EUROPEAN COMMISSION

Community Research

PHYLAWS

SEVENTH FRAMEWORK PROGRAMME

ICT Call 8

PHYsical LAyer Wireless Security

Secret Key Generation

3GPP SA3#80 Meeting
Tallinn, Estonia – 25/08/2015

Renaud Moliere

Coordinator Contact : F. Delaveau : francois.delaveau@thalesgroup.com phone : + 33 (0)1 46 13 31 32
Author Contact : R. Moliere : renaud.moliere@thalesgroup.com phone : + 33 (0)1 41 30 33 60

1- ABOUT THE PHYLAWS PROJECT

2- CURRENT SECURITY THREATS IN PUBLIC TELECOMMUNICATIONS

3- PRESENTATION OF PHYSICAL LAYER SECURITY

4- SECRET KEY GENERATION - DESCRIPTION

5- SKG - EXPERIMENTAL RESULTS

6- SKG – PRACTICAL POINT OF VIEW

7- CONCLUSION

8- APPENDICES

9- ACRONYMS

- **MAIN GOALS**
  - **Studying and improving security of wireless links by developing key-free solutions based on Physical Layer Security (PHYSEC)**
  - **Searching and testing practical implementations in existing and future public Radio Access Technology (RAT) such as WiFi and LTE**

- **AN ORIGINAL APPROACH**
  - **Merge academic and industrial skills on radio-channels, radio-communications and security**
  - **Test usual hypothesis with return of practical experience**
  - **Consider any kind of threats at physical layer: passive and active attacks**
  - **Focus on signaling and access phases of RATs, 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
Email: francois.delaveau@thalesgroup.com
Project website: www.phylaws-ict.org

4 Partners
Institut Mines-Telecom ParisTech (FR),
Imperial College London (UK),
Teknologian Tutkimuskeskus VTT (FI),
Celeno Communications Israel Ldt (IS).

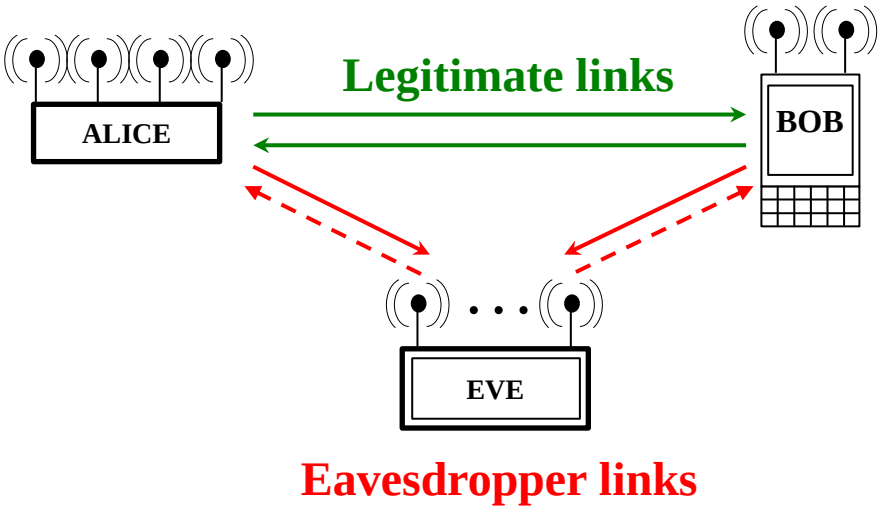
Duration
4 years (November 2012 – October 2016)

Funding scheme
STREP

Contract Number
CNECT-ICT-317562

COMMUNICATION SCENARIO

- LEGITIMATE links are Alice to/from Bob
- EAVESDROPPER links are Alice to Eve and Bob to Eve
- Eve can be
  - Passive
  - Man-In-The-Middle
  - Active



DEFINITIONS

- TRANSEC (Transmission Security) is the waveform protection of the legitimate link face to interception of the transmitted radio signal and to intrusion attempts.

- NETSEC (Network Transmission Security) is the protection of the signalling of the network of the legitimate link. Usual solutions are authentication and integrity control, sometimes ciphering of signalling in military networks.

- COMSEC (Communication Security) is the protection of the content of user messages. Most of solutions are based on ciphering and integrity control schemes.

- **FLAWS OF CURRENT SECURITY TECHNIQUES HAVE BEEN REVEALED AND EXPLOITED RECENTLY**
  - **Traditional techniques to obtain cryptographic keys**
    - **Hacking of cryptographic algorithm**
      - **Algorithms A5/1-2, A3, A8 (see appendices 5 and 6)**
    - **Spoofing attack (IMSI Catcher)**
      - See *Bott, R. & Frick, J. Method for identifying a mobile phone user or for eavesdropping on outgoing calls. Patent EP 1051053 B1. 2003*
  - **Modern techniques to obtain cryptographic keys**

    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 (to obtain Ki keys)

    - **Hacking of SIM manufacturers by security agencies**
    - **Subscribers' keys may not be secret in practice**

CONCLUSION ON RECENT EVENTS

- **Lack of perfect forward secrecy**
  - **Information leakage in signaling messages**
  - **Part of authentication procedure is in clear text**
  - **Concerns both downlink and uplink**
- **Privacy can be attacked with the knowledge of the Ki Keys**
  - **Distribution of unchanging cryptographic keys can be a threat to security**
  - **New add-on security schemes must be developed independently of Ki keys**

LONG TERM SOLUTION

- **Achieve forward secrecy of signaling and data messages**
- **Achieve return secrecy of access and data messages**
- **Prevent disclosure of future keys with the knowledge of past keys**

- **NEW ADD-ON SECURITY SCHEMES SHALL**
  - **Not rely on pre-distribution of keys**
  - **Be compatible with an infinite 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**

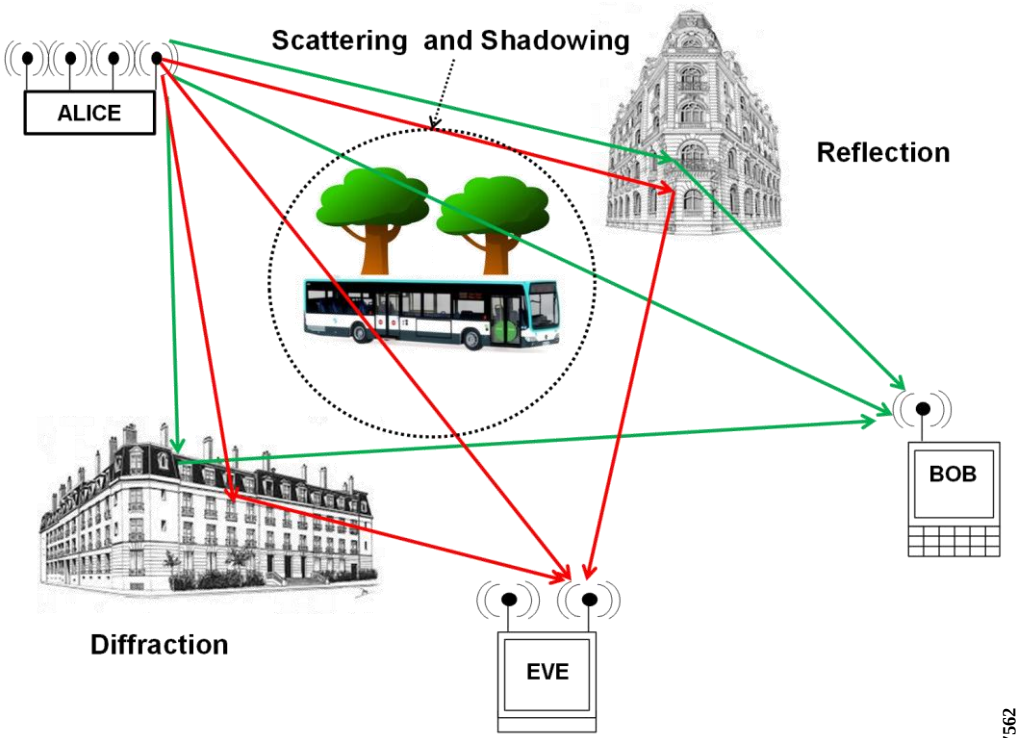
EXPLOITING THE RANDOM PROPAGATION OF WIRELESS RADIO CHANNEL

- **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 → Bob and Bob → 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

- **3 MAIN APPROACHES FOR PHYSEC**
  - **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

  - **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**

    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

  - **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

HYPOTHESIS FOR PHYSEC

- Channel reciprocity
  - Direct application to TDD RATs,
  - Channels measurements are performed in the time of coherence of the channel
- Spatial decorrelation between Bob and Eve for distances longer than λ/2 (NLOS case) and to 4λ (LOS case)
- Authenticated Channel State Information between Alice and Bob

ADVANTAGES OF PHYSEC

- Does not rely on pre-distribution of cryptographic key
- Ensures security pairing and authentication of devices
- Low impact at upper layer (MAC, software)
- Can take large benefits of advanced RATS such as massive MIMO and Full-Duplex
- Easy to implement and compliant with current RAT (especially WiFi and LTE)

REMAINING GAPS OF PHYSEC

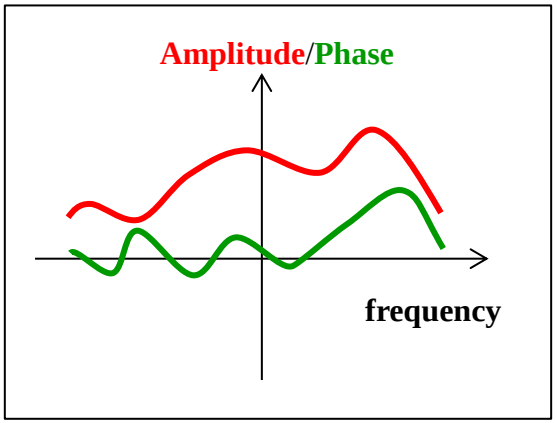
- All PHYSEC schemes need authenticated and precise Channel State Information
  - The channel estimate must be exclusively known by Alice and Bob
  - Reconciliation between Alice and Bob to delete estimation mismatches <u>without any exchange</u>
- Some PHYSEC schemes requite a better SNR for the legitimate links
- More investigations required for FDD schemes

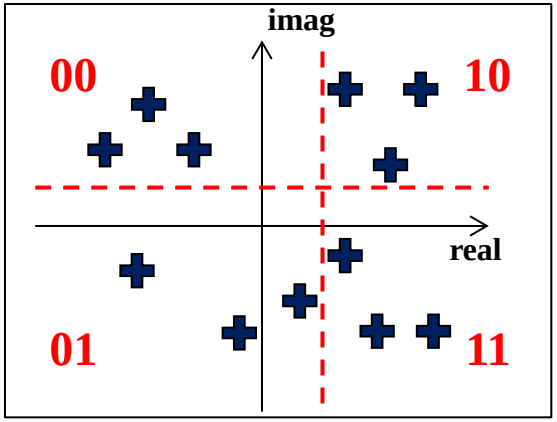
PRINCIPLE

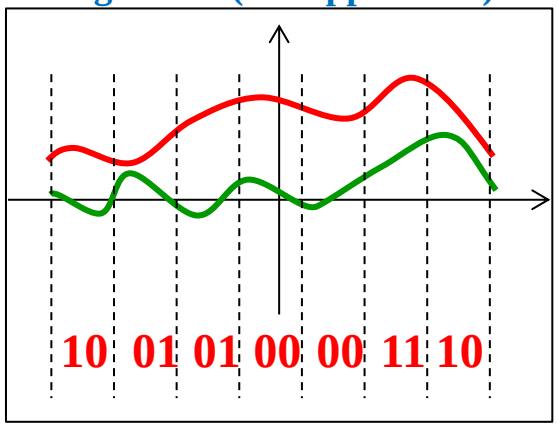
- The goal is to use channel randomness to extract Transec keys
- Keys computed by legitimate users should be exactly the same
- Keys computed by eavesdroppers should be indepedent from the secret key

SIMPLIFIED GENERATION PROCESS OF SECRET KEYS

- Step 1: Quantization
  - channel coefficients are quantized according to a defined and public algorithm (see Appendix 2)





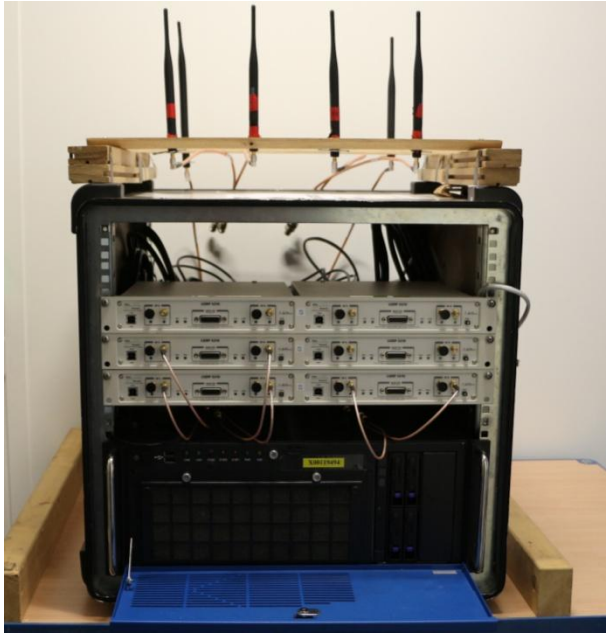


- Estimation of the Channel Frequency Response (CFR)
- Quantization of the CFR
- Study of the repartition of the quantized points
- Each quantized point is then translated into bits according to its position

- Step 2: Information reconciliation
  - Alice and Bob use error-correcting code on the obtained key to suppress mismatch
- Step 3: Privacy amplification
  - Alice and Bob use hash functions or extractors to strengthen the quality of their key

EXPERIMENT TEST BED

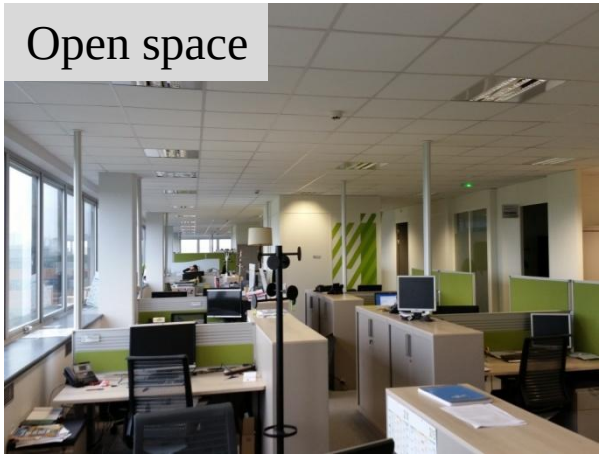
- **Compatible with 4 public networks**
  - WiFi (2.4GHz)
  - LTE (800/2600MHz)
  - UMTS (2.1GHz)
  - GSM (900/1800MHz)
- **Acquisition capabilities**
  - Up to 6 channels for WiFi/LTE 20MHz
  - Up to 12 channels for UMTS/GSM or LTE 10MHz
- **Records**



- WiFi Access Point

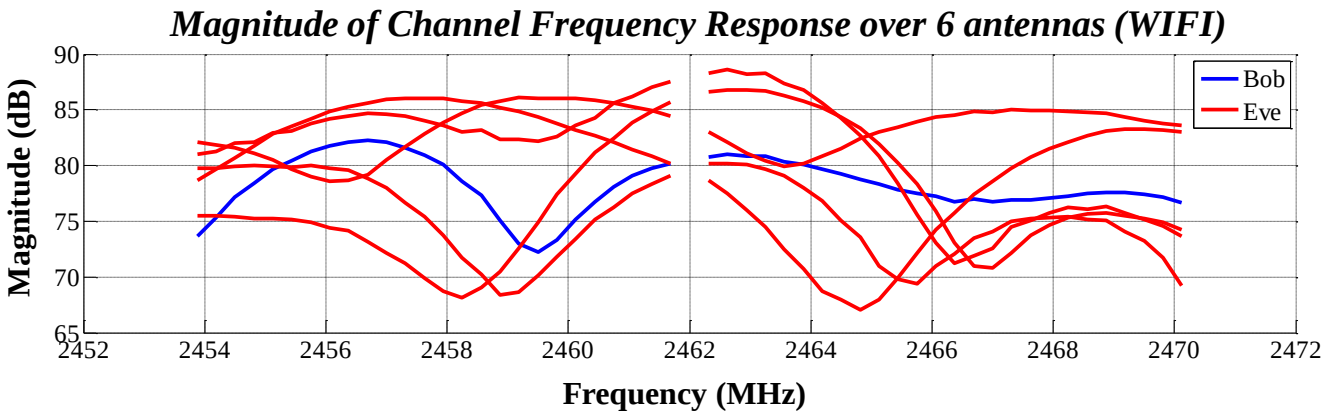
- Base Transceiver Station (BTS)

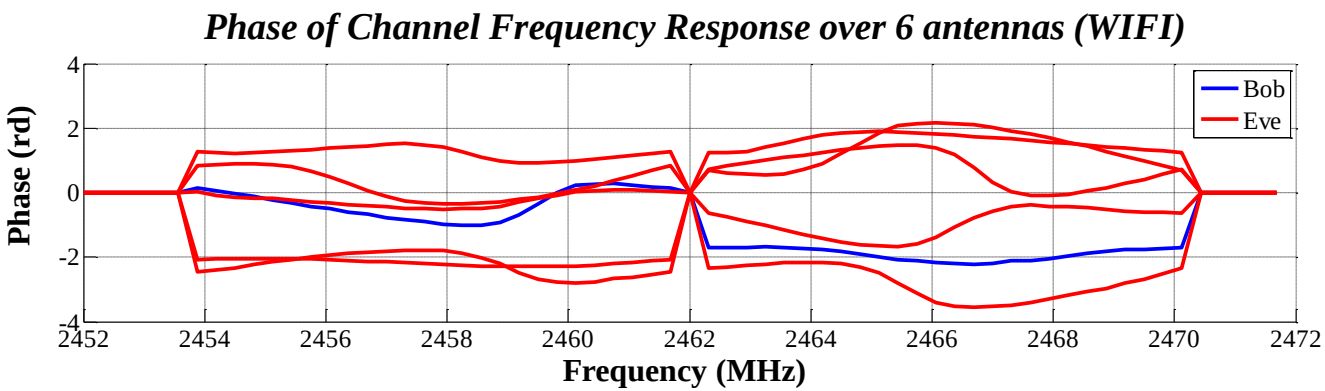
- **RECORDS AND ANALYSIS OF WIFI AND LTE TRAFFIC SIGNALS IN DIFFERENT ENVIRONMENTS**



EXEMPLE OF SPATIAL DIVERSITY IN WIFI

- **Computation of Channel Frequency Response**
  - **Distance between the antenna is λ ≈ 13 cm**





- **High spatial diversity enables computation of good transec keys**
- **Advantages of massive MIMO techniques to generate longer and better keys**

- **COMPUTATION OF SECRET KEYS FROM CHANNEL FREQUENCY RESPONSE**
  - **Two objectives**
    - **Analysis of the mismatch between Alice and Bob**
    - **Analysis of the Bit Error Rate (BER) between Eve and Bob**
  - **Mismatch between Alice and Bob**
    - **Impact of the mismatch between Alice and Bob rigth after quantization**
    - **The BER must be as close as 0 as possible**
  - **BER between Eve and Bob**
    - **Analysis of the evolution of Eve-Bob BER**
    - **Eve-Bob BER must be as close as 0.5 as possible)**
  - **Simulations parameters**
    - **Generated keys were 127 bits long**
    - **Channel Frequency Response are computed from LTE (using PSS) or WiFi (using LTF)**
    - **10^4 simulations were carried out**
    - **BCH(127,92,11) was used in the information reconciliation step**

PERFORMANCE OF SKG

- **Keys are 127 bits long**
- **LTE**
  - **Recording time is 5s**

LTE	Outdoor/Indoor 800MHz	Outdoor/Indoor 2.6GHz	Urban Street 800MHz	Urban Street 2.6GHz
Number of generated keys	72	58	348	306

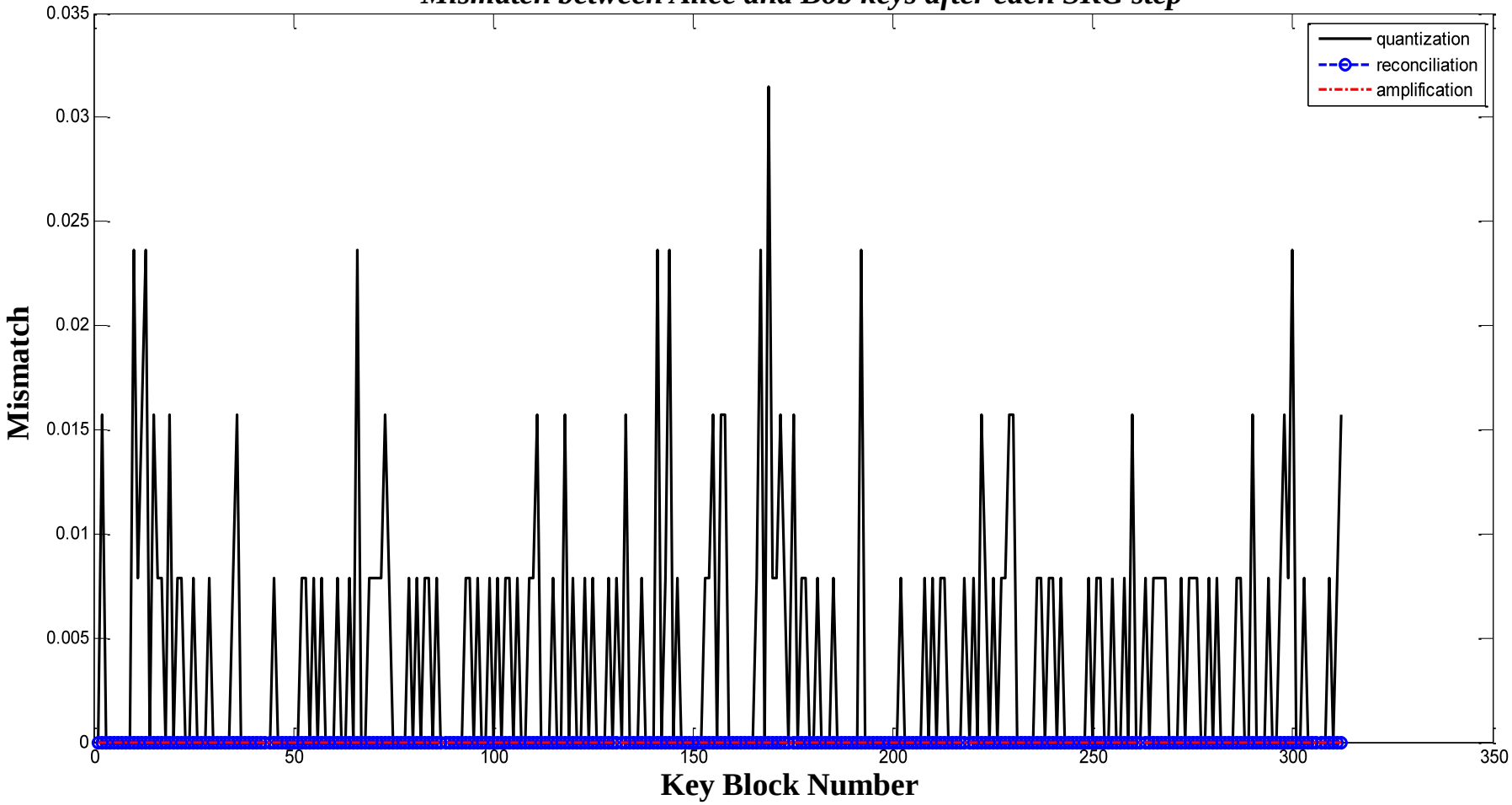
- **WiFi**
  - **Recording time is 2s**

WIFI	LOS	NLOS
Number of generated keys	124	136

- **High number of keys is available within a short amount of time**

- **MISMATCH BETWEEN KEYS COMPUTED BY ALICE AND BOB (SNR_{AB}= 28 dB)**
  - **Mismatch can occur after quantization**
  - **Reconciliation through FEC is nécessary to achieve a perfect equality of the keys**

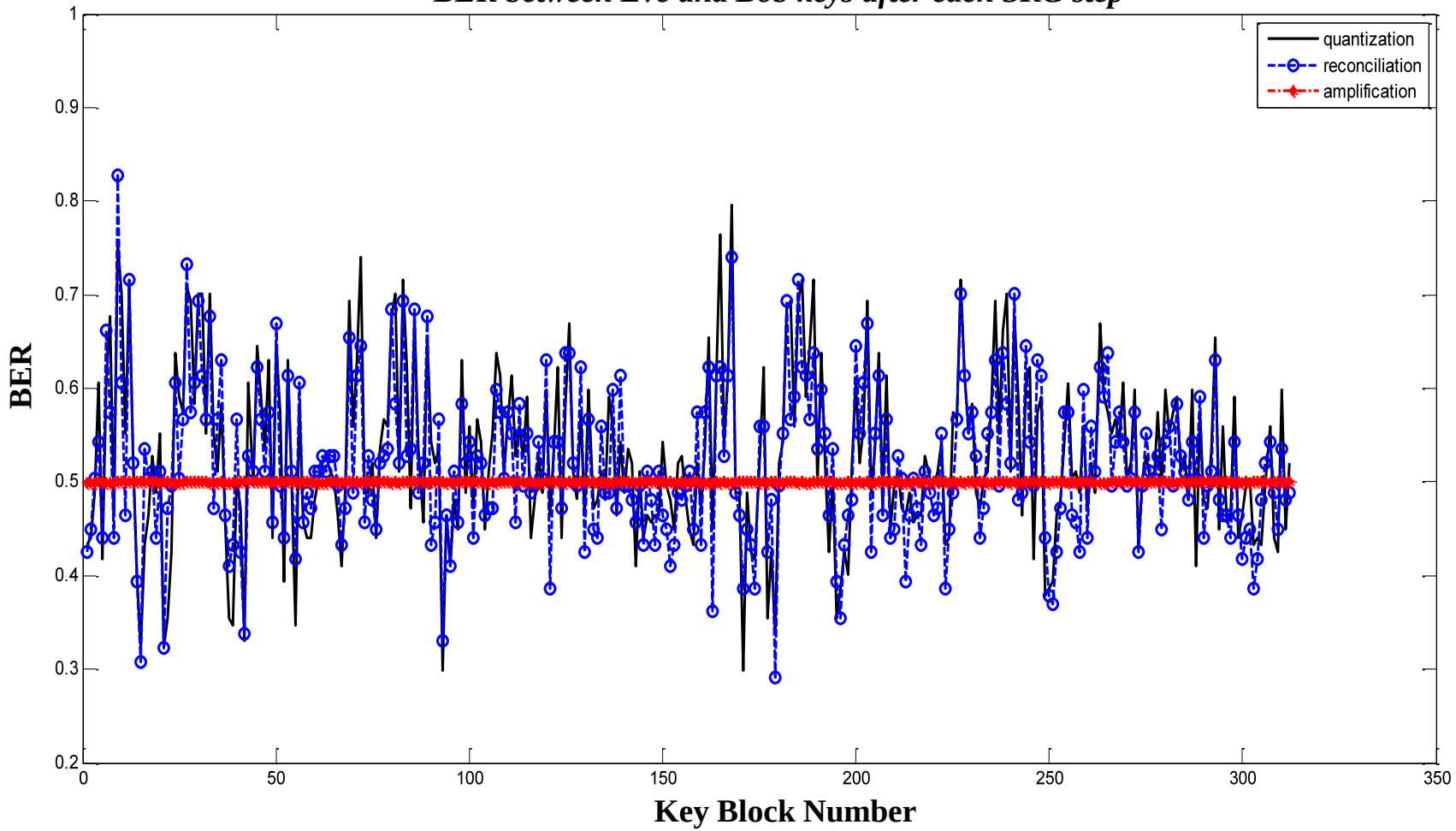
Mismatch between Alice and Bob keys after each SKG step



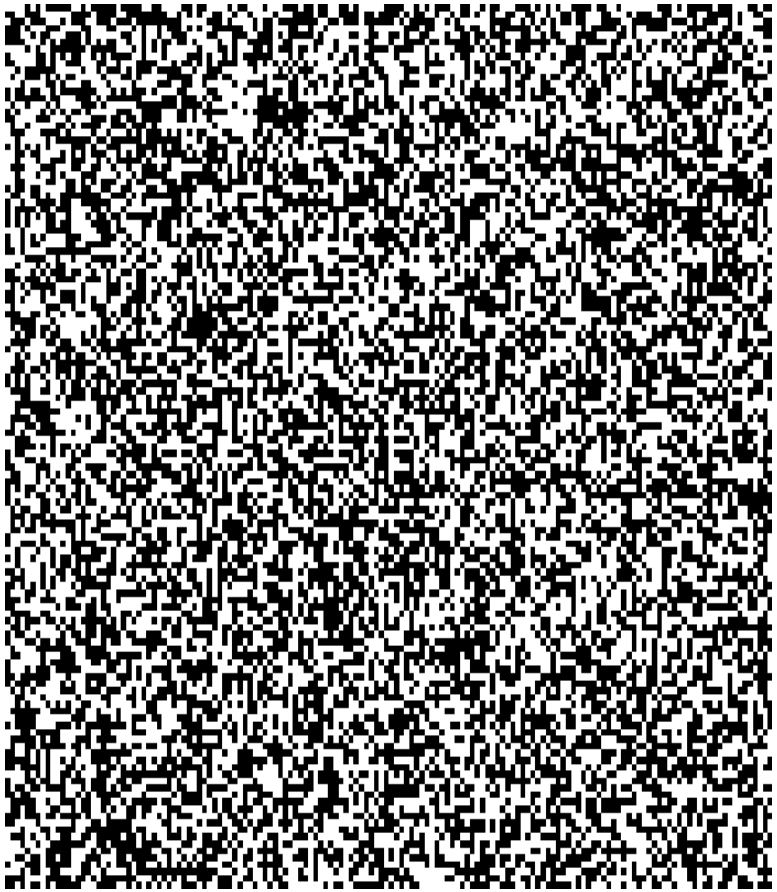
BER BETWEEN EVE AND BOB

- **Amplification secures secret keys by ensuring a BER of 0.5 between Eve and Bob**
- **Eve cannot find Bob's key**

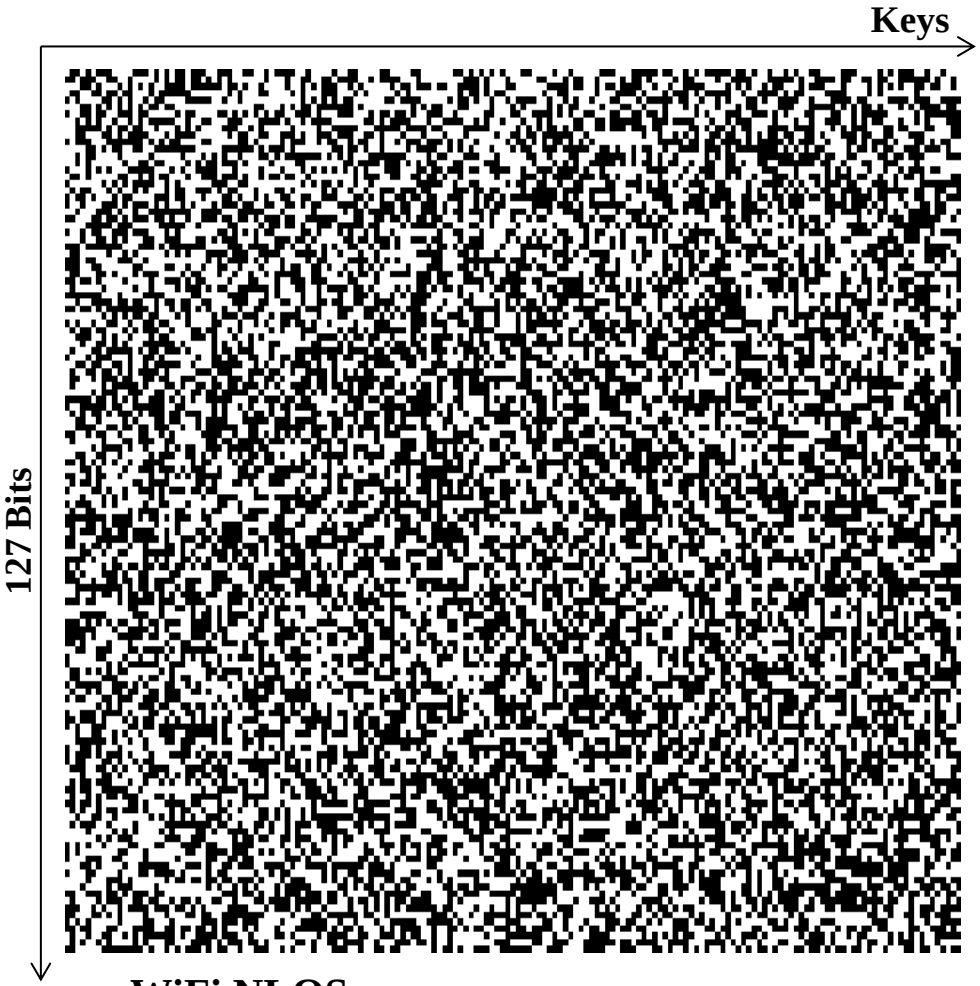
BER between Eve and Bob keys after each SKG step



- **SECRET KEYS OBTAINED IN WIFI**
  - **Keys are generated from Channel Frequency Response measured on the LTF, with reconciliation and amplification steps**

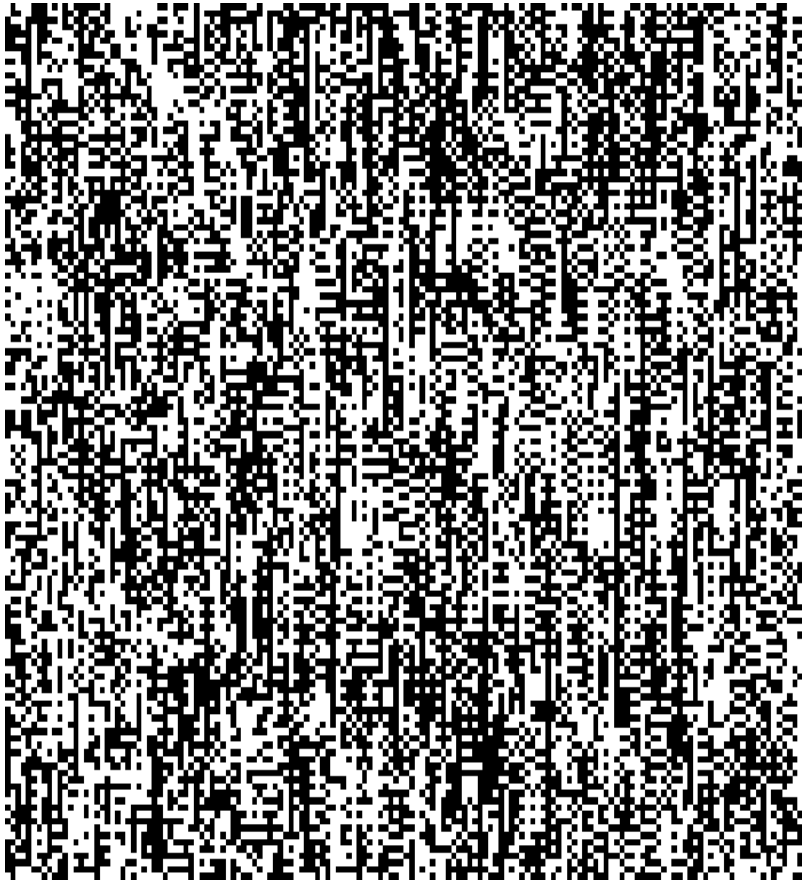


- **WiFi LOS**

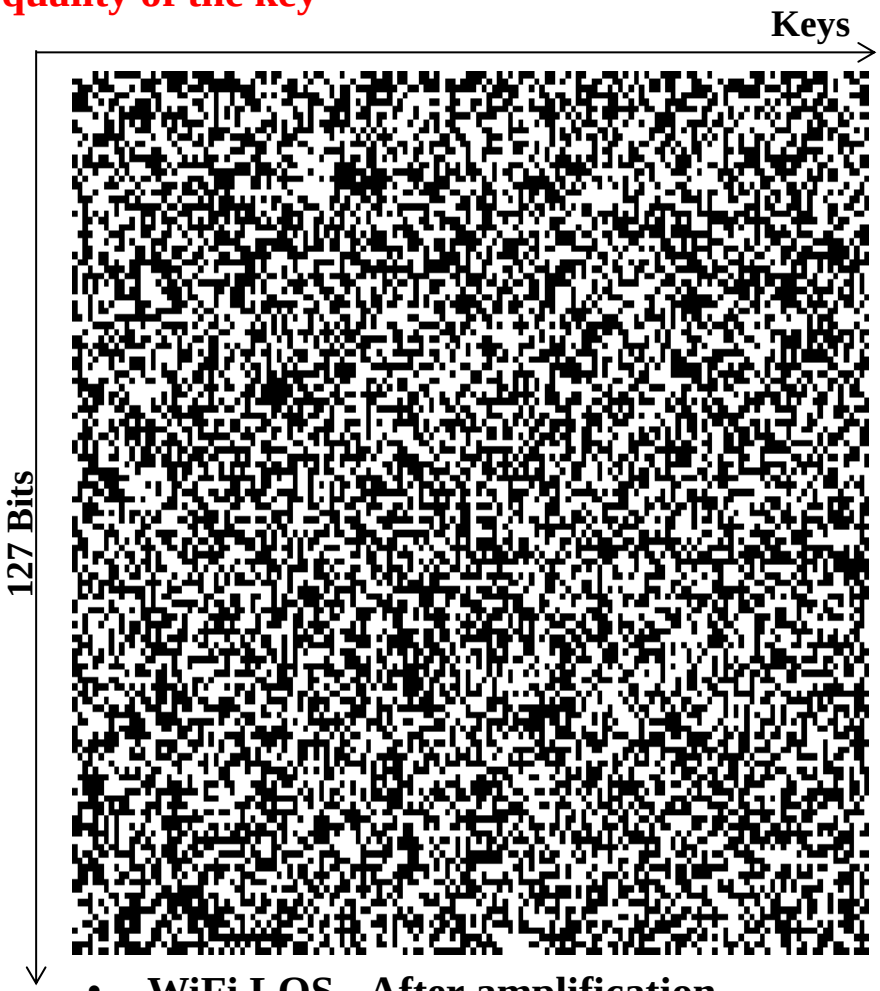


- **WiFi NLOS**

- **SECRET KEYS OBTAINED IN WIFI BEFORE AND AFTER AMPLIFICATION**
  - **Keys are generated from Channel Frequency Response measured on the LTF**
  - **Impact of the amplification step on the quality of the key**

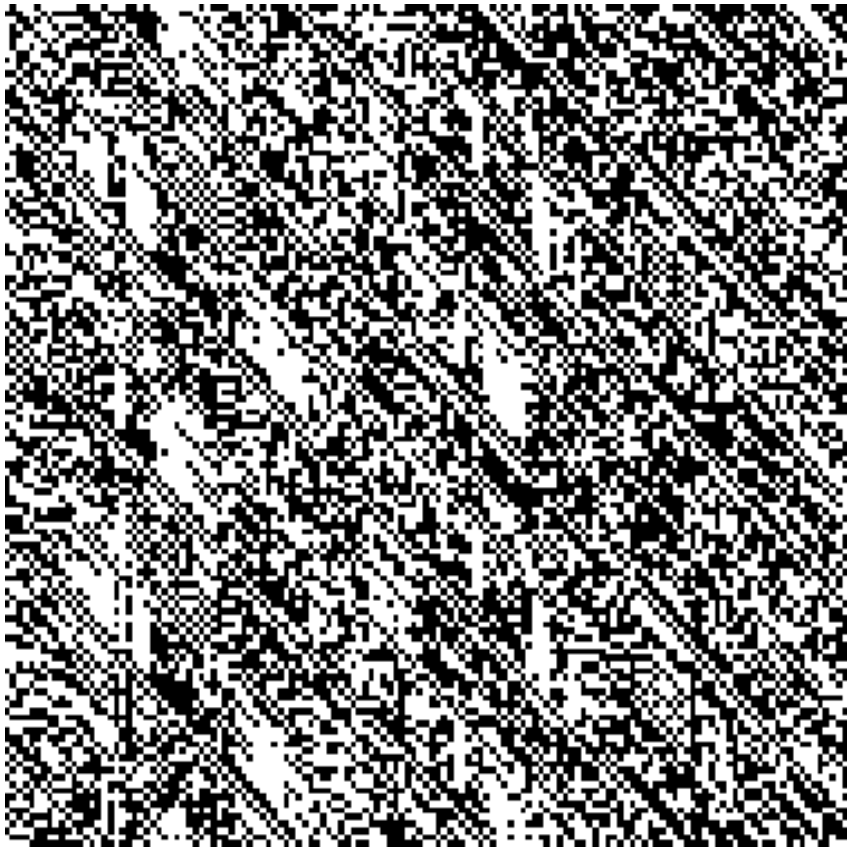


- **WiFi LOS – After quantization only**

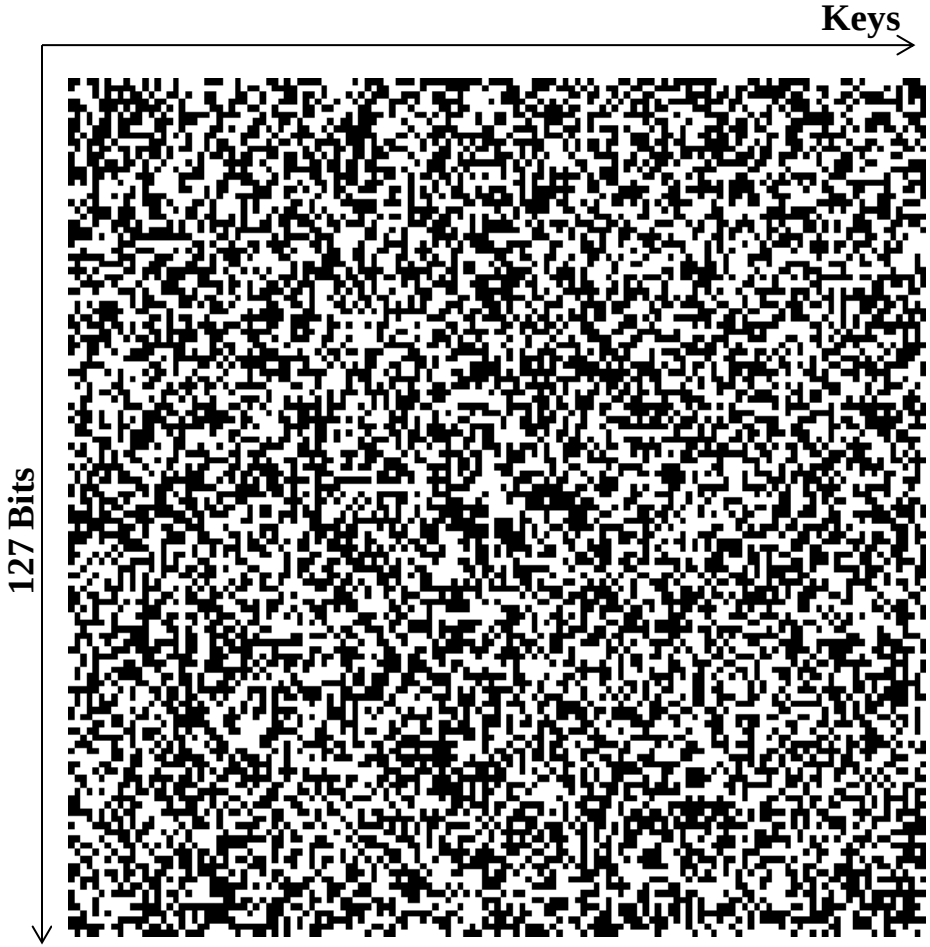


- **WiFi LOS - After amplification**

- **SECRET KEYS OBTAINED IN LTE BEFORE AND AFTER AMPLIFICATION**
  - **Keys are generated from Channel Frequency Response measured on the PSS**
  - **Impact of the amplification step on the quality of the key**



- **LTE Urban street after quantization only**



- **LTE Urban street after amplification**

QUALITY OF THE KEYS – 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

WIFI	LOS	NLOS
Quantization	81%	98%
Amplification	99%	99%

LTE	Outdoor/ Indoor 800MHz	Outdoor/ Indoor 2.6GHz	Urban Street 800MHz	Urban Street 2.6GHz
Quantization	99%	93%	100%	99%
Amplification	99%	100%	100%	100%

- Runs tests

WIFI	LOS	NLOS
Quantization	81%	98%
Amplification	99%	99%

LTE	Outdoor/ Indoor 800MHz	Outdoor/ Indoor 2.6GHz	Urban Street 800MHz	Urban Street 2.6GHz
Quantization	94%	80%	98%	94%
Amplification	100%	99%	99%	100%

IMPLEMENTATION AND USAGE

- **Computation of Channel Frequency Response**
  - Specific calculation with known and simple reference signal – (See Appendix 1)
    - PSS, SSS, CRS in LTE
  - Output of equalizer
- **Quantization of the Channel Frequency Response**
  - CQA algorithm can be computed easily (See Appendix 2)
- **Reconciliation step of Secret Key Generation**
  - Based on existing and standard FEC code (See Appendix 3)
    - Turbo Code, LDPC, BCH
- **Amplification step of Secret Key Generation**
  - Mainly based on logic operations (See Appendix 4)
- **Use of Secret Key**
  - Additional authentication key for the users
  - Additional security protection of the encryption of the signaling and access and traffic data

- **ADVANTAGES OF SECRET KEYS**
  - **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**

- **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 delete 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**

Thank you for your attention

Find more information on our website

www.phylaws-ict.org

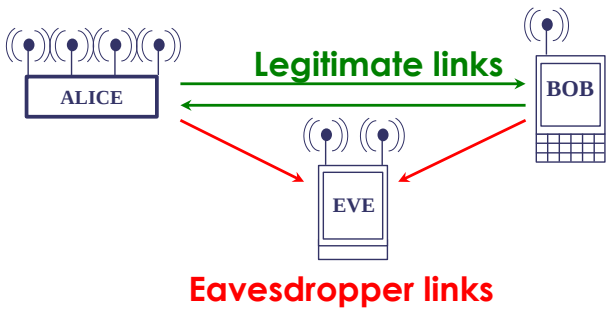
Coordinator Contact: F. Delaveau : francois.delaveau@thalesgroup.com phone : + 33 (0)1 46 13 31 32
Author Contact: R.Moliere : renaud.moliere@thalesgroup.com phone : + 33 (0)1 41 30 33 60

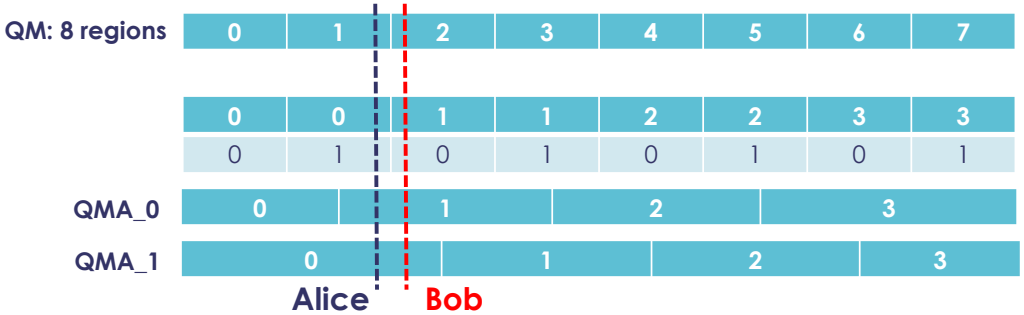
- **PRINCIPLE**
  - Comparison between the received signal (Y) and a reference signal (X)
  - In WiFi, reference signal is the LTF or the PLCP
  - In LTE, reference signal is the PSS, SSS or CRS

- **ESTIMATION IN THE FREQUENCY DOMAIN**
  - Channel Frequency Response (CFR)
  - $\widehat{H}_f(k) = \frac{Y(f_k)}{X(f_k)}$
  - Suitable for OFDM waveform (LTE/WiFi)

- **ESTIMATION IN THE TIME DOMAIN**
  - Channel Impulse Response (CIR)
  - $\widehat{H}_t = \left(X_{n,,L,N}^H X_{n,L,N}\right)^{-1} X_{n,L,N}^H Y_n$
  - Very efficient for low correlated reference signal such as PN sequences
  - Especially suitable for UMTS

8- APPENDIX 2: CHANNEL QUANTIZATION ALGORITHM (CQA)





- ## SKG STRATEGIES
  - **Quantization: Alice and Bob quantize their channel measurements**
  - **Information reconciliation: Alice and Bob exchange messages over a public channel to agree on the same sequence of bits**
  - **Privacy amplification: Alice and Bob suppress the information leaked to Eve**

- ## QUANTIZATION
  - **Channel State Information (CSI) based**
  - **CQA Algorithm (Wallace2010)**

- ## CQA ILLUSTRATION
  - **The total space of observable channels is divided on 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)**

- ## 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

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**

ALGORITHM

- **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: $\widehat{K_a} = \hat{c} \oplus s$**

REFERENCES

- 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

HASH FUNCTION

- We choose a two-universal family of hash functions

DEFINITION

- 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 $\mathcal{G}$

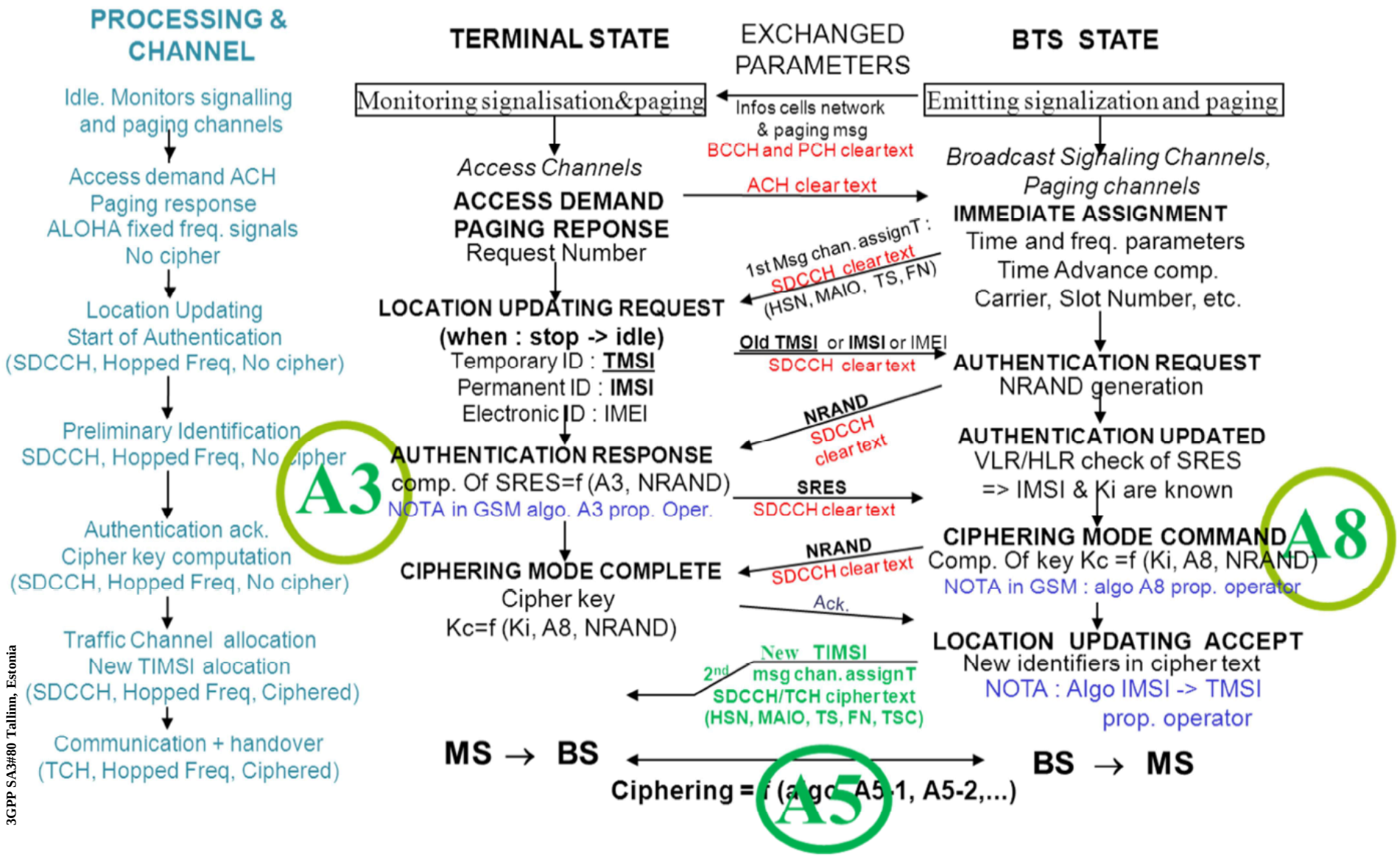
CONSTRUCTION OF A TWO-UNIVERSAL FAMILY OF HASH FUNCTIONS

- 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 $aK \in GF(2^n)$
- Universal2 family of hash function for $1 \leq r \leq n$

REFERENCE

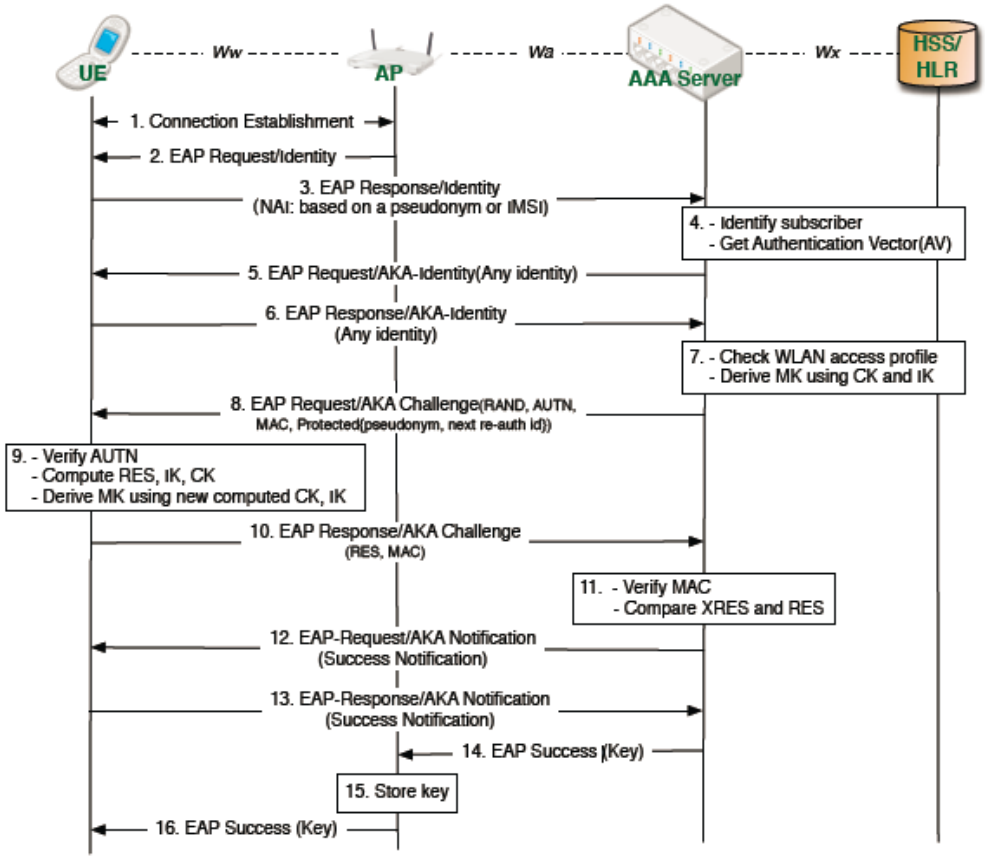
- Bennett, C.H.; Brassard, G.; Crepeau, C.; Maurer, U.M., "Generalized privacy amplification," Information Theory, IEEE Transactions on , vol.41, no.6, pp.1915,1923, Nov 1995

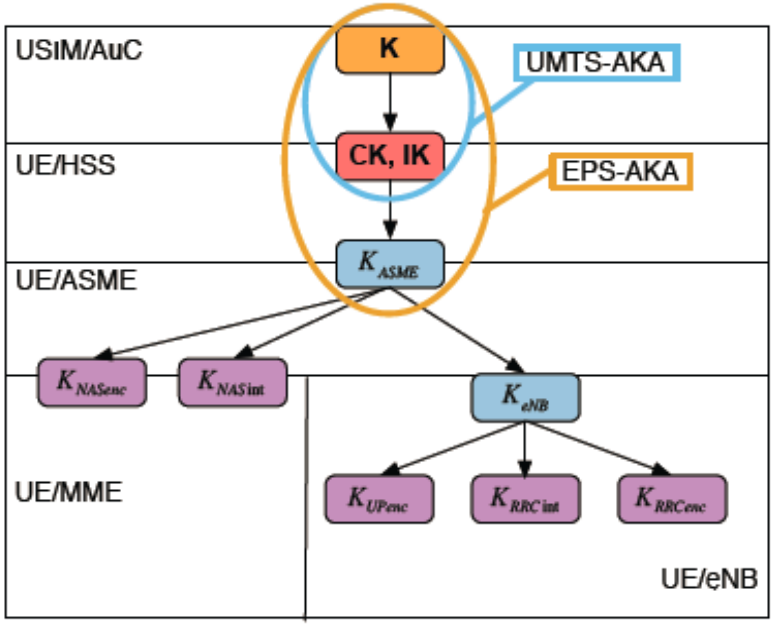
8- APPENDIX 5: AUTHENTICATION PROTOCOL IN GSM



- **NB: A5-1/2, A3 A8 are cracked since end 1990s**

8- APPENDIX 6: EAP- AKA PROTOCOL OF 3GPP





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 are exchanged in clear text without Transec protection**
  - **Passive Eve can decode**
  - **Active Eve can jam, spoof, replay**

- **When Eve gets the key K she gets everything by passive monitoring only**

REFERENCE

- *Ref: Hyeran Mun, Kyusuk Han and Kwangjo Kim1-4244-2589-1/09/ $20.00 2009 IEEE, "3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement based on EAP-AKA »*

9- ACRONYMS

AN	Artificial Noise
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
GSM	Global System for Mobile communications
IMSI	International Mobile Subscriber Identity
LDPC	Low Density Parity Check
LOS	Line Of Sight
LTE	Long Term Evolution
LTF	Long Training Field
MAC	Media Access Control
MIMO	Multiple Input Multiple Output
NIST	National Instrument of Standards and Technology
NETSEC	Network Transmission Security
NLOS	Non Line Of Sight
PHYSEC	Physical Layer Security
PSS	Primary Synchronization Sequence
RAT	Radio Access Technology
SIM	Subscriber Identity Module
SKG	Secret Key Generation
SNR	Signal to Noise Ratio
SS7	Signaling System No.7
SSS	Secondary Synchronization Sequence
TDD	Time Division Duplex
TMSI	Temporary Mobile Subscriber Identity
TRANSEC	Transmission Security
UMTS	Universal Mobile Telecommunications System
VIP	Very Important People