Context aware 6G security: The role of the physical layer

Arsenia Chorti

ETIS UMR8051, CYU, ENSEA, CNRS, FR and Barkhausen Institut gGmbH, DE

2022 Joint IEEE SPS and EURASIP Summer School on Defining 6G

Talk outline

1. Key ideas in cryptography
2. What changes in 6G, trust and trustworthiness
3. The role of physical layer security in future generations

Fundamentals security concepts

Jean Luc Godard: *All you need to make a film is a girl and gun*

Crypto expert: *all you need to do cryptography is a XOR and a key...*

Info theorist: *all you need to do information theory is a log and a limit*

Security goals

What do we want to achieve?

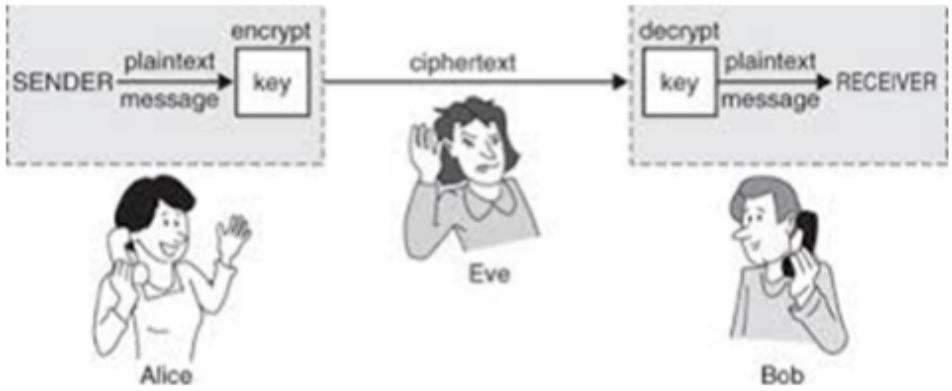
- What is the system model?
- What are the assumptions?
- What are the desirable properties?

What do we aim to achieve?

- Data confidentiality; eavesdropping (passive) attacks
- Data integrity; active attacks
- User / device authentication (i.e., access control); active attacks
- Availability; active attacks

What is the System Model?

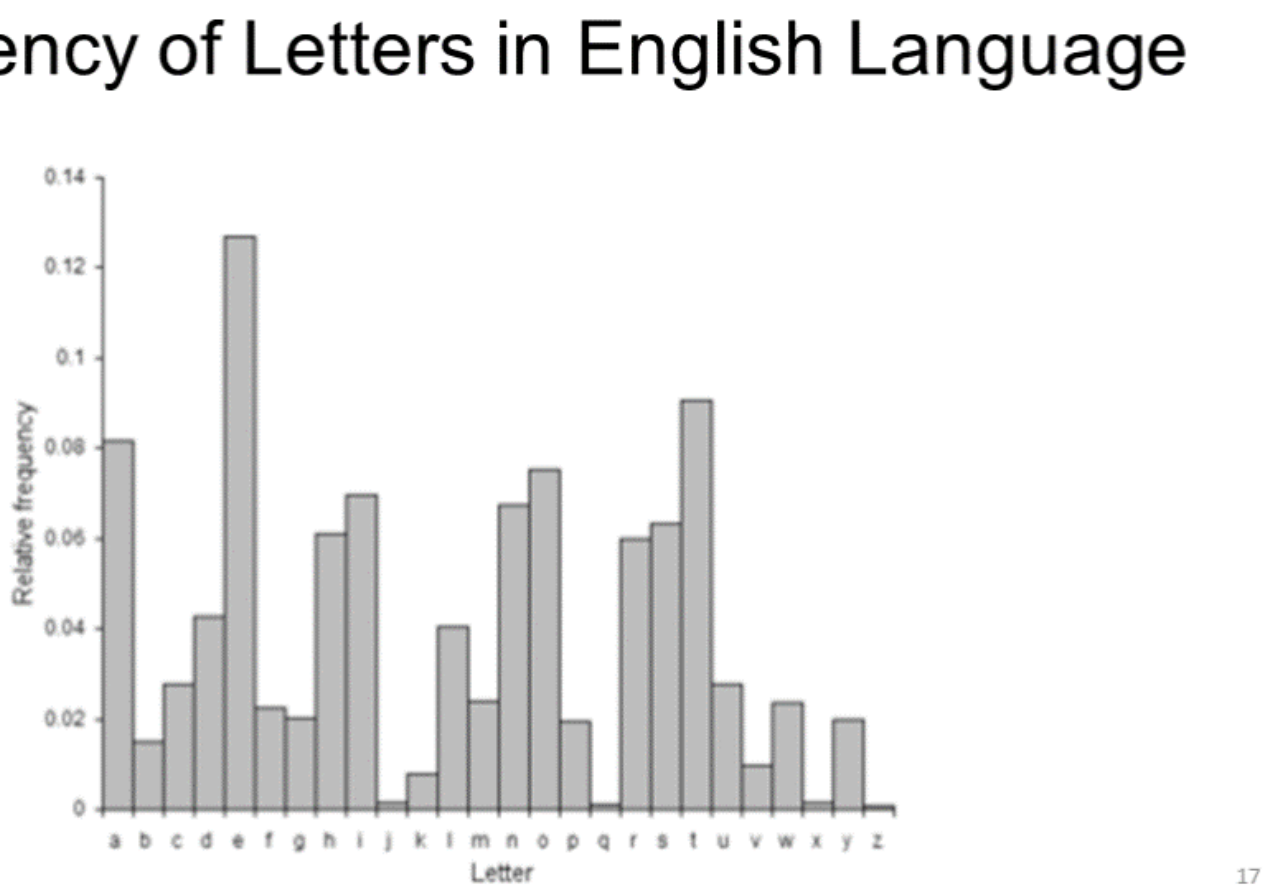
- Basic model
- Extended model



Old example of symmetric key cipher

Substitution cipher: each letter is moved k positions to right (or left) in the alphabet

Brute force attack infeasible!



17

Perfect secrecy (Shannon 1949)

One time pad (OTP)

A cipher E, D over $\mathcal{M}, \mathcal{K}, \mathcal{C}$ has perfect secrecy if the entropy of the secret key is at least equal to the entropy of the message

$$c = k \oplus m, \;\; c \in \mathcal{C}, k \in \mathcal{K}, m \in \mathcal{M}$$

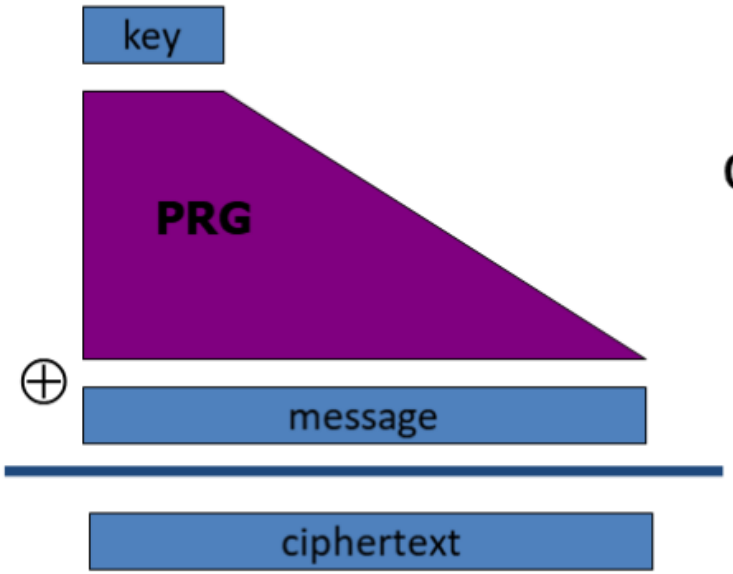
This means that the length of the key should be at least equal to the length of the message

The bad news: OTP is impractical

Stream Ciphers: making OTP practical

Problem: OTP key is as long the message

Solution: Pseudo random key -- stream ciphers



$c \leftarrow \text{PRG}(k) \oplus m$

credit: Dan Boneh, Cryptography 1

Semantically secure PRG

Indistinguishability

The ensemble $\{G(U_n)\}_{n\in N}$ is pseudorandom, iff for any probabilistic polynomial-time algorithm A, for any positive polynomial p and for all sufficiently large n,

$$\left|Pr(A(G(U_n)) = 1) - Pr(A(U_{l(n)}) = 1)\right| < \frac{1}{p(n)} \qquad (1)$$

Next bit predictors

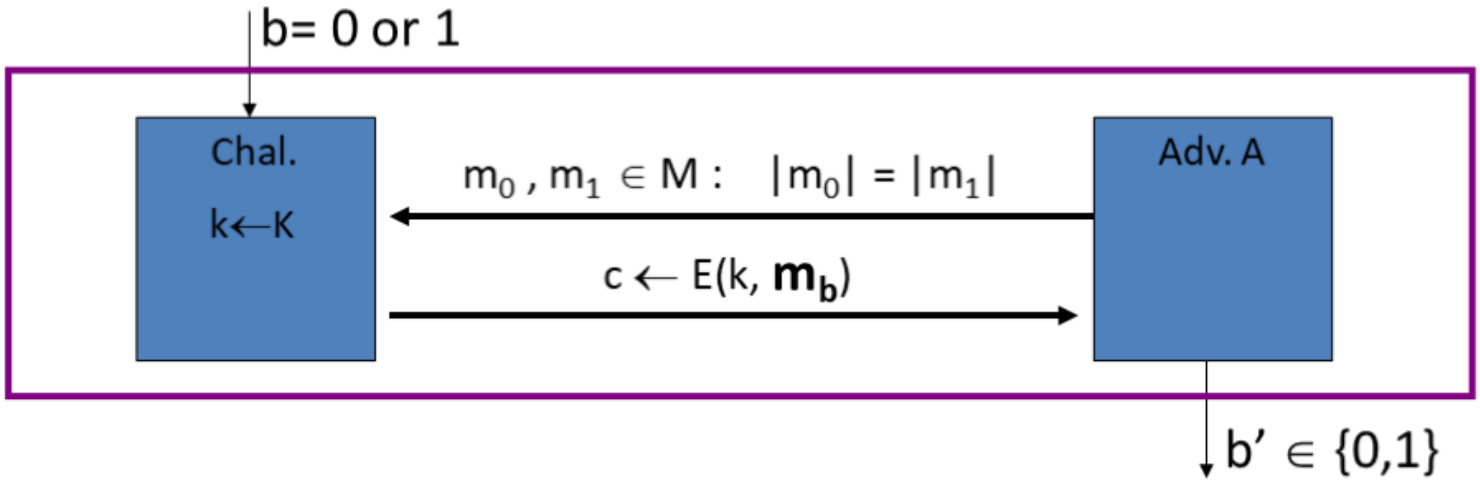
We say that $G : \mathcal{K}\{0,1\}^n$ is predictable if $\exists$ an efficient algorithm A and an index i s.t.

$$Pr\left[A\left(G(k)|_{1,\ldots,i}\right) = G(k)|_{i+1}\right] > \frac{1}{2} + \epsilon$$

for non-neglible $\epsilon > \frac{1}{p(n)}$

Semantic Security (one-time key)

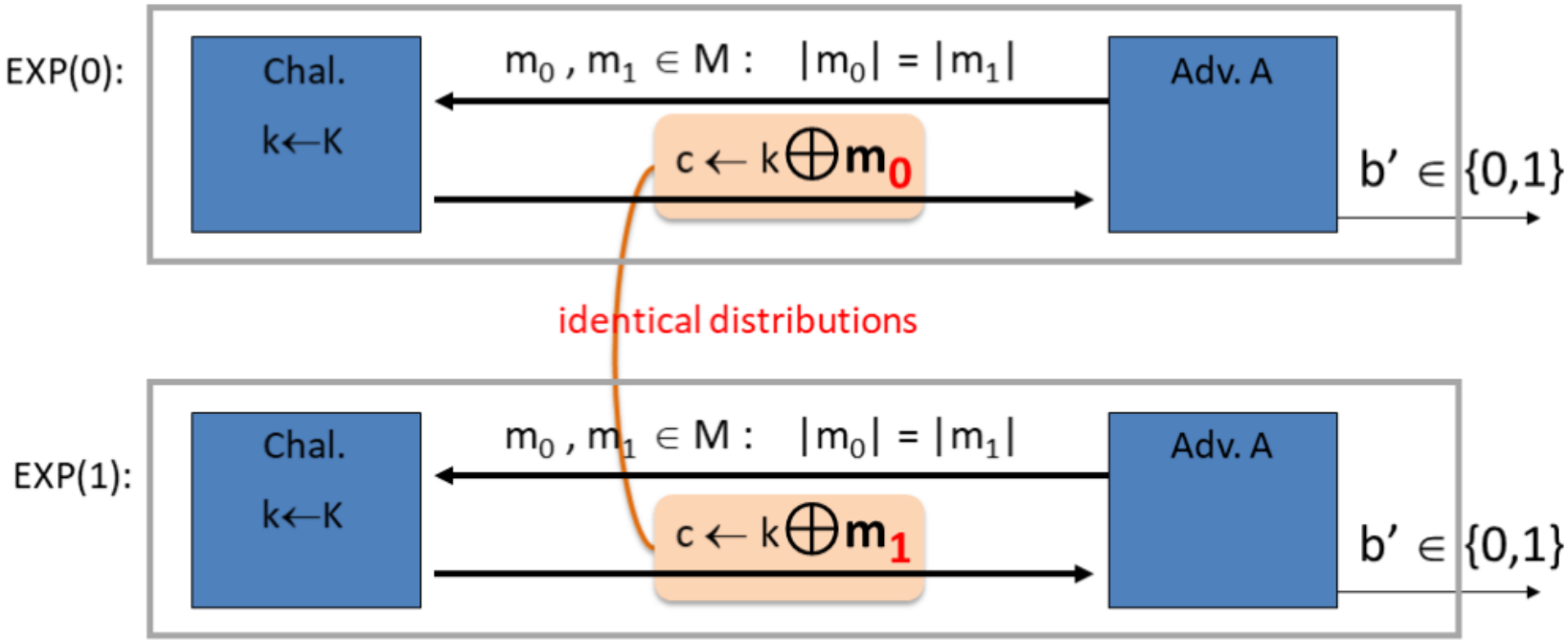
Define two experiments EXP(0) and EXP(1) as that correspond to messages m_0 and m_1



If there exists at least one experiment that would allow the adversary to predict which experiment was performed with non negligible probability then we don't have semantic security

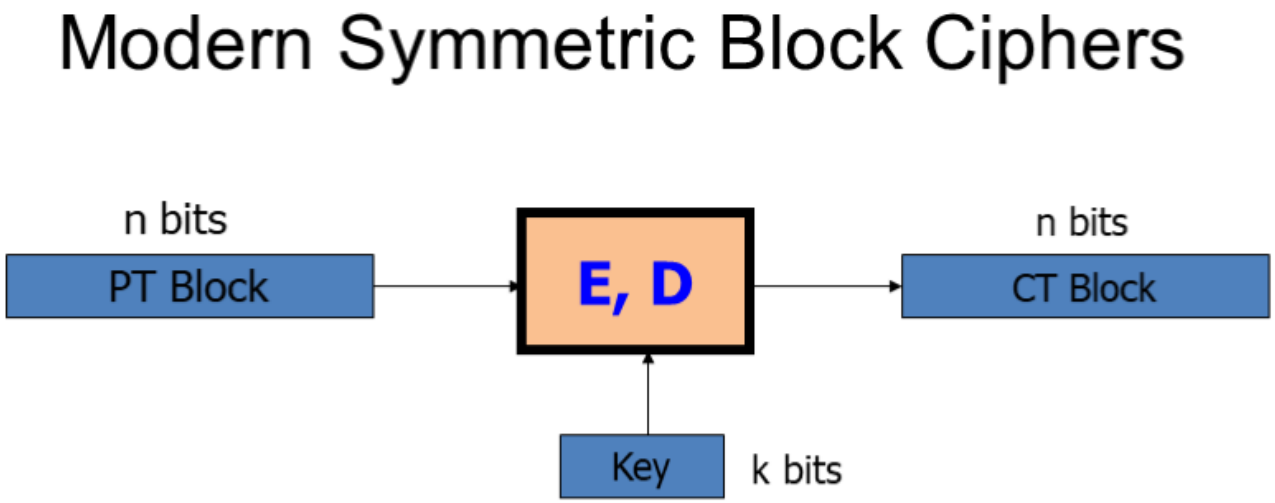
credit: Dan Boneh, Cryptography 1

OTP is semantically secure



credit: Dan Boneh, Cryptography 1

Pseudorandom permutations and functions



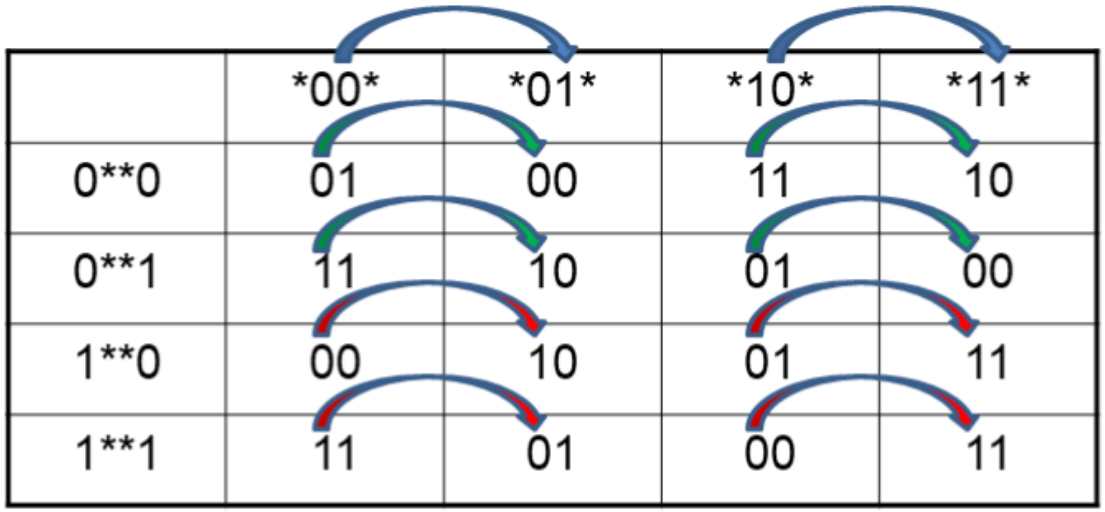
- Feistel Networks : DES, 3DES, CLEFIA (lightweight scheme)
- Substitution-permutation Networks: AES: n=128 bits, k = 128, 192, 256

credit: Dan Boneh, Cryptography 1

Creating confusion using S-boxes

- S-box or a substitution box is a function producing a highly non-linear substitution of bits in a binary array
- S-boxes are normally represented as look-up tables

S-box: Non-linearity

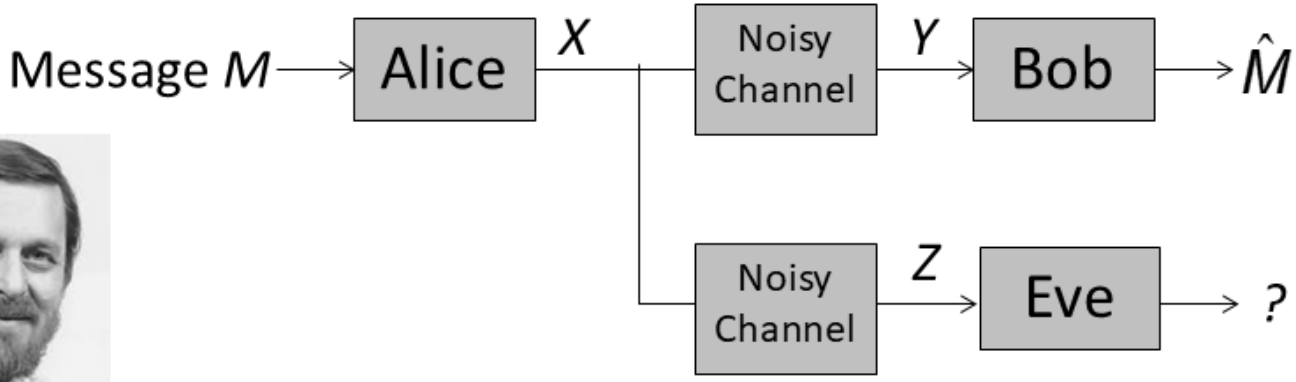


	00	*01*	*10*	*11*
0**0	01	00	11	10
0**1	11	10	01	00
1**0	00	10	01	11
1**1	11	01	00	11

For example, does the first bit of the output depend on the third bit of the input?
Yes in a half of the cases, No in the other half of the cases

Information Theoretic Security:
Wyner's Model

"The Wiretap Channel"



- Tradeoff: reliable rate R to Bob vs. the equivocation $H(M|Z)$ at Eve
- Secrecy capacity = maximum R such that $R = H(M|Z)$
- Wyner (1975): Secrecy capacity > 0 iff. Z is degraded relative to Y

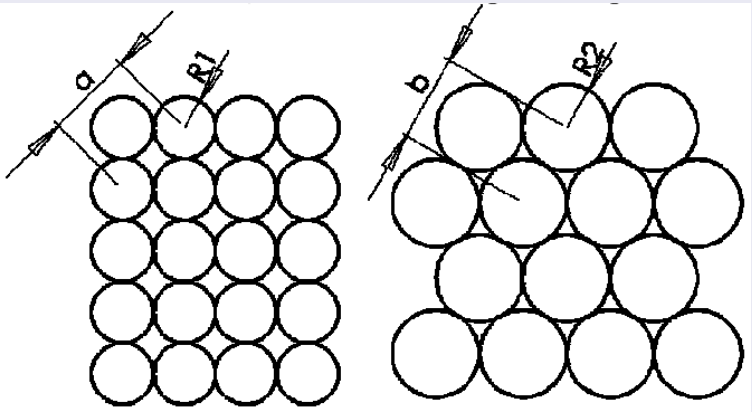
Physical layer security (PLS)

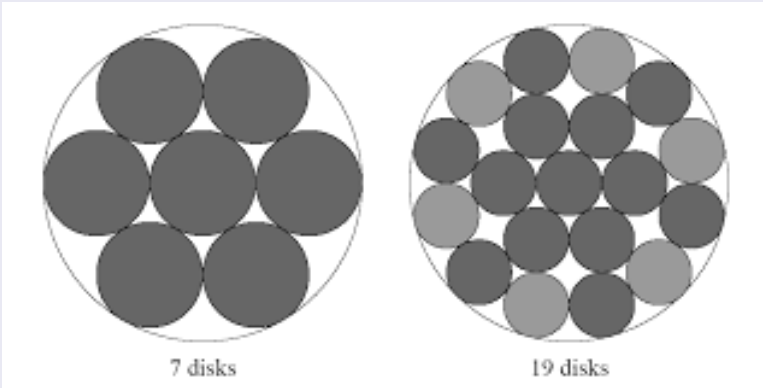
Physical properties of radio propagation (**diffusion, superposition and reciprocity**) provide opportunities for this

- Fading: provides natural degradedness over time
- Interference: allows active countermeasures to eavesdropping
- Spatial diversity (mMIMO, relays): creates "secrecy degrees of freedom"
- Randomness (small scale fading): sources of common randomness for key generation

Reminder on code construction for AWGN

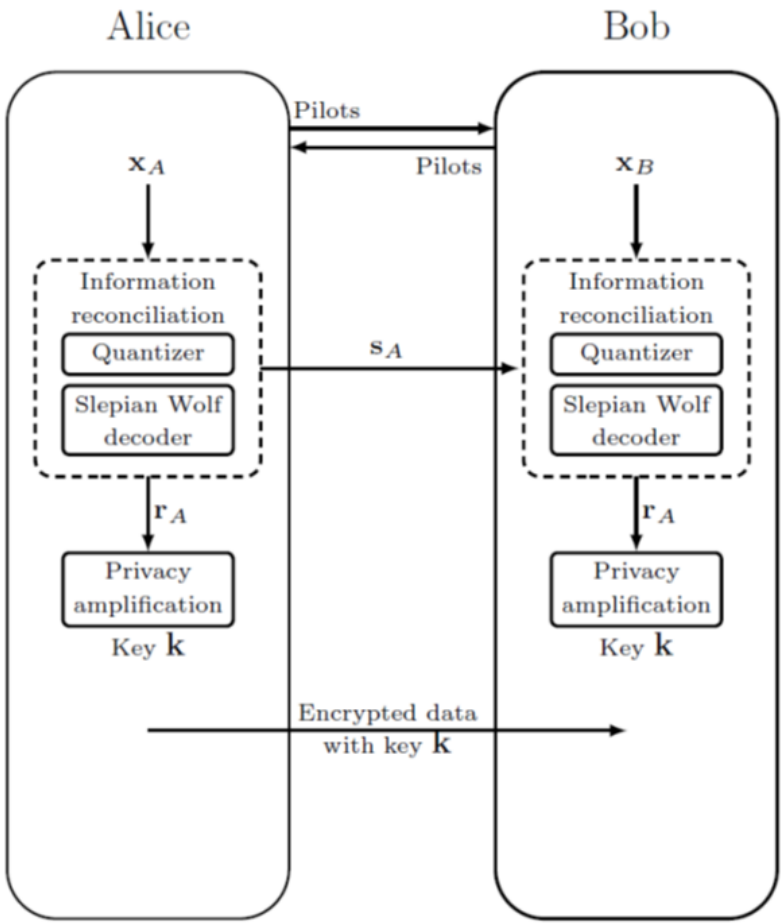
For codelength $K \to \infty$, the observed vector in an AWGN with noise variance σ^2 channel lies, with high probability, near the surface of a sphere with radius $\sqrt{K}\sigma$. For secrecy, use double binning.





Secrecy capacity of broadcast channels

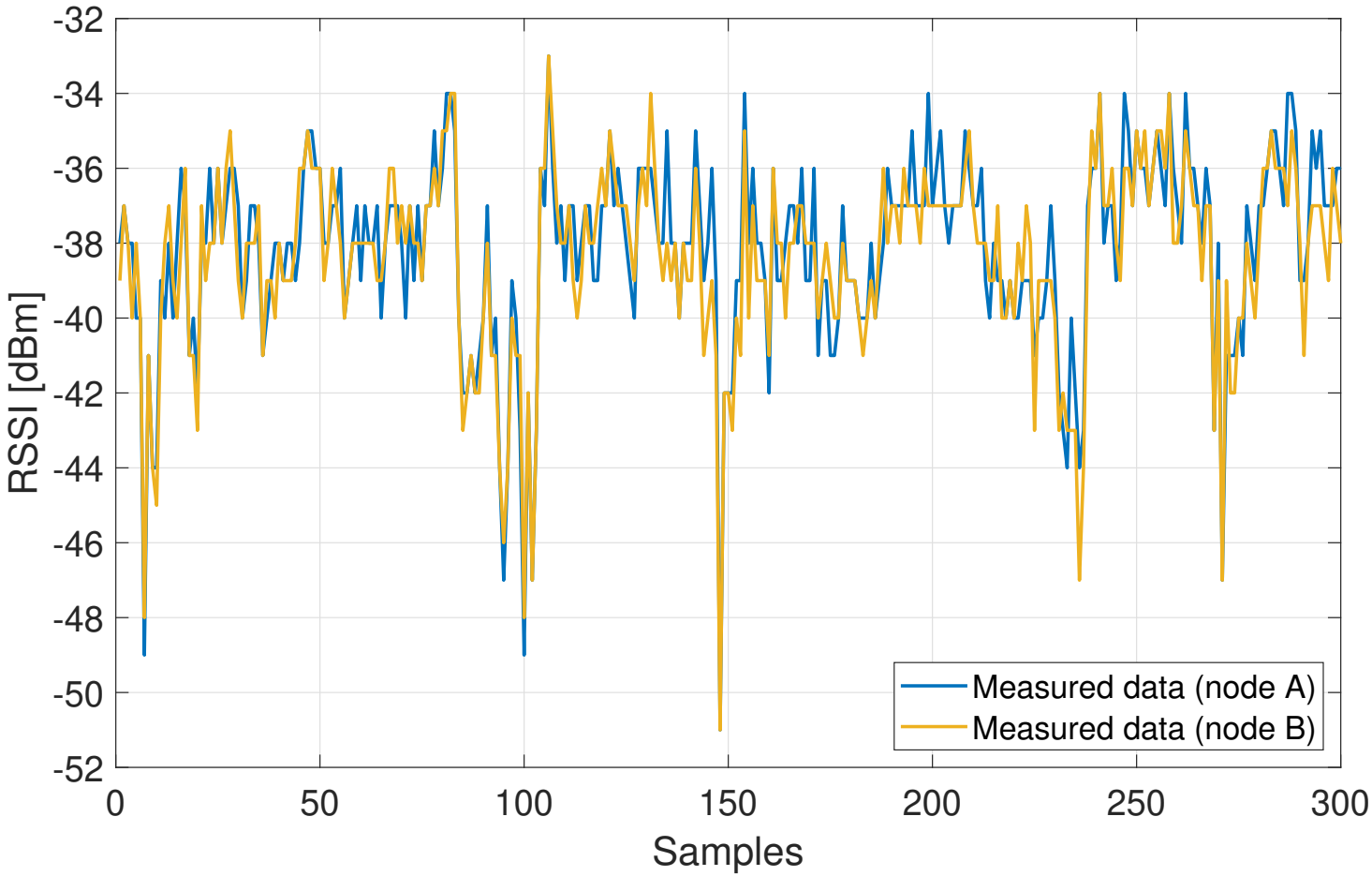
$$C_s = \max_{p(x)} \left[I(X;Y) - I(X;Z) \right]^+ \tag{2}$$



1. Quantizer outputs $\mathsf{r}_A = \mathsf{d} \oplus \mathsf{e}_A, \mathsf{r}_B = \mathsf{d} \oplus \mathsf{e}_B$
2. Reconciliation: reconstruct r_A from r_B as $\mathsf{r}_A = \mathsf{r}_B \oplus \mathsf{e}_B \oplus \mathsf{e}_A$
   - Temporal / spatial / frequency independence
3. Privacy amplification

Secret key capacity

Alice and Bob observe a shared random event.



Secret key capacity

$$C_k \leq I(X;Y|Z) \tag{3}$$

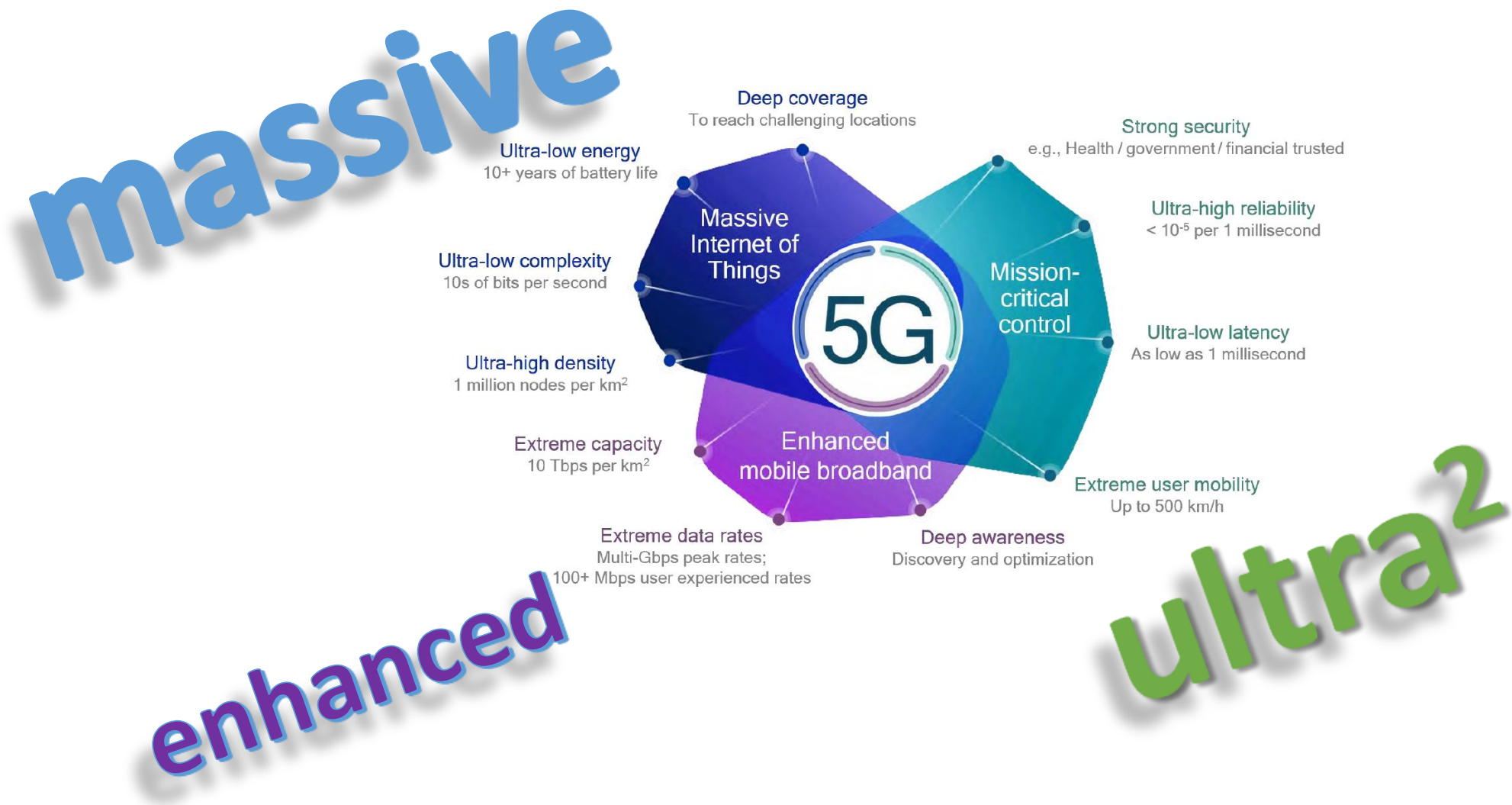
What changes in 6G?
(Will PLS be part of 6G?)

The need

The momentum

The technological roadmap

The need


massive
Deep coverage
To reach challenging locations
Ultra-low energy
10+ years of battery life
Strong security
e.g., Health / government / financial trusted
Massive Internet of Things
Ultra-high reliability
< 10-5 per 1 millisecond
Ultra-low complexity
10s of bits per second
5G
Mission-critical control
Ultra-low latency
As low as 1 millisecond
Ultra-high density
1 million nodes per km2
Extreme capacity
10 Tbps per km2
Enhanced mobile broadband
Extreme user mobility
Up to 500 km/h
Extreme data rates
Multi-Gbps peak rates;
100+ Mbps user experienced rates
Deep awareness
Discovery and optimization
enhanced
ultra2

Open issues

- **Latency**: $\sim$ 20 msec to verify digital signatures on a vehicle [A. Teniou *et al.*, Security and Privacy, 2018]
- **Scalability** in massive IoT: authentication and key distribution
- **Quantum computing**: post quantum cryptography
- **Constrained devices**, some deployed for 10+ years...
- **Artificial intelligence**, adversarial machine learning

Low-end IoT...

Picture taken from BBC News (4th May 2021)

..."He made Belgium bigger and France smaller, it's not a good idea," David Lavaux, mayor of the Belgian village of Erquelinnes, told French TV channel TF1. That sort of move caused a headache between private landowners, he pointed out, let alone neighbouring states...

Down the road

- **Fusion of digital and physical worlds**, autonomous systems making decisions

Νοῦς ὑγιὴς ἐν σώματι ὑγιεῖ

A sound mind in a healthy body

Trust and quality of security (QoSec)

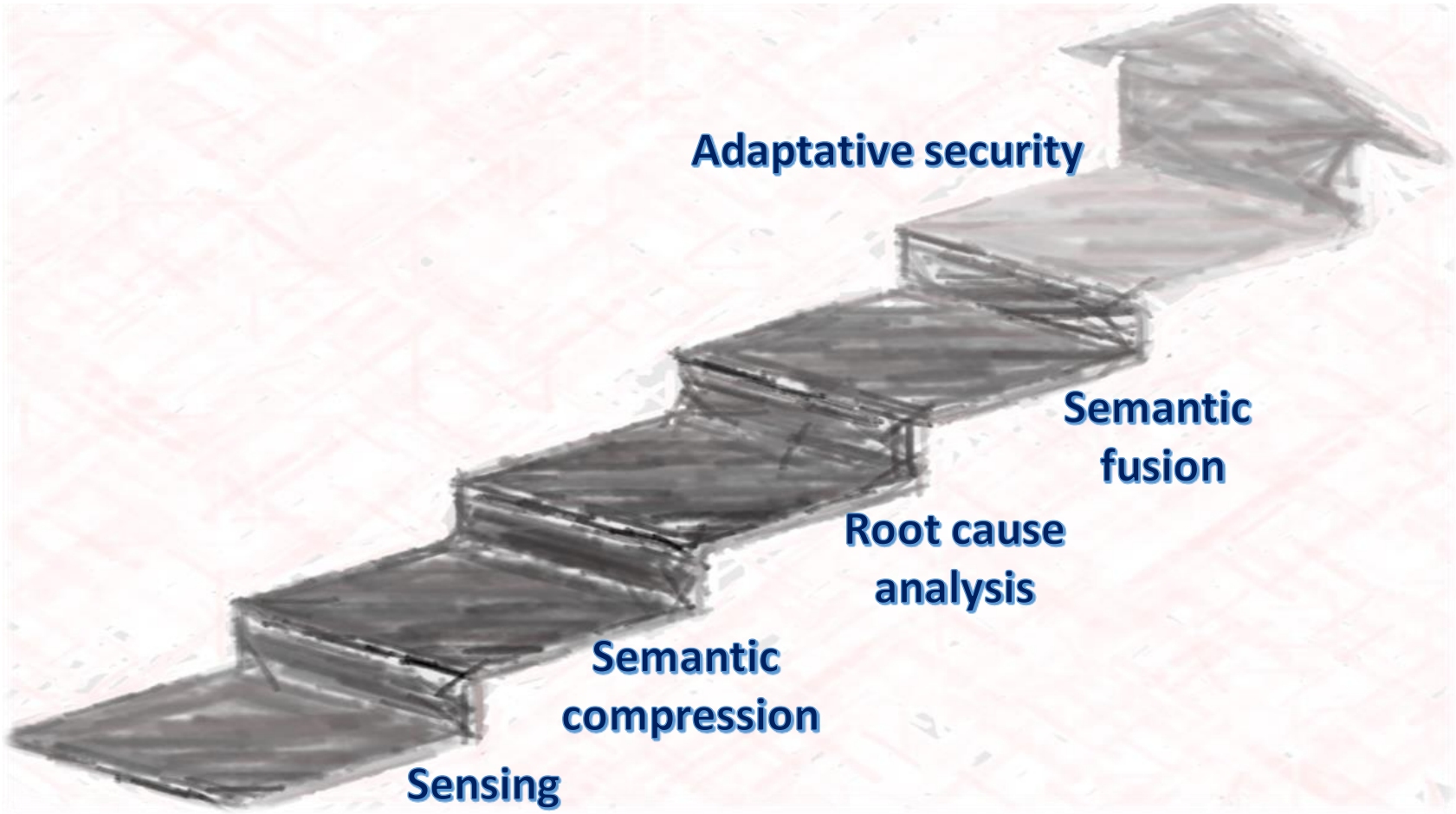
Until now trust has been studied for digital / cyber worlds

In 6G trust should include the physical world as well

QoSec: adaptive security levels, best effort security

1. Define security / trust levels
2. Build adaptive security controls
3. To deploy we need context awareness

Context aware security: a sketch



IEEE PLS Focus Group

Formed in September 2021, part of IEEE INGR Security

Steering Committee: A. Chorti (chair), A. Yener, M. Bloch, E. Hamad

More than 40 academic experts and industrial partners

- Main task: pave way for std WG on PLS for 6G
- Prepare white paper
- Engage with std organizations

4 working subgroups

- Use cases and applications (Stefano Tomasin)
- Threat model (Stefan Kopsell)
- Metrics and evaluation (Marco Baldi)
- Implementation aspects (Gunes Kurt)

What physical layer security (PLS) can do for us

A spectrum of technologies with different TRLs:

1. Counter-jamming at PHY (DoS attacks)
2. Localization / RF fingerprinting as an authentication factor
3. Physical unclonable functions (PUFs) for device authentication
4. Secret key generation (SKG) from shared randomness
5. Anomaly detection monitoring hardware
6. Secrecy codes for wiretap channels, geofencing

Roadmap *or* Why is PLS not in 5G?

Issue 1: the channel is not the one in the proof

Guarantees depend on assumptions for adversarial channel

$$\begin{aligned} C_s &= (C_m - C_e)^+ \\ P_{out}^{(s)} &= \mathbb{E}[C_{s,k} < \tau] \end{aligned}$$

$$C_k = I(Z_A; Z_B | Z_E)$$

Solutions possible in 6G:

- Online, site specific learning of channel, let the data speak!
- Engineer transmission so that end-to-end it looks like in the proof
- Context awareness: taxonomy of PLS, which technology under what conditions

Security guarantees in finite blocklength

Solutions possible in 6G:

- QoSec, privacy
- Recent important results

$$R_s(n, \epsilon, \delta) = C_s - \sqrt{\frac{V}{n}} Q^{-1}\left(\frac{\delta}{1-\epsilon}\right) + \mathcal{O}\left(\frac{\log n}{n}\right) \qquad (4)$$

  δ: leakage and ϵ: Bob's error probability [Yang *et al.*, TIFS 2019]
- Analyses for stable throughput, scheduling, etc.

Issue 3: compromised rates

PLS compromises transmission rates!

0.5 b/s/Hz not guaranteed even in subTHz when active attacks

[Ma *et al.*, Nature, 2018]

Breaking the deadlock:

- Use PLS to distil / distribute keys
- Hybrid schemes, no need for high rates!
- Example: TLS AES 256 GCM SHA384 [GCM]: 96 bytes of key material for records of 2^{14} bytes, i.e., 0.006 bits/sec
- Keys can be used over multiple records (e.g., up to 2^{24})

PLS is inherently adaptive: great match for 6G

Adjust secrecy outages depending on QoSec level

$$P_{out}^{(s)} = \mathbb{E}[R_s < \tau] \tag{5}$$

τ	:	rate for key distribution
$P_{out}^{(s)}$	:	select from QoSec
R_s	:	finite blocklength analysis
		transmission engineering
$\mathbb{E}[\cdot]$	:	online learning of channel statistics

Determinism & Randomness in Wireless Links for Authentication & Key Distillation

with Drs. Muralikrishnan Srinivasan, Sotiris Skaperas, Mahdi Shakiba Herfeh

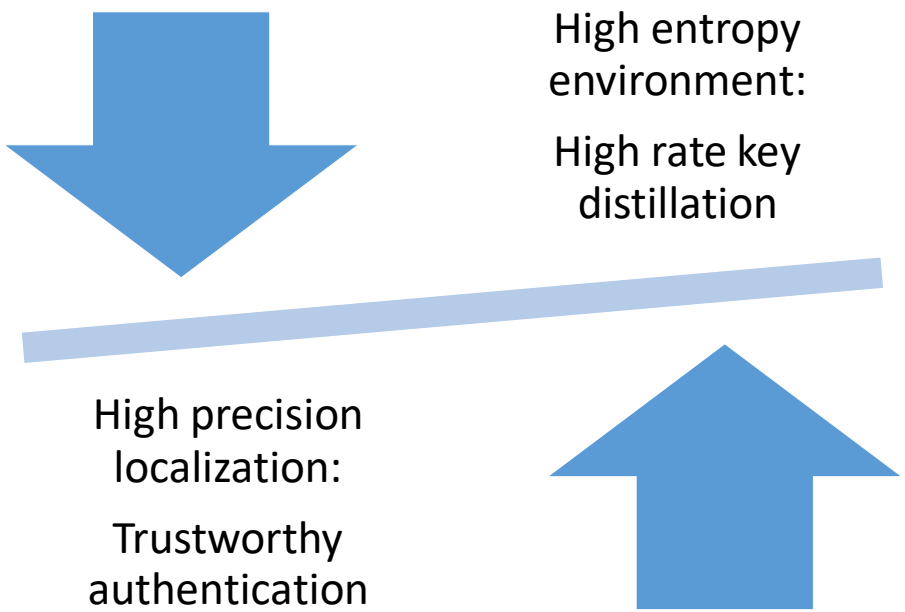


projects: SAFEST (DIM RFSI with Nokia Bell Labs)
ELIOT (ANR PRCI with Univ. Sao Paolo and PUC Rio)
eNiGMA (CYU INEX), PHEBE (CYU INEX)

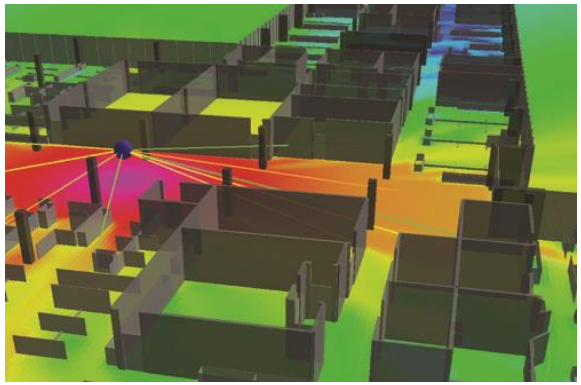
The dual role of the wireless channel

Wireless coefficients can be used for:

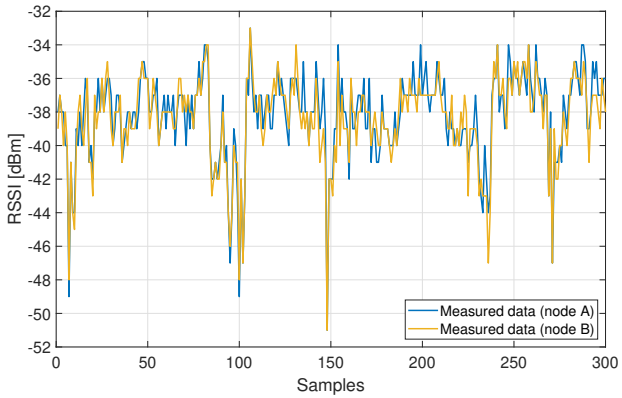
1. Authentication through RF fingerprinting / localization
2. Symmetric secret key generation (SKG) $\Longrightarrow$ Tx and Rx distil keys from "shared" randomness



Deterministic and stochastic fading



Ray tracing



WiFi RSS at 9 m distance

- **Large scale fading** related to positioning
- Largely predictable, useful for authentication
- *Separability* is important (not necessarily decorrelation)

- **Small scale fading** due to unpredictable variations in channel state information (CSI)
- Source of entropy to distil keys from shared randomness
- *Unpredictability* is important (resist next bit predictors)

Pseudorandom number generator

Pseudorandomness of generator G: the ensemble $\{G(U_n)\}_{n\in N}$ is pseudorandom, iff for any probabilistic polynomial-time algorithm A, for any positive polynomial p, and for all sufficiently large n,

$$\left|Pr(A(G(U_n); 1^{l(n)})) = 1) - Pr(A(U_{l(n)}; 1^{l(n)}) = 1)\right| < \frac{1}{p(n)} \quad (6)$$

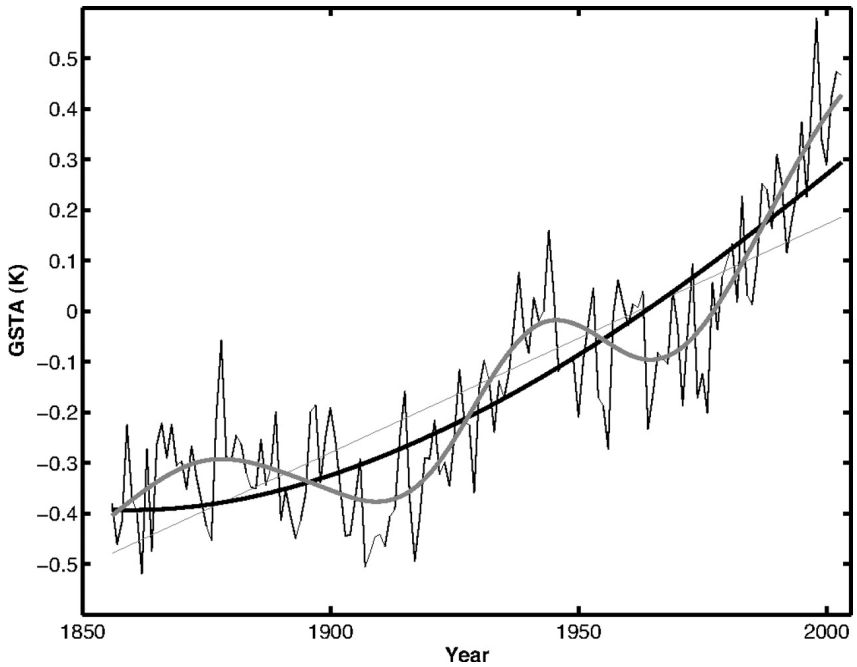
Sufficient condition of unpredictability is **independence**
Achievable SKG rate

$$R_k \leq I\left(X; Y|Z\right) \quad (7)$$

Goal: disentangle predictable / unpredictable components

Wold's decomposition theorem: every covariance-stationary time series can be written as the sum of two time series, one deterministic and one stochastic

Existence theorem, no guideline on how to do it



[Wu *et al.*, PNAS 2007]

How will we do it?

Key observation: separation more favourable in two domains, **frequency and power**

1. Predictable, position dependent and separable components are probably slow varying and dominant in power
2. Unpredictable, reciprocal and independent components are probably fast(er) varying, medium / low power

Proposed pre-processing

In this work: focus on power domain separation

Employ unsupervised learning: PCA and autoencoders

Implicate two different measures to capture separability and independence: TVD and HSIC

Work with synthetic *and* real data

Proposed metric for separability

Total variation distance (TVD)

$$TVD(P,Q) = \frac{1}{2}\sum_{\omega\in\Omega}|P(\omega) - Q(\omega)| \leq \sqrt{\frac{1}{2}D_{KL}(P||Q)} \quad (8)$$

Proposed metrics for unpredictability

1. Pearson cross-correlation coefficient

$$\rho(\tilde{\boldsymbol{h}}_1, \tilde{\boldsymbol{h}}_2) = \frac{\mathbb{E}\left(\tilde{\boldsymbol{h}}_1 - \mathbb{E}\left(\tilde{\boldsymbol{h}}_1\right)\right)\mathbb{E}\left(\tilde{\boldsymbol{h}}_2 - \mathbb{E}\left(\tilde{\boldsymbol{h}}_2\right)\right)}{\sigma_{\tilde{\boldsymbol{h}}_1}\sigma_{\tilde{\boldsymbol{h}}_2}} \tag{9}$$

2. dHSIC, kernel independence criterion based on Hilbert-Schmidt norm

$$dHSIC\left(\mathbb{P}^{(\tilde{\mathrm{H}}^1,\ldots,\tilde{\mathrm{H}}^N)}\right) := \left\| \prod\left(\mathbb{P}^{\tilde{\mathrm{H}}^1}\otimes,\ldots,\otimes\mathbb{P}^{\tilde{\mathrm{H}}^N}\right) - \prod\left(\mathbb{P}^{(\tilde{\mathrm{H}}^1,\ldots,\tilde{\mathrm{H}}^N)}\right)\right\|^2_{\mathcal{H}} \tag{10}$$

- $dHSIC = 0 \iff \mathbb{P}^{\tilde{\mathrm{H}}^1}\otimes,\ldots,\otimes\mathbb{P}^{\tilde{\mathrm{H}}^N} = \mathbb{P}^{(\tilde{\mathrm{H}}^1,\ldots,\tilde{\mathrm{H}}^N)}$
- *dHSIC* is applied as a non parametric hypothesis test
  H_0 : $N-$ vectors are mutually (pairwise) independent
  H_1 : not H_0

[N. Pfister, *et al.*, *J. Royal Statistical Society: Series B (Statistical Methodology)*, 2018]

Asymptotic behavior under H_0 (critical value)

$dHSIC_M\left(\tilde{\boldsymbol{H}}\right)$ can be approximated by a permutation test under H_0

- **Critical value**

$$CV_\alpha = \left[\mathrm{D}^{dHSIC}\right]_{\left\lceil (B+1)(1-\alpha)\right\rceil + \sum_{i=1}^{B} \mathbb{1}_{\{dHSIC(\tilde{\boldsymbol{H}}) = dHSIC(\tilde{\boldsymbol{H}}_i)\}}}$$

  - D^{dHSIC} contains the B Monte-Carlo realisations of $dHSIC(\tilde{\boldsymbol{H}})$ in an increasing order
  - $dHSIC\left(\tilde{\boldsymbol{H}}\right)$, $\tilde{\boldsymbol{H}} = \left(r_1(\tilde{\boldsymbol{h}}_1), \cdots, r_M(\tilde{\boldsymbol{h}}_M)\right)$ is constructed by $r_1, \cdots, r_M$ random re-samplings without replacement
  - B: Monte-Carlo realizations
  - $\lceil . \rceil$: ceiling function
  - $[.]_j$: j-th element of a vector
  - $\mathbb{1}_{\{.\}}$: indicator function

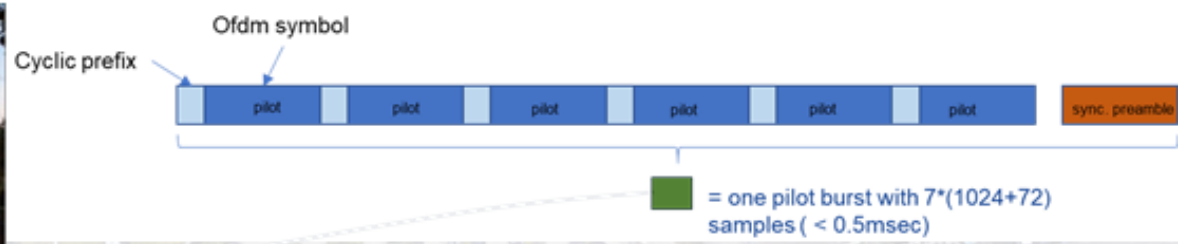
Proposed normalized-metric

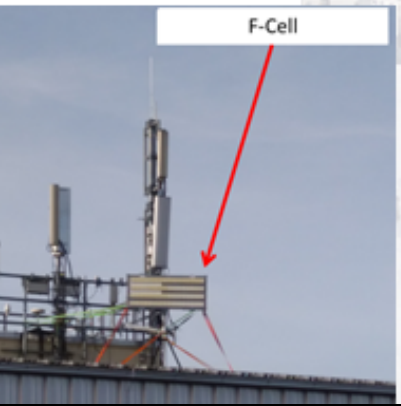
$$\overline{dHSIC} = \frac{dHSIC(\tilde{\boldsymbol{H}})}{CV_\alpha} \mathbb{1}_{\{dHSIC(\tilde{\boldsymbol{H}}) > CV_\alpha\}}$$

$\overline{dHSIC}$ near one $\implies$ low dependence

Nokia experimental dataset [S. Schwarz, *et al.* IEEE JSSP, 2019]

- 2.180 GHz, 64 antennas, BS at height of 20 m, 50 OFDM subcarriers, 40 dBm (avg.) Tx power (7 dBi antenna gain)
- Each track has 45 subtracks, of 2000 timeshots of 64 complex channel measurements per subcarrier, subsampling by factor 5





Threat model for SKG

Passive attacker (eavesdropper)

On the shoulder attack!

Active attacks addressed in other works:

- Jamming attacks: frequency hopping and energy harvesting
- Injection (impersonation): pilot randomization
- Tampering side information: authenticated encryption using SKG

Statistical characterisation of the Nokia dataset (1)

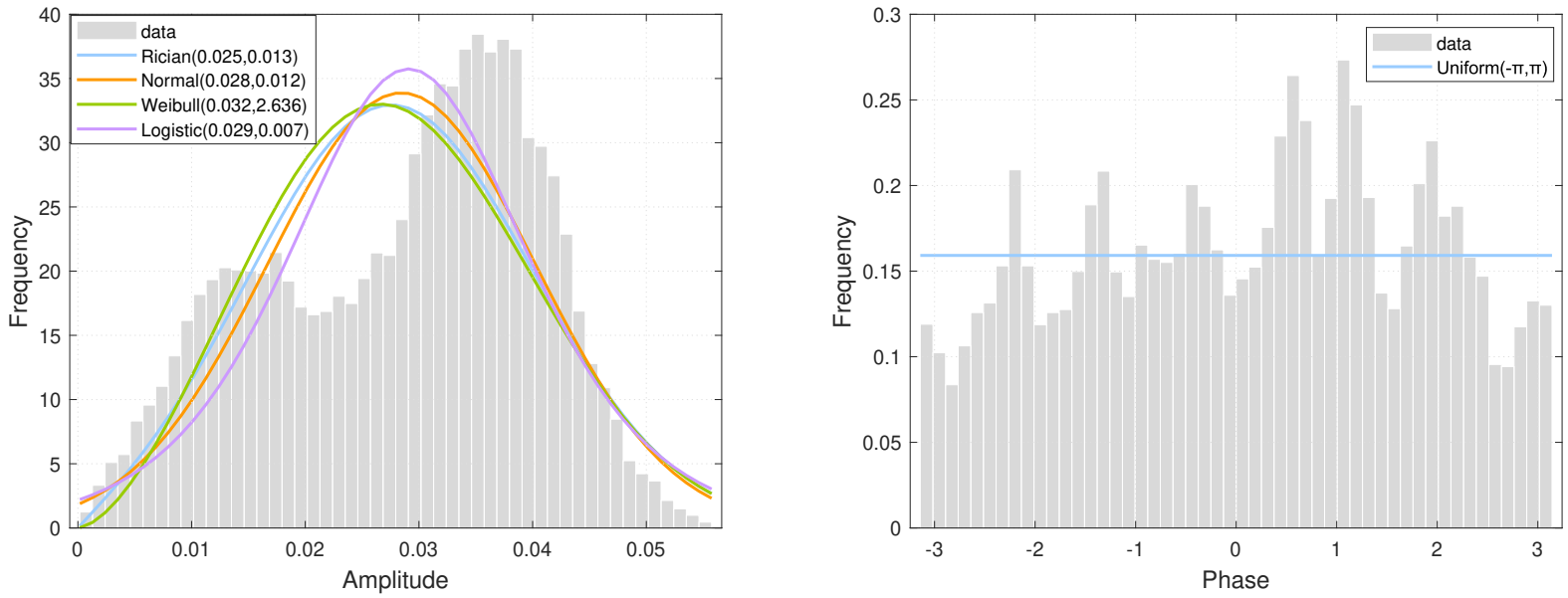


Figure: PDF fitting for the amplitude and the phase of measured CSIs on track 6

Statistical characterisation of the Nokia dataset (2)

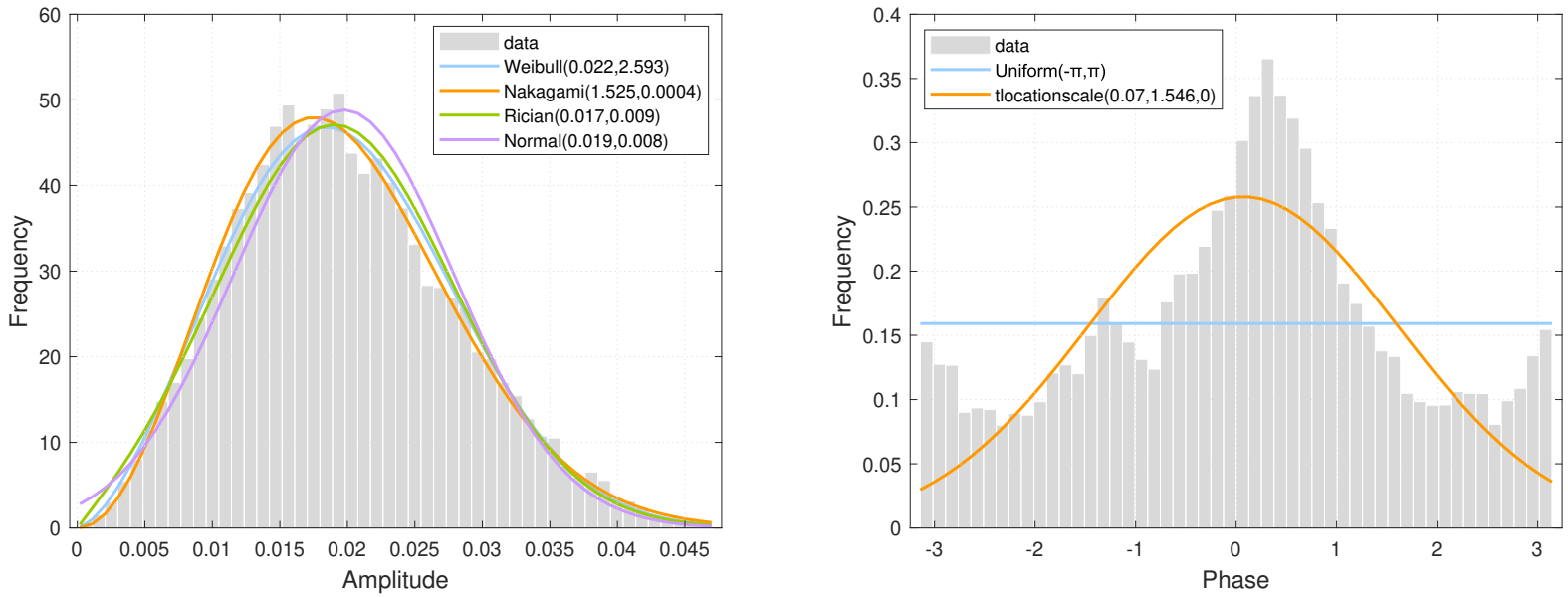


Figure: PDF fitting for the amplitude and the phase of measured CSIs on track 12

PCA based preprocessing at BS

Conjecture: large scale fading dominant in power

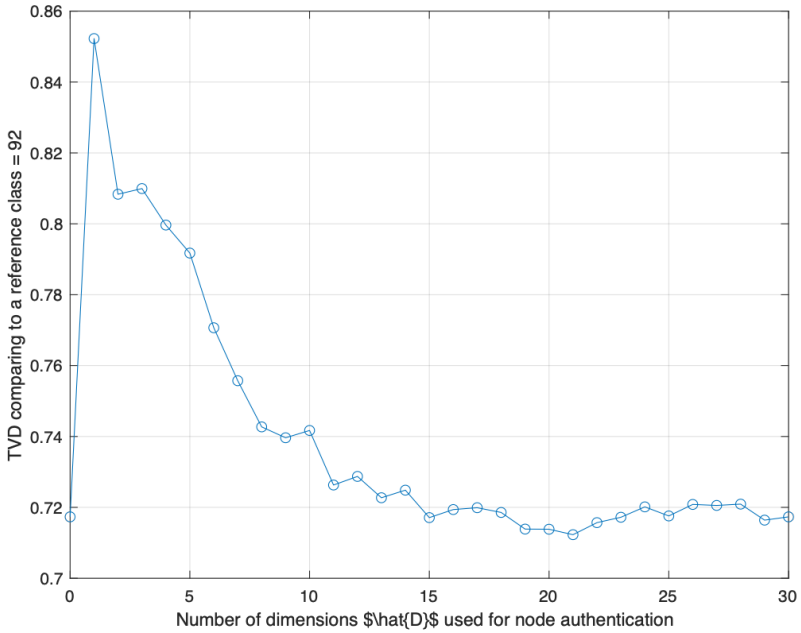
1. PCA of the CSI matrix to perform eigenvector decomposition
2. Inverse PCA (invPCA) for *specific ranges* of eigenvectors (principal components – PCs)
3. **RF fingerprint**: invPCA over first $\widehat{D}$ PCs
4. **Shared randomness**: invPCA over range $\tilde{D}_1$ to $\tilde{D}_1 + \tilde{D}_2$ PCs
5. **Denoising** by ignoring components after $\widehat{D} + \tilde{D}_1 + \tilde{D}_2$

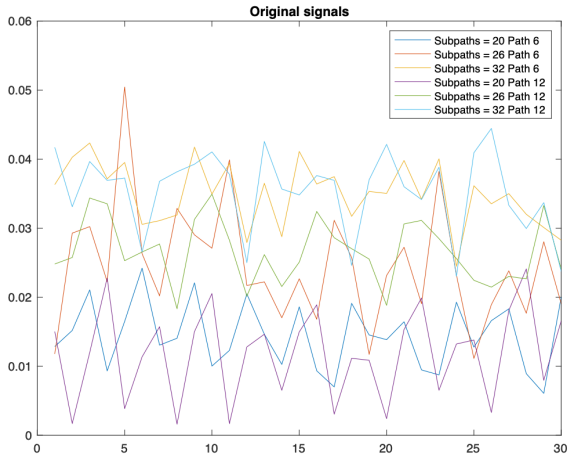
Design criterion

The triplet $\{\widehat{D}, \tilde{D}_1, \tilde{D}_2\}$ chosen so that

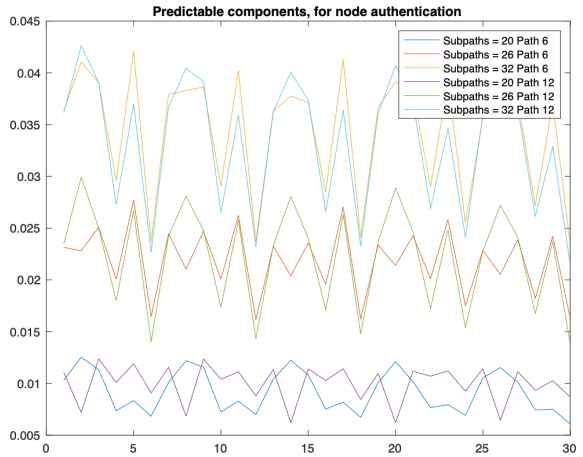
- TVD between RF fingerprints is maximum
- Unpredictable components have low spatial, frequency (or time) correlation / dependence *while* being reciprocal

PCA preprocessing for RF fingerprinting - Nokia



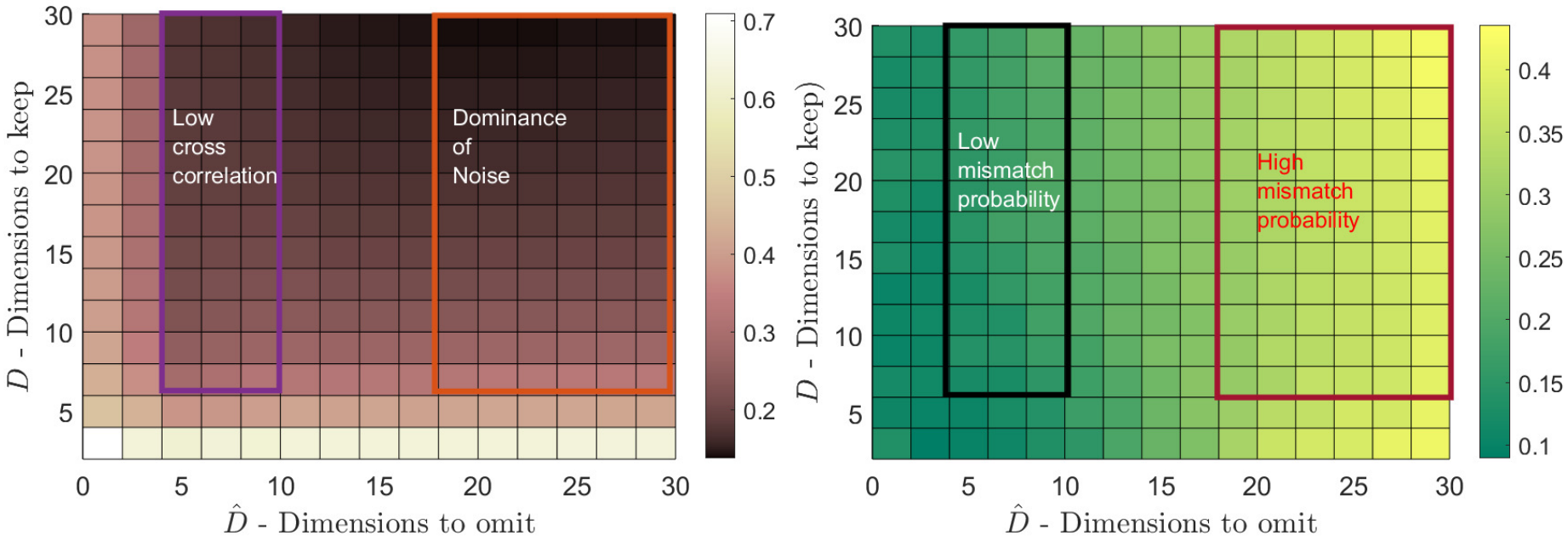


(a) Signals of 6 subtracks on tracks 6 and 12, SNR=20 dB



(b) First PC of 6 subtracks on tracks 6 and 12, SNR=20 dB

PCA SKG pre-processing SNR=20 dB - Nokia



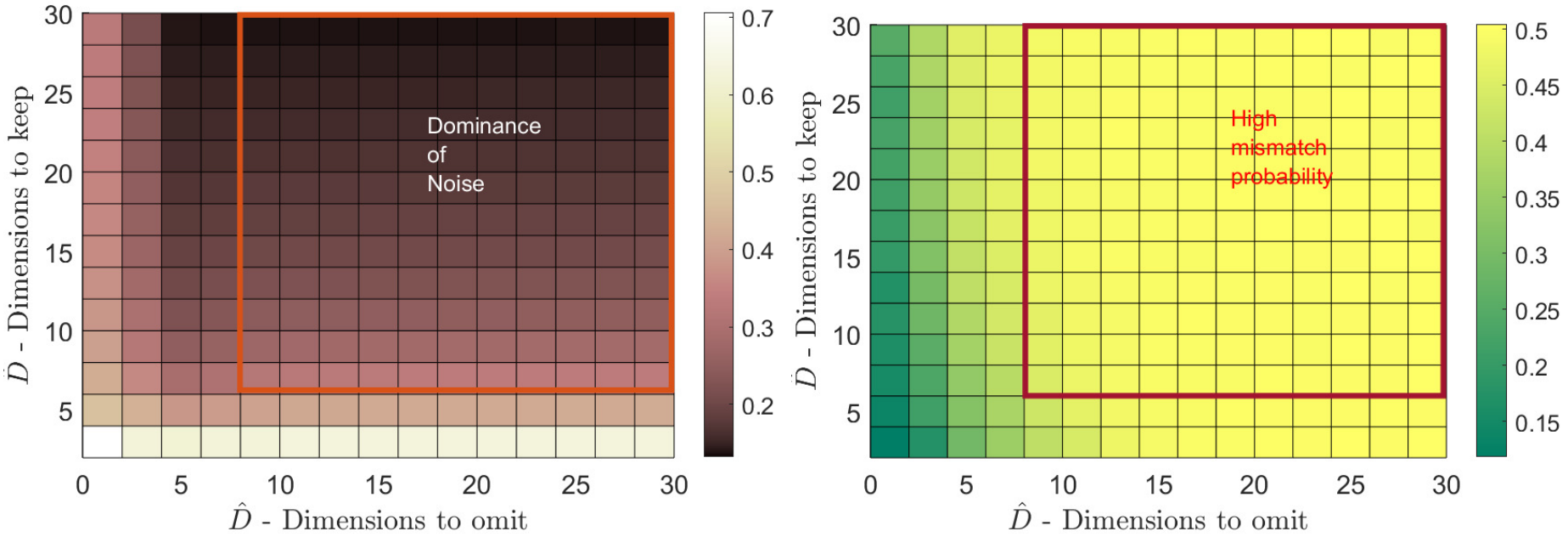
(a) Average CC (Original= (0.38)

(b) Average MP

Figure: Trade-off for the Residual components for SNR = 20 dB for Nokia Data-set

For $\tilde{D}_1 = 6$, $\tilde{D}_2 = 30$, CC drops to 0.14 with insignificant increase in MP

PCA SKG pre-processing SNR=5 dB - Nokia



(a) Average CC (Original= (0.23)

(b) Average MP

Figure: Trade-off for the Residual components for SNR = 5 dB for Nokia dataset

Evolution of $\overline{dHSIC}$

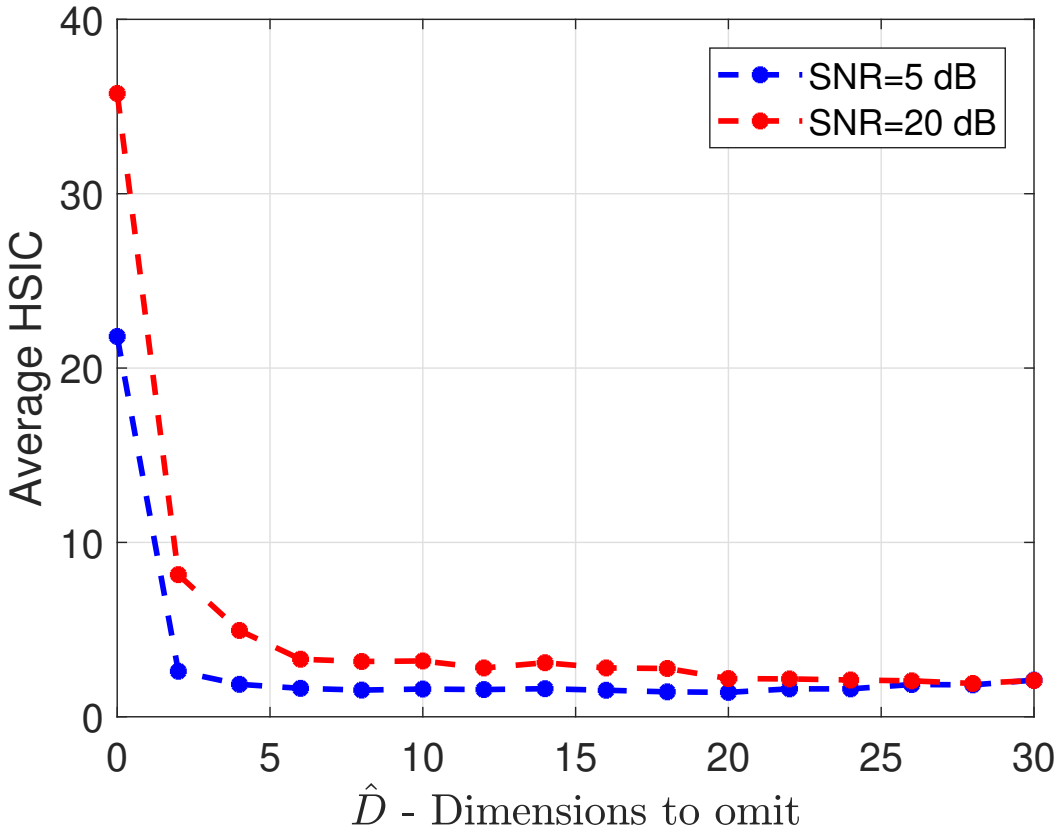
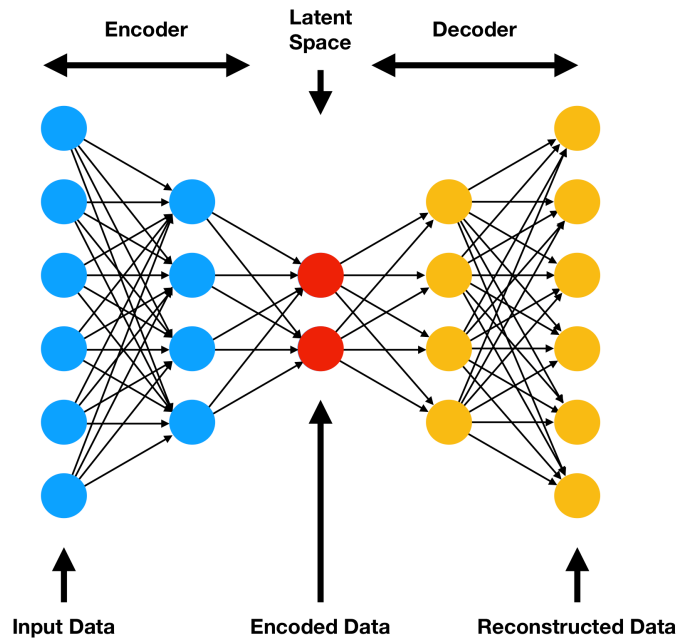


Figure: Nokia

Figure: Evolution of $\overline{dHSIC}$ with $\tilde{D}_1$ for $\tilde{D}_2 = 30$ for Quadriga and Nokia datasets

Autoencoder 1 - AE1



- Encoder maps M-d input matrix $\boldsymbol{h}_{nu}$ to $\tilde{D}$ dimensions
- Decoder maps back to an M dimensional output $\hat{\boldsymbol{h}}_{nu}$
- Loss-function: MSE is minimized

$$E_1 = \frac{1}{N}\sum_{n=1}^{N} \|\boldsymbol{h}_{nu} - \hat{\boldsymbol{h}}_{nu}\|_2^2, \text{ for } u \in \{a, b\} \tag{11}$$

- Unpredictable component

$$\left\{\tilde{\boldsymbol{h}}_{nu}(D)\right\}_{n=1}^{N} = \{\boldsymbol{h}_{nu} - \hat{\boldsymbol{h}}_{nu}\}_{n=1}^{N}, \text{ for } u \in \{a, b\} \tag{12}$$

Modified AE (AE2)

- Loss function includes an additional weighted correlation term
- Modified loss function

$$E_2 = \frac{1}{N} \sum_{\substack{n_1=1 \\ n_2 \in \mathcal{U}(n_1)}}^{N} \{\boldsymbol{h}_{n_1 u} - \hat{\boldsymbol{h}}_{n_1 u}\}^T \{\boldsymbol{h}_{n_2 u} - \hat{\boldsymbol{h}}_{n_2 u}\}, \quad \text{for } u \in \{a, b\} \tag{13}$$

where $\mathcal{U}(n_1)$ is the nearest neighbours of n_1 (e.g., 8 by considering the first square grid around each point)

AE architecture

[Studer *et al.*, *IEEE Access*, 2018]

Layer	Dimensions	Activation
Input	200	Linear
1	100	tanh
2	50	softplus
3	20	tanh
Intermediate	$\widehat{D}$	linear
4	20	relu
5	50	softplus
6	100	tanh
Output	200	Linear

Table: The layers and activation function for AE1. For AE2 the only change is that the dimensions of the input and the output layers are 400

AE Nokia data

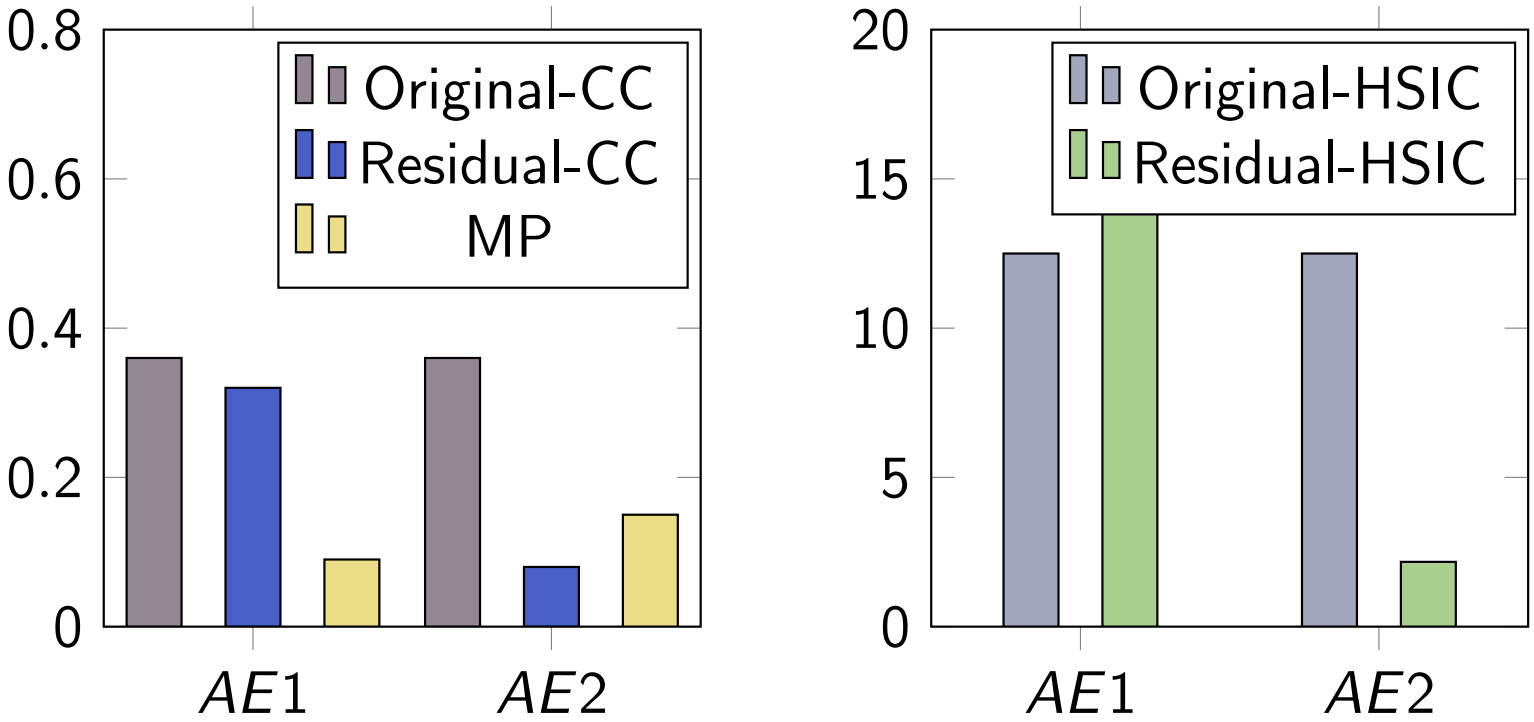


Figure: Key results for Nokia dataset for SNR= 20 dB and $\tilde{D} = 8$

Zoom in at AE2

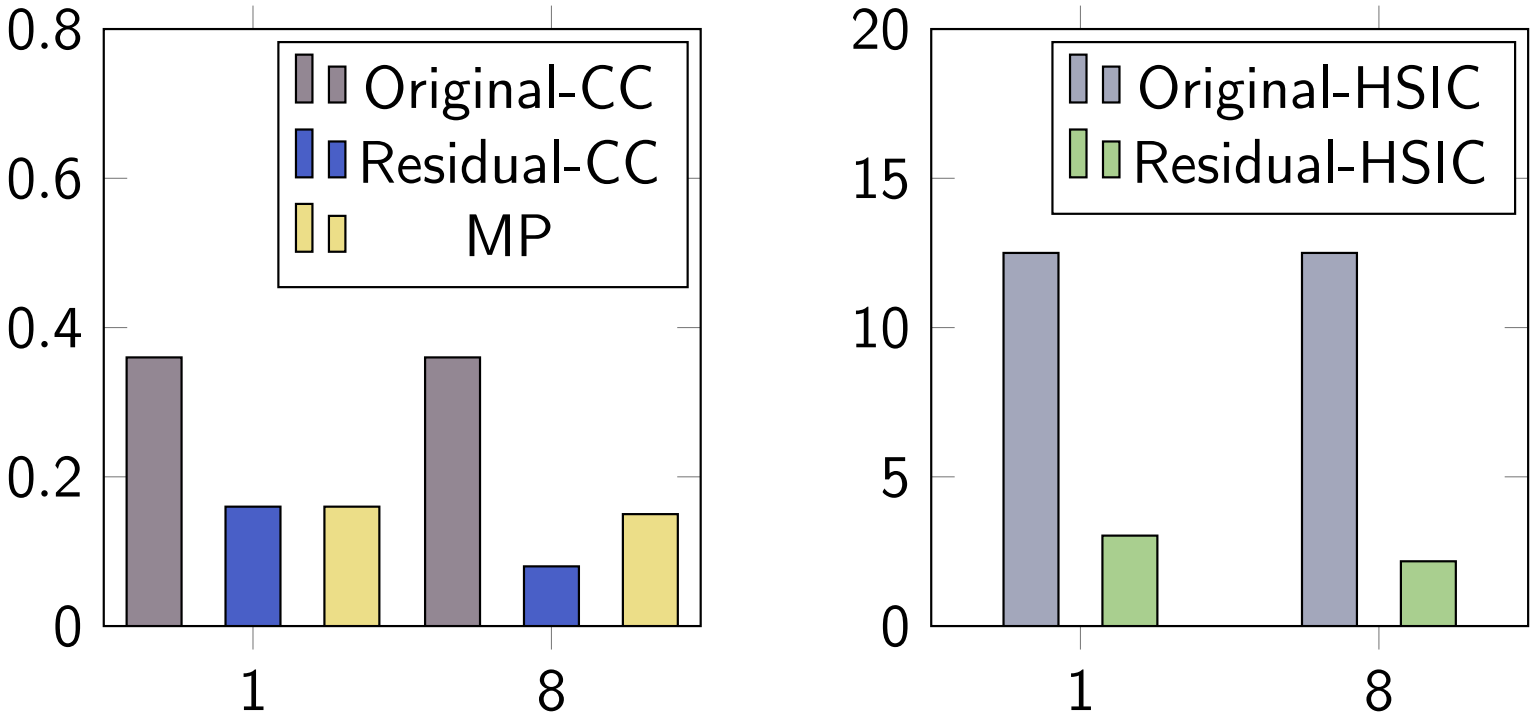


Figure: Key results of AE2 for Nokia dataset for SNR= 20 dB to show the difference between $\tilde{D} = 1$ and 8

Ongoing work

- AE3 with composite loss function: weighted sum of $\overline{dHSIC}$ and MP
- Online evaluation of channel statistics
- Trade-off between pre-processing and more hashing!

Selected related papers

- M. Srinivisan, S. Skaperas, M.S. Herfeh, A. Chorti, Joint Localization Based Node Authentication and Secret Key Generation, to appear in Proc. IEEE ICC 2022
- M. Srinivasan, S. Skaperas, and A. Chorti, "On the use of CSI for the generation of rf fingerprints and secret keys," in 25th Int. ITG Workshop on Smart Ant., 2021
- M. Mitev, A. Chorti, M.J. Reed and L. Musavian, Authenticated secret key generation in delay-constrained wireless systems, Eurasip J. Wireless Com. Network, 2020, vol. 122
- M. Shakiba-Herfeh, A. Chorti, and H. Vincent Poor, Physical Layer Security: Authentication, Integrity, and Confidentiality. Springer Inter- national Publishing, 2021, pp. 129–150.
- M. Shakiba-Herfeh and A. Chorti, "Comparison of short blocklength slepian-wolf coding for key reconciliation," in IEEE Stat. Signal Process. Workshop SSP 2021, 2021
- A. Chorti, A. N. Barreto, S. Kopsel, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. Poor, Context-aware security for 6G wireless, the role of physical layer security, IEEE Communications Standards Mag., March 2022
- A. N. Barreto, S. Köpsell, A. Chorti, B. Poettering, J. Jelitto, J. Hesse, J. Boole, K. Rieck, M. Kountouris, D. Singelee and Kumar Ashwinee, Towards Intelligent Context-Aware 6G Security, under review IEEE Network Mgz
- W. Njima, M. Chafii, A. Chorti, R. M. Shubair, and H. V. Poor, "Indoor localization using data augmentation via selective generative adversarial networks," IEEE Access, vol. 9, pp. 98 337–98 347, 2021
- G. Rezgui, E.V. Belmega, A. Chorti, "Mitigating Jamming Attacks Using Energy Harvesting", IEEE Wireless Communications Letters, 2019
- A. Chorti, "Optimal signalling strategies and power allocation for wireless secret key generation systems in the presence of a jammer," in 2017 ICC, IEEE, 2017
- E.V. Belmega, A. Chorti "Protecting Secret Key Generation Systems against Jamming: Energy Harvesting and Channel Hopping Approaches", IEEE Trans. Inf. Forensics Security, 2017
- G.A. Nunez Segura, A. Chorti, C. Borges Margi, "Centralized and Distributed Intrusion Detection for Resource Constrained Wireless SDN Networks", early access IEEE IoT Journal, 2021
- G.A. Nunez Segura, C. B. Margi, A. Chorti, "Understanding the Performance of Software Defined Wireless Sensor Networks Under Denial of Service Attack", Open Journal of Internet of things (OJIOT), 2019

Directions and contributions

- **Trust and trustworthiness in 6G**: moving away from static security
- **Securing RAN**: first line of defence for 6G
- **PLS enabled by sensing and AI**: towards context aware security
- **Preprocessing for RF fingerprinting and SKG with unsupervised learning**: PCA and AE

Thank you for the invitation!

Questions? email: arsenia.chorti@ensea.fr