Analysis of Secret Key Robustness in Indoor Radio Channel Measurements

Taghrid Mazloum, Francesco Mani, and Alain Sibille

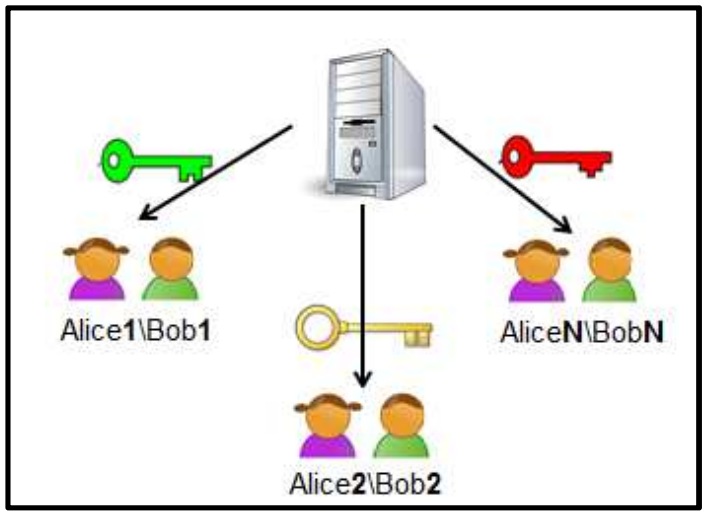
Communications & Electronic Department,
Telecom ParisTech/LTCI,
Paris, France

Outline

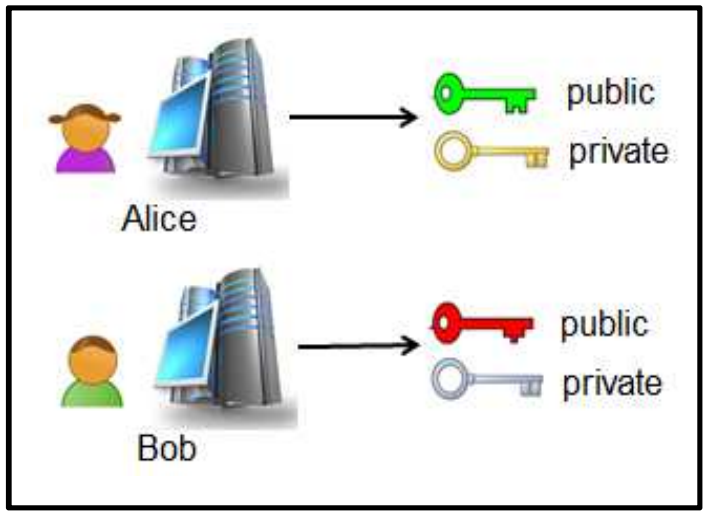
- Introduction
- Objectives
- Measurements description
- Simplified channel model
- Channel quantization
- Results: Reliability and vulnerability performance assessments
- Conclusion

Introduction

- **Conventional cryptosystems issues.**



Symmetric key generation and distribution



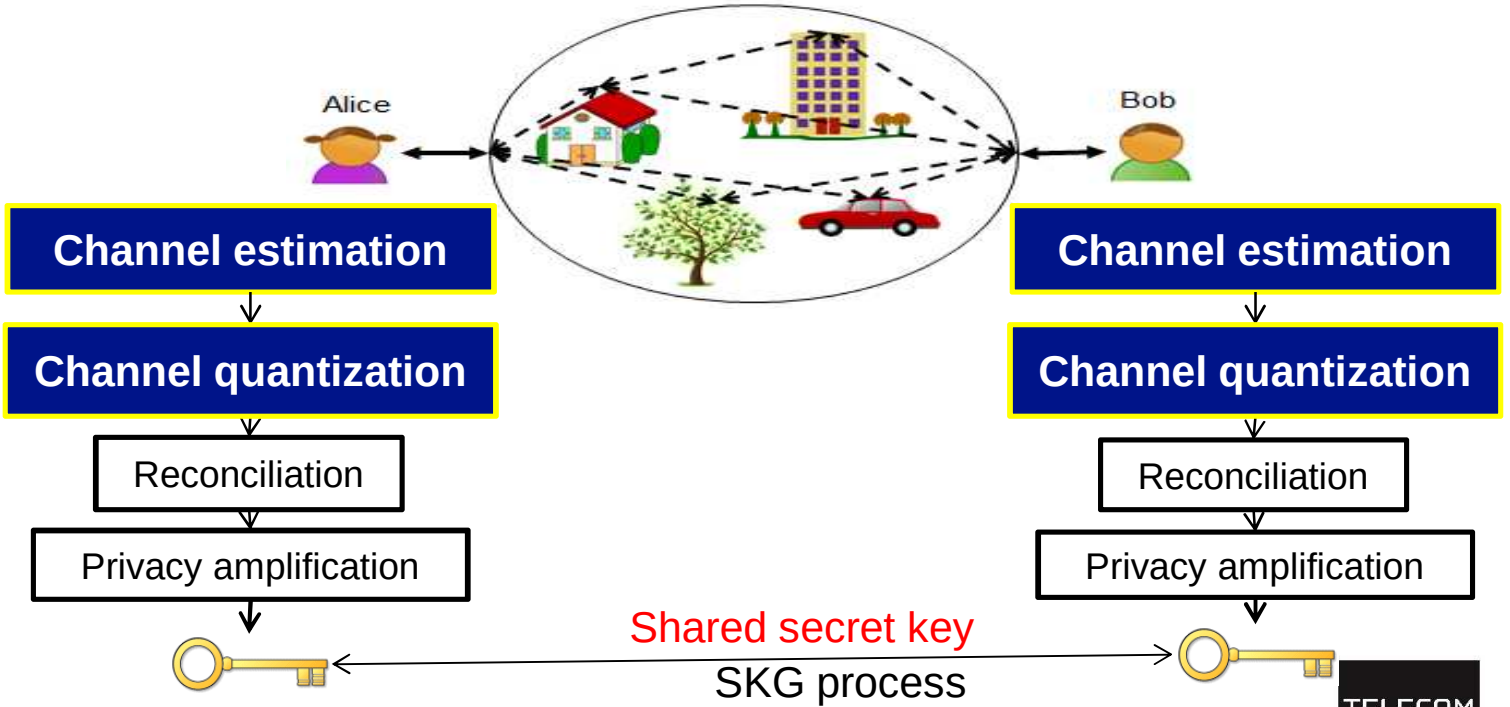
Computational cost of asymmetric cryptosystems

Computation-based security

Introduction

- **Information-theoretic physical layer security:**
  - Secret key generation (SKG) from the reciprocal fading channel.
    - Reciprocity.
    - Unpredictable fast fading character of multipaths signals.
    - Confidentiality through spatial channel decorrelation.

Eve: Exploiting information to break security



Objectives

- **The impact of true radio channel features on SKG performance.**

- **The SKG performance analysis of a simplified channel model in comparison with the measured channels.**

- **NB** and **WB** targeting OFDM systems.
- **LOS/NLOS** propagation conditions.
- Channel estimation error and **noise**.

Relation?

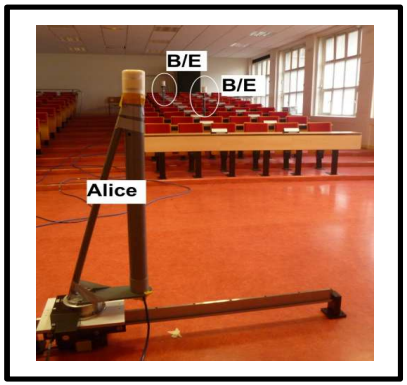
- **Reliability** between Alice and Bob.
- **Vulnerability** with respect to Eve.

Measurements description

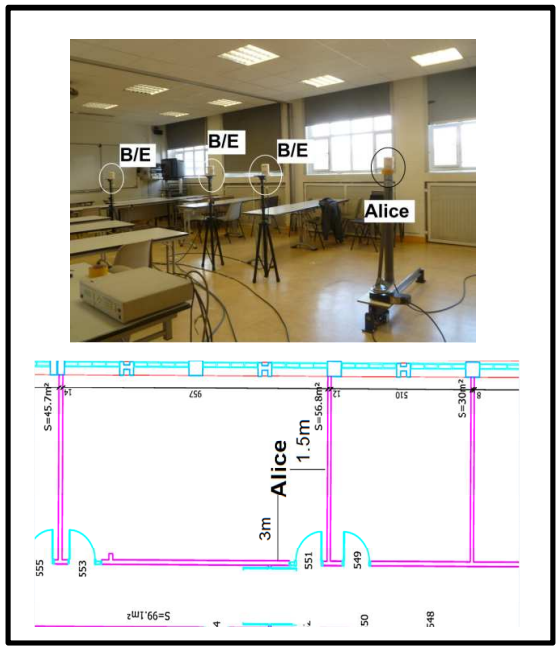
- **4-port VNA (1 port for Alice and 3 ports for Bob/Eve).**
- **Alice spatially scanned over 11x11 square grid with ~λ\2 step.**
  - Statistically independent channel coefficients.
- **LOS/NLOS propagation conditions.**
- **Performance analysis centered on 5.4 GHz.**

Start frequency	2 GHz
Stop frequency	6 GHz
Tx power	10 dBm
Frequency points	1601
IF bandwidth	5 KHz

VNA setup parameters



Auditorium (42 positions)



Classrooms (51 positions)

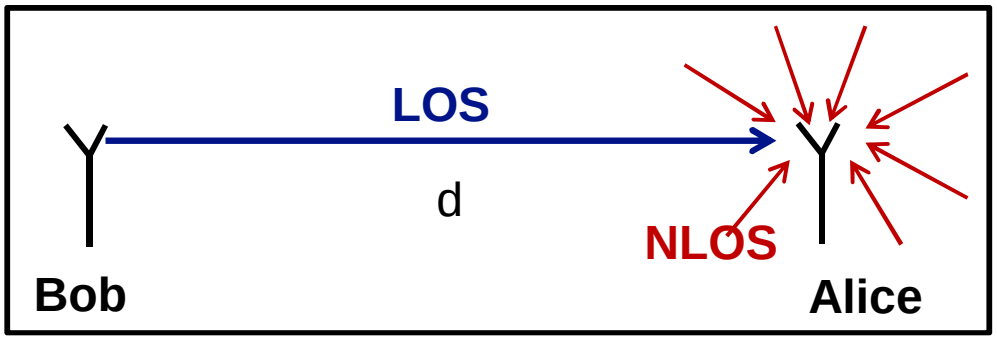
Simplified channel model

- **Simplified channel model for LOS case:**

Multipath channel coefficient = **LOS path** + **NLOS paths**

$$h_{los} = \frac{S}{d}\exp\{j\frac{2\pi}{\lambda}d\} \qquad \sim CN(0,\sigma^2)$$

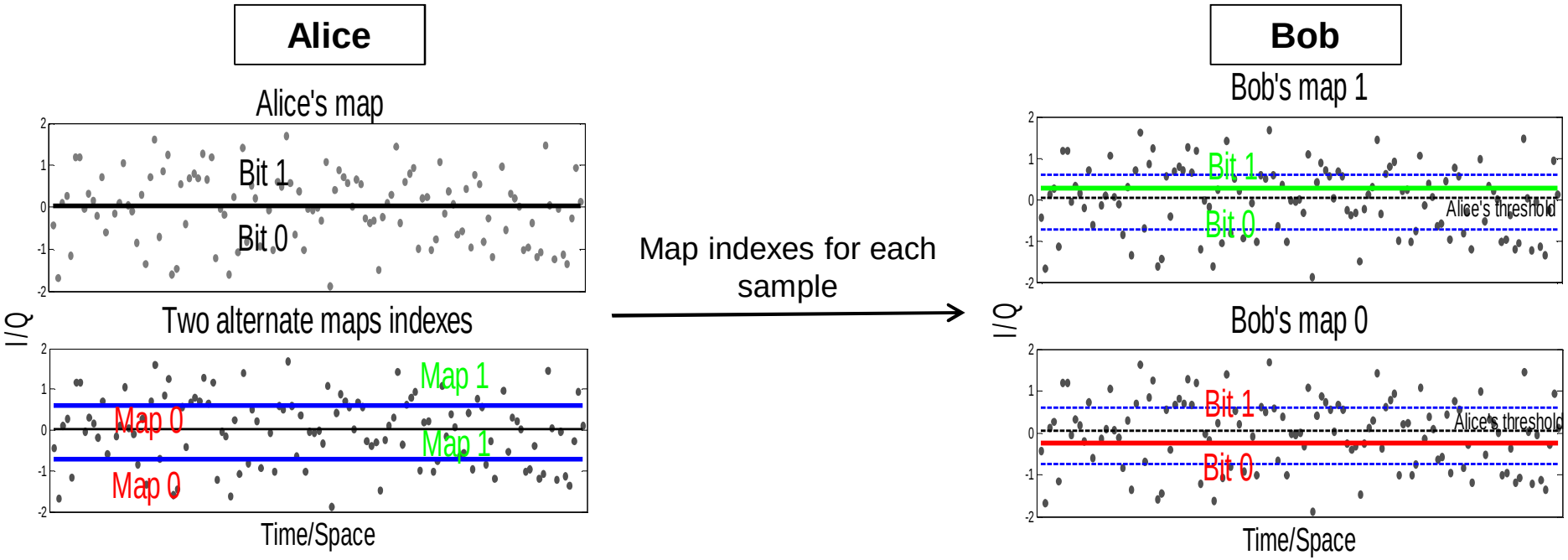
  - Rician factor: $K = \frac{E\{|h_{los}|^2\}}{\sigma^2}$.



- **Simplified channel model for NLOS case:**
  - $\sim CN(0,\sigma^2)$

Channel quantization

- **Quantizing complex channel coefficients into M quantization regions.**
- **Channel Quantization Alternating (CQA)** [1] **algorithm:**
  - Usage of alternate maps instead of symbol rejection.
  - Improvement of Alice-Bob bit agreement ratio.



[1] J. Wallace and R. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis", *IEEE Trans. Inf. Forensics and Security*, Sep. 2010.

Results: Reliability and Vulnerability performance assessment

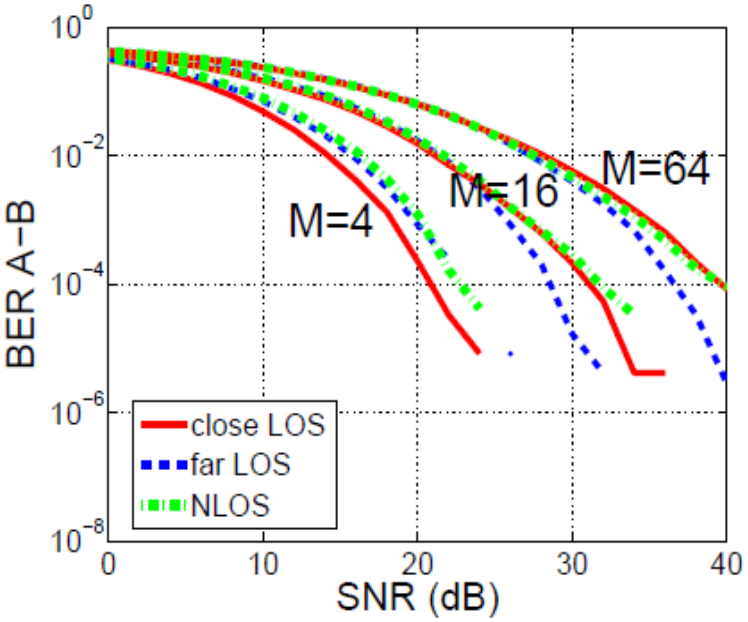
- **Reliability performance assessment:**
  - Secret key agreement between Alice and Bob.
  - Key randomness.

- **Vulnerability performance assessment.**
  - Bit error rate between keys extracted by Alice/Bob and Eve.

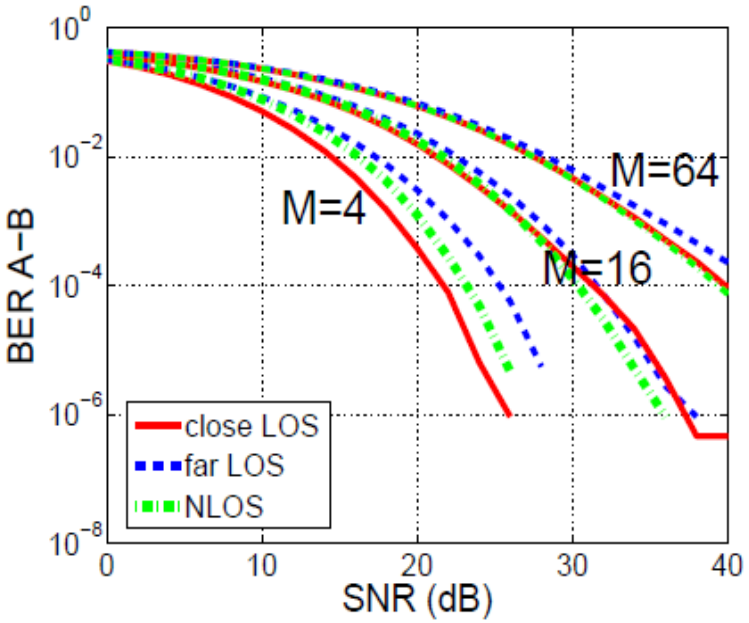
- **VNA: high dynamic range conditions.**
  - The addition of artificial noise $\sim \boldsymbol{CN}(\mathbf{0}, \boldsymbol{\sigma^2})$ such as $\boldsymbol{SNR} = \frac{\boldsymbol{E}\{|\boldsymbol{h}|^2\}}{\boldsymbol{\sigma^2}}$.

Secret key agreement between Alice and Bob

- **Bit error rate between keys extracted by both Alice and Bob (BER A-B).**



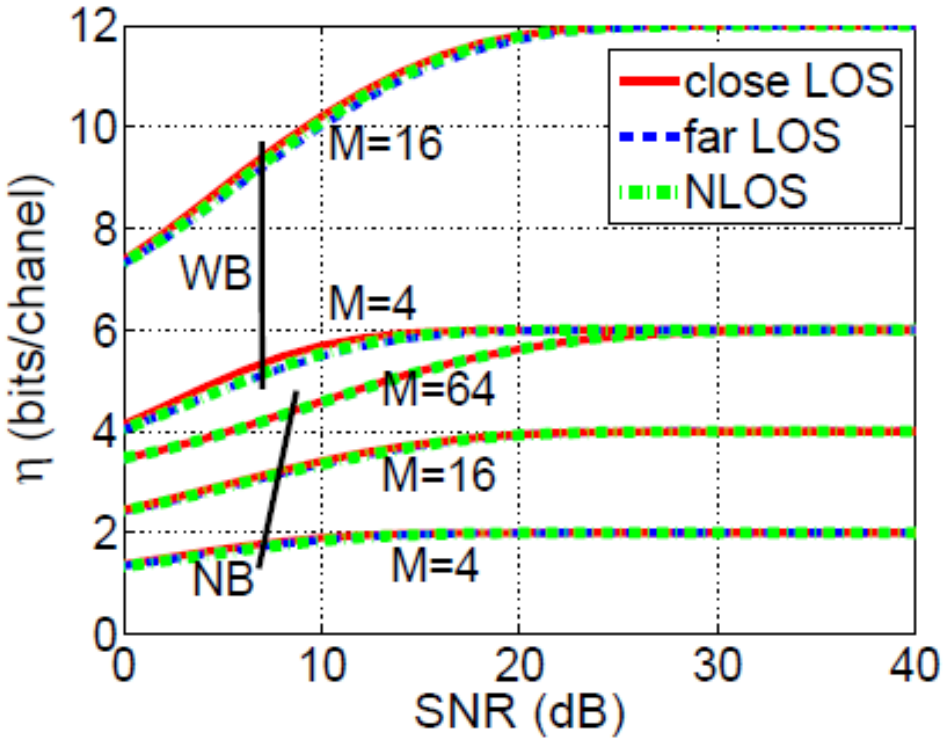
NB channels



WB channels
BW = 80MHz & Δf = 10MHz

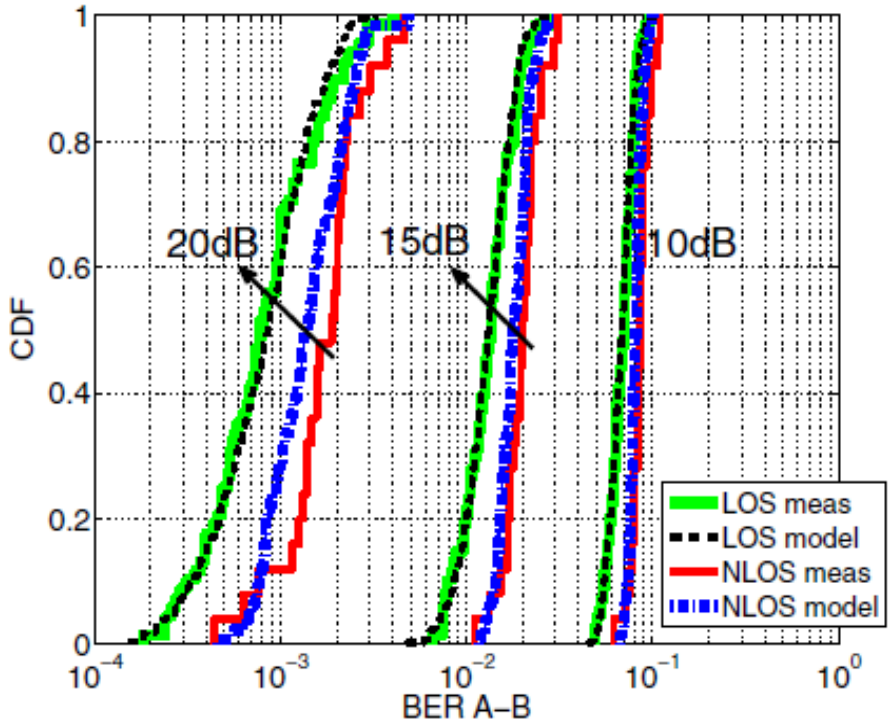
Secret key agreement between Alice and Bob

- **Secret key rate: Number of shared key bits between Alice and Bob per channel observation.**
  - $\eta = (1 - BER)N_f \log_2 M$



Secret key agreement between Alice and Bob

- **BER Alice-Bob**
  - Model vs. measurements
  - LOS vs. NLOS.
  - NB channels.



- A good fit for LOS.
- An imperfect fit for NLOS due to the limited number of significant paths.
- Less Alice-Bob BER for LOS cases.

Randomness of the generated key

- **Key randomness behavior at high SNR**
  - National Institute of standards and technologies (NIST) statistical test suite.
- **Randomness is considered if the proportion of key sequences passing a given test is very high.**

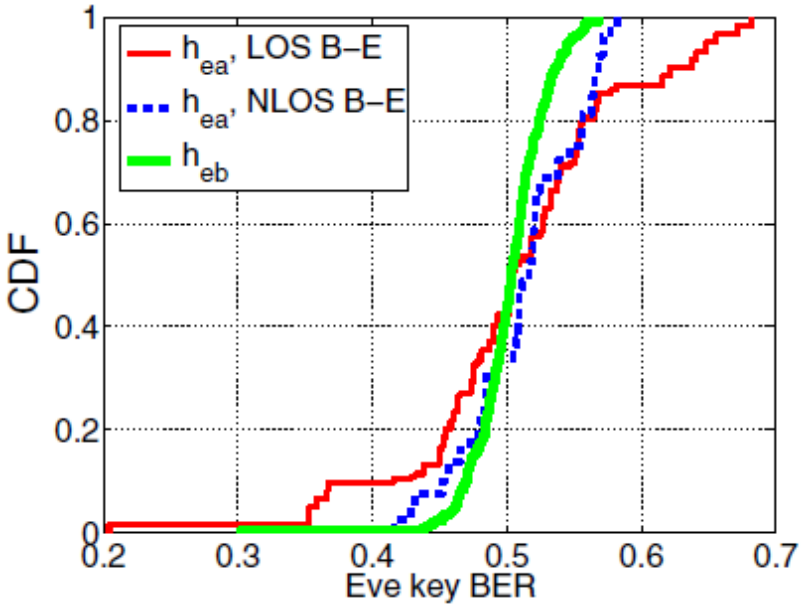
	LOS (68 sequences)			NLOS (25 sequences)		
	NB	BW=80MHz Δf=2.5MHz	BW=80MHz Δf=40MHz	NB	BW=80MHz Δf=2.5MHz	BW=80MHz Δf=40MHz
Bit frequency	1	1	1	1	1	1
Block frequency	0.9	0.57	0.93	0.92	0.64	0.92
Runs	0.87	0.07	0.68	1	0	0.72
Approximate entropy	0.9	0	0.41	1	0	0.48

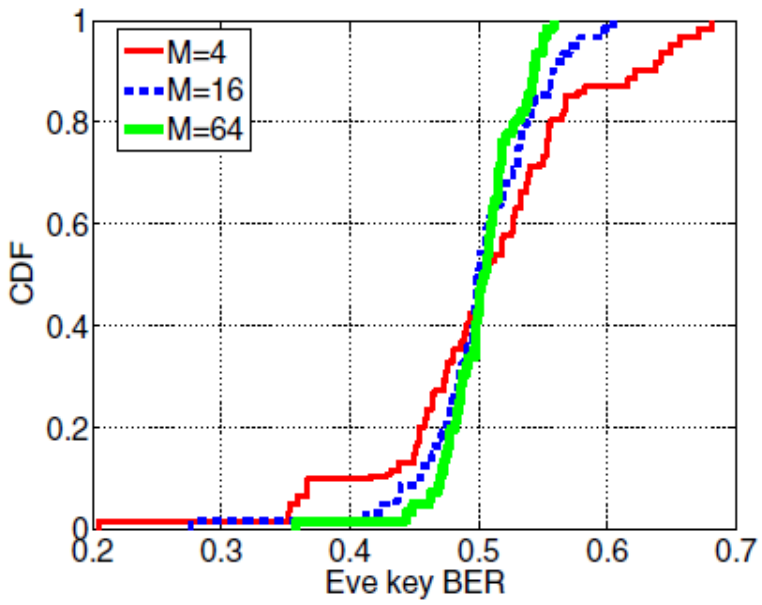
The worst performance: frequency step less than the coherence bandwidth

The best performance

Security performance with respect to Eve

- **BER between keys extracted by Alice/Bob and Eve.**
  - NB channels at SNR=15 dB.
  - Eavesdropping when either the Tx is Alice (h_{ea}) or Bob (h_{eb}).





- The worst BER for h_{eb}.
- Information leakage to Eve for Bob-Eve LOS.
- Less vulnerability for larger M.

Conclusion

- **Analysis of the security performance according to true radio channel characteristics:**
  - Advantage of Alice-Bob LOS for the agreement step between Alice and Bob.
  - Disadvantage of Bob-Eve LOS due to the information revealed to Eve.
  - Robust secure key bits provided by WB channels if the sub-carriers are enough separated.

- **Several major features of the SKG performance are reproduced by the simplified channel model.**

TELECOM ParisTech

Institut Mines-Télécom

Thank you for your attention

This work has been partly funding by the European Union Seventh Framework Programme *FP7/2007-2013* under *grant agreement* n°317562.