable communication to legitimate users by approaching the Shannon capacity**
- **Mitigating the information for any Eavesdropper (at any other location)**

■ REQUIREMENTS

- **Legitimate link must have a better radio link (\sim SNR in AWGN channel) than Eve**

■ MAIN CHALLENGES

- **Existence of optimal Secrecy Codes is proven. No straightforward general design method**
- **Explicit secrecy code construction only for « ideal » channel models (BEC, BSC)**
- **Existing design of polar codes for the wiretap AWGN channel applies only for very long code length (2^{20})**
- **Researches are in progress for advanced channel models (lattice coding, etc.)**

■ PROPOSAL FOR A (SIMPLIFIED) SECRECY CODING SCHEME

- **Take advantage of the secrecy properties of the polar code**
- **Mitigate the poor finite-length performance of the polar code by exploiting the error-correction capability of LDPC codes**

■ THE PROPOSED SECRECY CODING (SIMPLIFIED) SCHEME

- Concatenation of two codes
 - Outer code: a polar code to provide secrecy
 - Inner code: any error-correcting code able to provide sufficient error correction capability



■ POLAR CODES

- Construction
 - Length of the code: $N = 2^n$
 - Design of finite-length polar code is dependent on a target channel's error probability
- Advantages of polar codes
 - Capacity achieving code for binary input symmetric discrete memoryless channels
 - Explicit code design
 - Low encoding and decoding complexity: $O(N \log(N))$
 - Provide secrecy over the AWGN channel when the block length goes to infinity
- Drawbacks
 - Poor decoding performance at moderate and short block length
 - Not practical for real communication systems

■ DESIGN OF THE LDPC CODE (AS SIMPLE AND CLASSICAL AS POSSIBLE)

- Quasi-Cyclic LDPC code defined in the 802.11 standard
- Length of the code: $N = 1296$
- Rate of the code: $R = 5/6$

■ DESIGN OF POLAR CODE

- From Information Theory
- H.Mahdavifar and A.Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," 57 ed IEEE Transactions on Information Theory, 2011, pp. 6428-6443

WP4-T4.2 – POLAR CODES– Brief Introduction

■ Polar codes

- Introduced by Arikan in 2008
 - Arikan, E., "Channel polarization: A method for constructing capacity-achieving codes," Information Theory, 2008. ISIT 2008. IEEE International Symposium on , vol., no., pp.1173,1177, 6-11 July 2008
 - Arikan, E., "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," Information Theory, IEEE Transactions on , vol.55, no.7, pp.3051,3073, July 2009
- Capacity achieving for any binary-input discrete memoryless channel
- Explicit code construction
- Low decoding and encoding complexity:

■ Binary Discrete Memoryless Channel (B-DMC)

- Generic B-DMC,
- Transition probabilities: $(\quad | \quad)$
- Input alphabet: $\{ \quad \}$, output alphabet: arbitrary
- uses of $(\quad | \quad)$

■ Example of Binary Discrete Memoryless Channels

- Binary Erasure Channel (BEC)
- Binary Symmetric Channel (BSC)

Year 2 review - Meeting EC Brussels, 09-September-2015

PHYLAWS FP7 ICT call n. 34317562

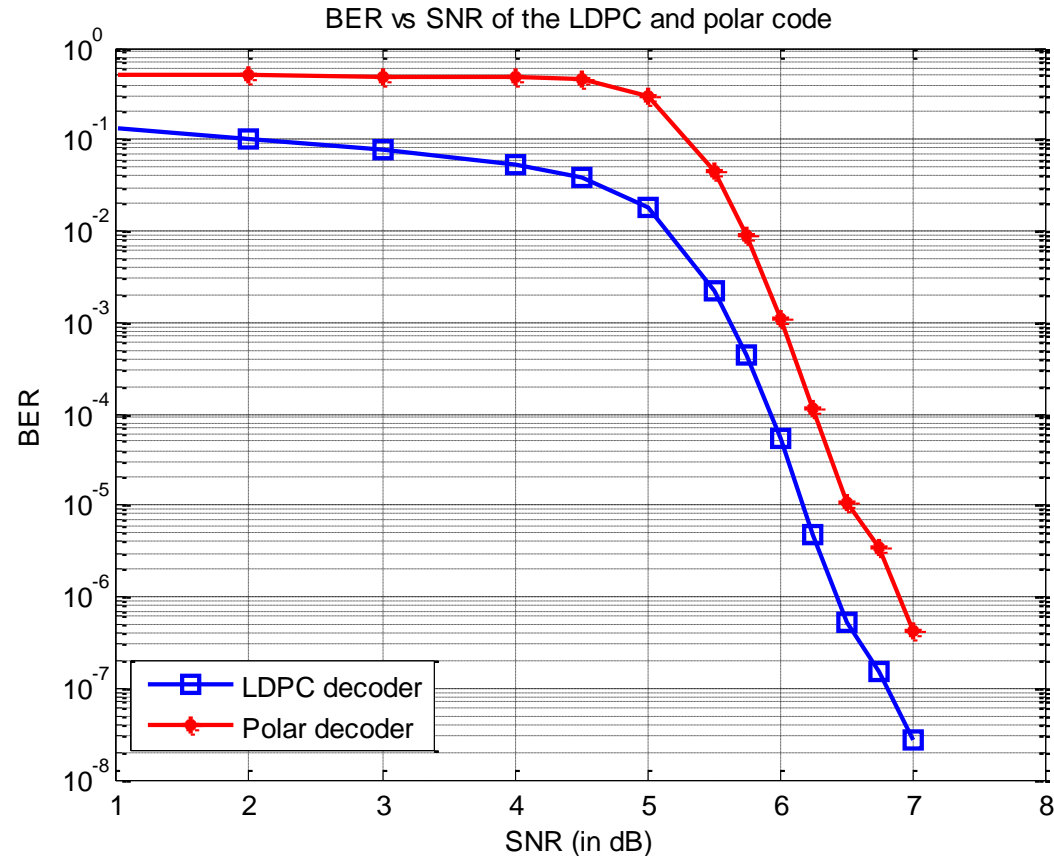


1

■ FIRST SIMULATIONS WITH GENERATED QPSK SIGNALS

■ CODE PARAMETERS

- $N = 2^{10} = 1024$
- AWGN
- QPSK Modulation
- Belief propagation algorithm to decode LDPC and polar codes
- **Final secrecy code rate: 0.35**



■ RESULTS AT THE OUTPUT OF THE SECRECY CODING SCHEME

BER = 0.5 when SNR ≤ 4 dB

BER < 10⁻⁵ when SNR ≥ 6.5 dB

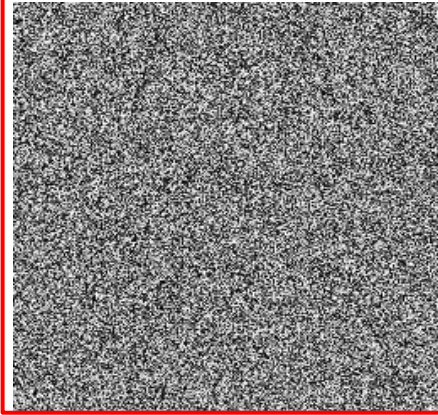
Security gap (~ Min radio advantage): 2.5 dB

Original Image (to be sent over the wiretap channel)

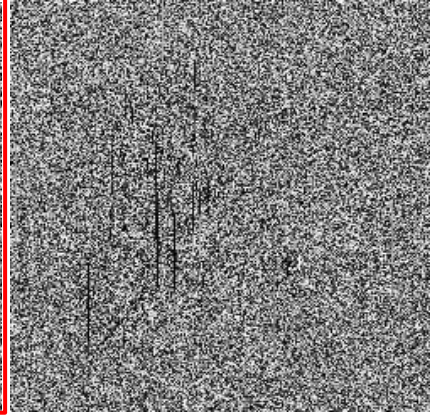


IMAGE RECEIVED BY EVE

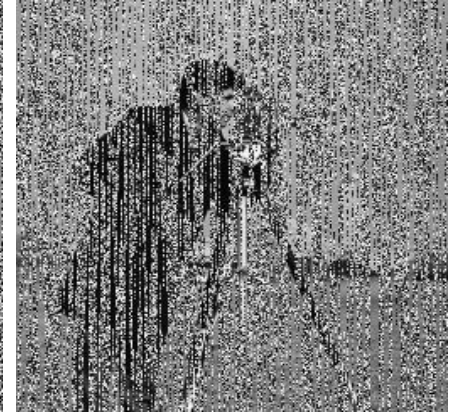
Received image, SNR = 4dB



Received image, SNR = 4.5dB



Received image, SNR = 5dB



Received image, SNR = 5.5dB



Received image, SNR = 6dB



Received image, SNR = 6.5dB



Received image, SNR = 7dB



IMAGE RECEIVED BY BOB

■ PERFORMANCE ILLUSTRATION (TRANSMISSION AN IMAGE)

- The received image contains random pixels when $\text{SNR} \leq 4 \text{ dB}$
- Perfect reception of the image when $\text{SNR} \geq 6.5 \text{ dB}$

Security gap : 2.5 dB
~ Min radio advantage

■ SUMMARY OF WORK ON SECRECY CODING

- Evidence that Eve's BER should be close to 0.5
 - At SNR = 5 dB, BER = 0,297 but Eve can guess the transmitted image from the received one
- The **polar code provides security**
 - Thanks to the polar code BER = 0.5 when SNR \leq 4dB
 - No information is leaked to Eve
- Poor overall performance of the polar code (due to the small length of the code)
 - Final BER is always higher than the error probability of the BSC channel (LDPC decoder BER)
- The **LDPC code provides reliability**
 - Good transition to the waterfall region, no error floor at 10^{-8}

■ PROVISORY CONCLUSION ON SECRECY CODING

- Do not require mobility or scatterers in the environment
- Secrecy code requires better SNR for legitimate link than eavesdropper link
- Reliability is ensured by LDPC codes
 - already widely used in wireless standard
- Secrecy is achieved by only adding a polar code
 - Low encoding and decoding complexity
 - Loss of reliability (0.5 to 1 dB) due to short length of polar code using belief propagation

Thank you for your attention



Find more information on our website

www.phylaws-ict.org

R.Moliere
F. Delaveau
C. Kameni

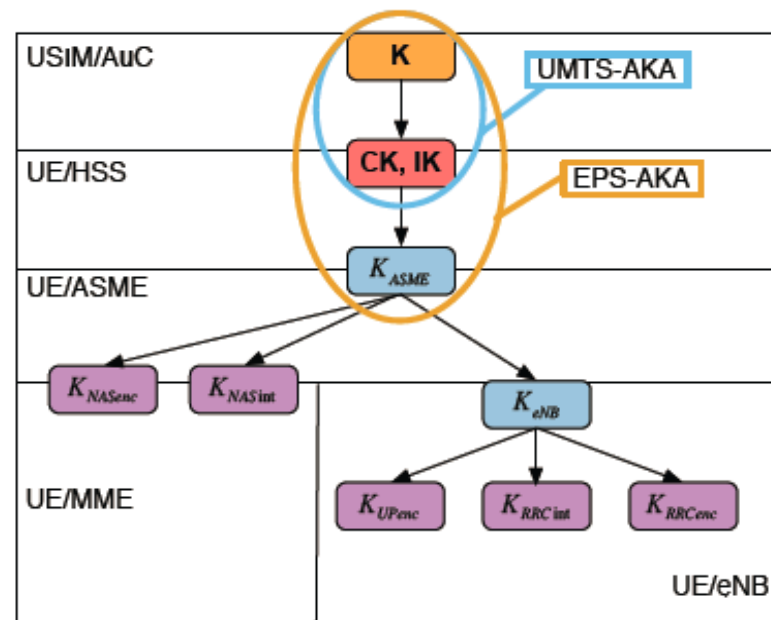
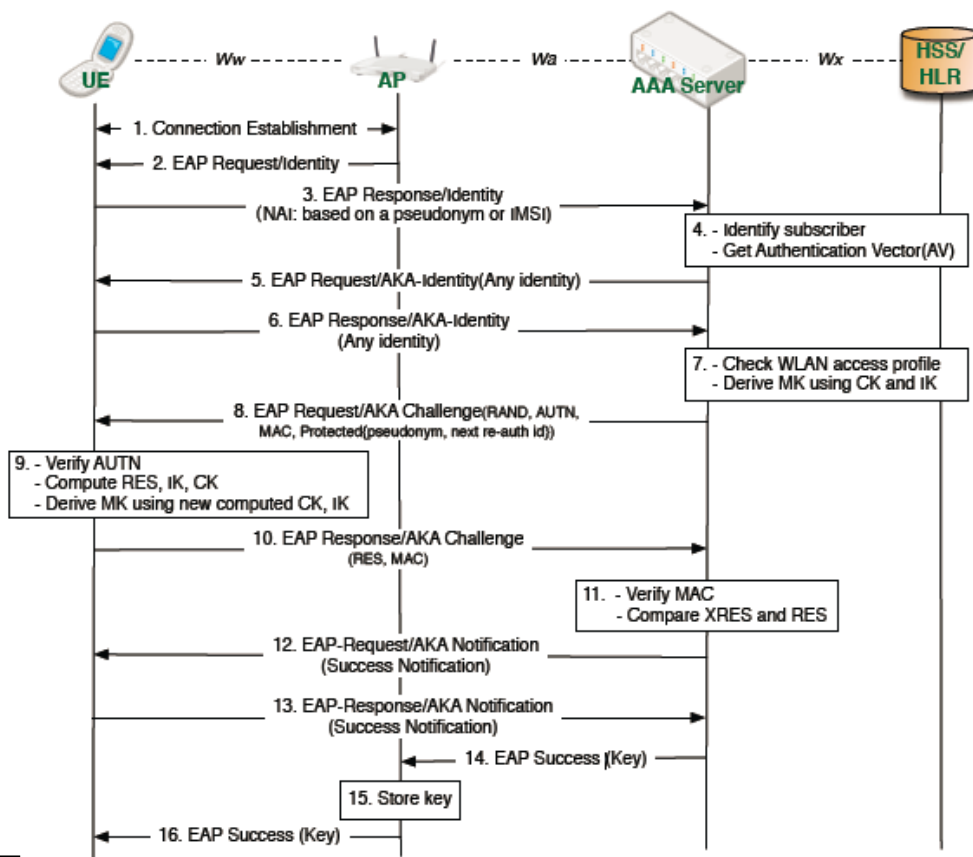
renaud.moliere@thalesgroup.com
francois.delaveau@thalesgroup.com
christiane.kameni@thalesgroup.com

phone : + 33 (0)1 41 30 33 60
phone : + 33 (0)1 46 13 31 32
phone : + 33 (0)1 41 30 30 19

AN	Artificial Noise	NETSEC	Network Transmission Security
BCH	Bose Ray-Chaudhuri Hocquenghem	NLOS	Non Line Of Sight
BER	Bit Error Rate	PHYSEC	Physical Layer Security
BTS	Base Transceiver Station	PSS	Primary Synchronization Sequence
CIR	Channel Impulse Response	RAT	Radio Access Technology
CFR	Channel Frequency Response	SIM	Subscriber Identity Module
CQA	Channel Quantization Algorithm	SKG	Secret Key Generation
COMSEC	Communication Security	SNR	Signal to Noise Ratio
CRS	Cell-specific Reference Signal	SS7	Signaling System No.7
FDD	Frequency Division Duplex	SSS	Secondary Synchronization Sequence
FEC	Forward Error Correction	TDD	Time Division Duplex
GSM	Global System for Mobile communications	TMSI	Temporary Mobile Subscriber Identity
IMSI	International Mobile Subscriber Identity	TRANSEC	Transmission Security
LDPC	Low Density Parity Check	UMTS	Universal Mobile Telecommunications System
LOS	Line Of Sight	VIP	Very Important People
LTE	Long Term Evolution		
LTF	Long Training Field		
MAC	Media Access Control		
MIMO	Multiple Input Multiple Output		
NIST	National Instrument of Standards and Technology		

APPENDIX 1– INTEREST OF PHYSEC: More on security lacks in mobile network

Hyeran Mun, Kyusuk Han and Kwangjo Kim 1-4244-2589-1/09/ \$20.00 2009 IEEE,
 “3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement based on EAP-AKA »



K_{NASenc} : Protection of NAS traffic with particular encryption
 K_{NASint} : Protection of NAS traffic with particular integrity
 K_{UPenc} : Protection of UP traffic with particular encryption
 K_{RRCint} : Protection of RRC traffic with particular integrity
 K_{RRCenc} : Protection of RRC traffic with particular encryption

(T/I)MSI AV RAND RES etc. ARE EXCHANGED IN CLEAR TEXT WITHOUT TRANSEC PROTECTION
→ PASSIVE EVE CAN DECODE
→ ACTIVE EVE CAN JAM, SPOOF, REPLAY...

WHEN EVE GET THE KEY K SHE GETS ALL...
...BY PASSIVE MONITORING ONLY.



Basics of PHYsical LAYer Wireless Security FWD sense - Wiretap channel – Passive Eve



THREE BASIC MODELS OF THREATS

1 /

Three basic models of threats 1/3

Passive Eve - Short model description:

Eve's procedures

- Aware about the standard, sometimes about subscriber keys
- Records all signal
- demodulates and decodes signalling and data messages between Alice and Bob
- does not emit any signal

Eve's limits / drawbacks

- cannot influence the legitimate exchanges
- Very sensitive to radio propagation and poor energy budget

Eve's advantages

- no real-time constraints of any kind

Major risks for legitimates

- ⇒ Monitoring of 2G (A5-1/2 A8 A3) and WLAN (WEP and WPA - WPA2 in question)
- ⇒ In 3G 4G, maximal risk occurs when Eve is informed about their Subscribers keys (Ki on SIM, K on USIM, etc.) and can also compute off-line the complete legitimate data.

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

PROPHYLAXE AND PHYLAWS WORKSHOP Remlingen - 27 August 2015.

Information propiétaire de Thales. Tous droits réservés / Thales proprietary information. All rights reserved

Workshop PROPHYLAXE and PHYLAWS 2015-08-27
Presentation of PHYLAWS project FP7 ICT Id-317562

THALES
Celeno
TELECOM
PARISTECH
PHYLAWS
Imperial College
London
VIT

■ OBJECTIVE

- Eliminate any mismatch after quantization between Alice and Bob keys
- Minimize information leakage to Eve

■ SECURE SKETCH BASED ON ERROR-CORRECTING CODES

- Outputs public information s about an input K
- Does not reveal K but allows exact recovery of K given K' close to K

■ INFORMATION RECONCILIATION ALGORITHM STEPS

- **Alice:**
 - selects a random codeword c from an error-correcting code \mathcal{C}
 - computes the secure sketch $s = K_a \oplus c$
 - sends the shift s to Bob over the public channel
- **Bob:**
 - Bob subtracts s from its key $K_b : c_b = K_b \oplus s$
 - Bob decodes c_b to recover the random codeword c_b and gets \hat{c}
 - Bob computes K_a by shifting back and gets: $\widehat{K}_a = \hat{c} \oplus s$

Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” SIAM J. Comput., vol. 38, no. 1, pp. 97–139, 2008.

Qian Wang; Hai Su; Kui Ren; Kwangjo Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," INFOCOM, 2011 Proceedings IEEE , vol., no., pp.1422,1430, 10-15 April 2011

▪ OBJECTIVE

- Reduce Eve's amount of information on the key
- Improve the randomness of the key
- Can be performed using hash function or extractors
 - We choose a two-universal family of hash functions

▪ TWO-UNIVERSAL FAMILY OF HASH FUNCTIONS

- A class \mathcal{G} of functions $\mathcal{A} \rightarrow \mathcal{B}$ is two-universal if for all $x_1 \neq x_2$:

$$\Pr[g(x_1) = g(x_2)] \leq \frac{1}{|\mathcal{B}|}$$

when g is chosen randomly from \mathcal{G}

▪ CONSTRUCTION OF A TWO-UNIVERSAL FAMILY OF HASH FUNCTIONS

- Select a random element $a \in GF(2^n)$ and interpret the key K as an element of $GF(2^n)$
- Consider the function $\{0,1\}^n \rightarrow \{0,1\}^r$ assigning to K the first r bits of $aK \in GF(2^n)$
- 2-Universal family of hash functions for $1 \leq r \leq n$

Bennett, C.H.; Brassard, G.; Crepeau, C.; Maurer, U.M., "Generalized privacy amplification," Information Theory, IEEE Transactions on , vol.41, no.6, pp.1915,1923, Nov 1995