A pain in the AES

Is LPWAN security doomed to be tedious ?

Nicolas MOREL

Supervisors: Stéphane DELBRUEL, Dave Singelée,

LPWAN days - 08/07/2024

KU LEUVEN

BORDEAUX INP

LaBRI

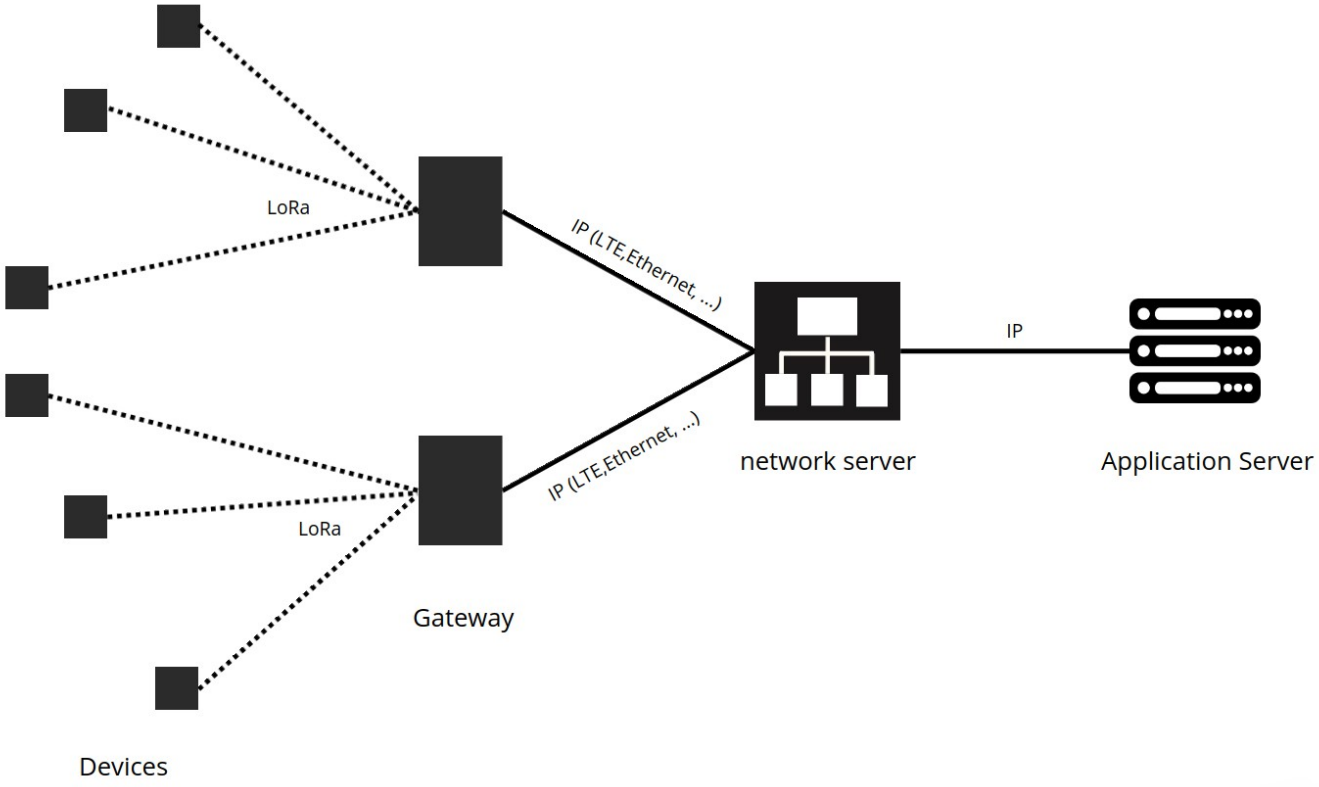
Context

- A need to ensure security for the whole stack (Physical ↔ Applicative)

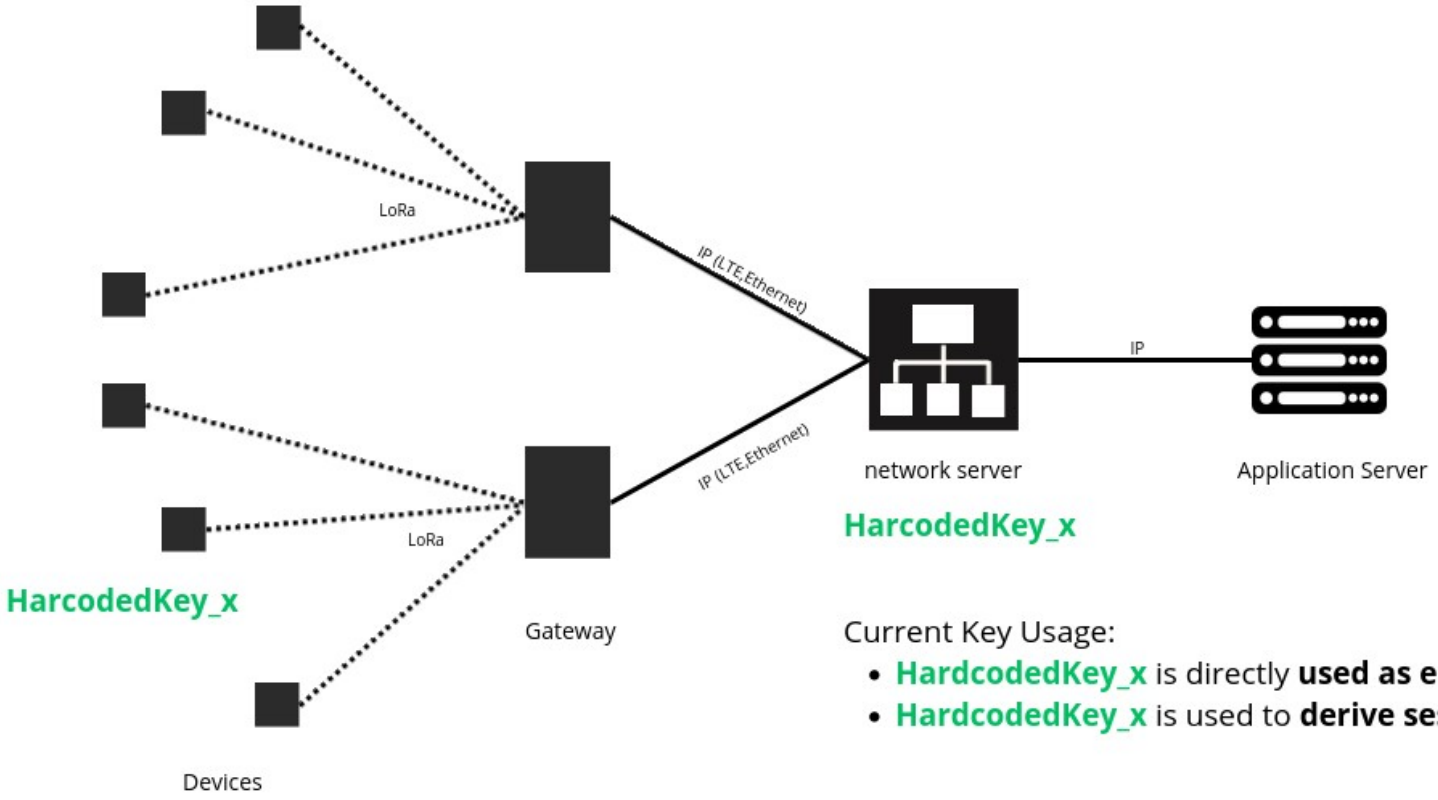
- Current security solutions seems not satisfying enough

LPWAN Security

- Based on a Central Authority



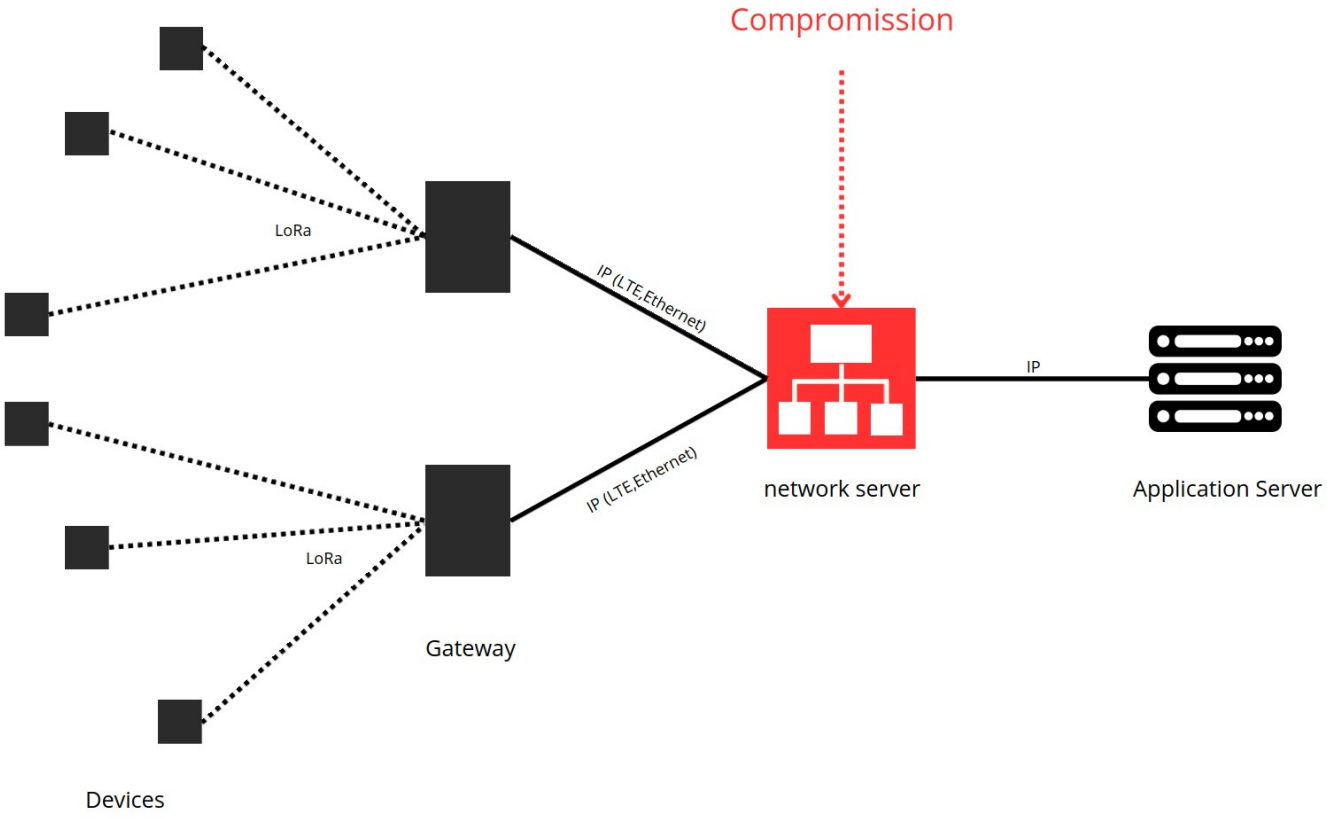
LPWAN Security - Issues/Limits



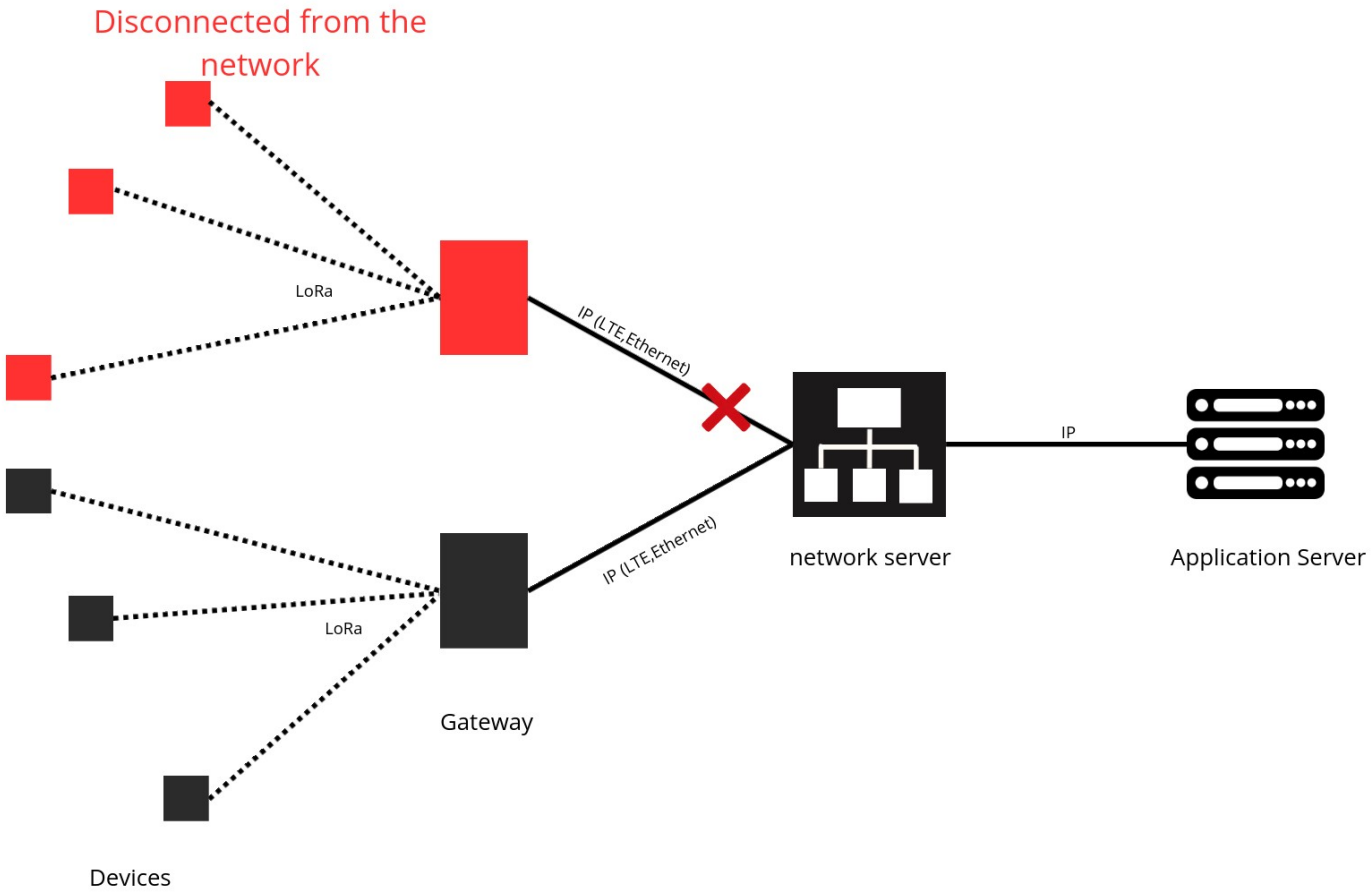
Current Key Usage:

- **HardcodedKey_x** is directly **used as encryption key**
- **HardcodedKey_x** is used to **derive session key**

LPWAN Security - Issues/Limits



LPWAN Security - Issues/Limits



PHYsec

Physical Layer based Security (PHYsec) proposes to rely on physical phenomena to provide security mechanisms

Leveraging on **Channel Reciprocity theorem** to offer new primitives :

- **Key Generation from unauthenticated channel** using channel features as common entropy source

- **Physical Authentication** (**RF Fingerprinting**) based on non-reproducible channel features

PHYsec – Channel Reciprocity Theorem

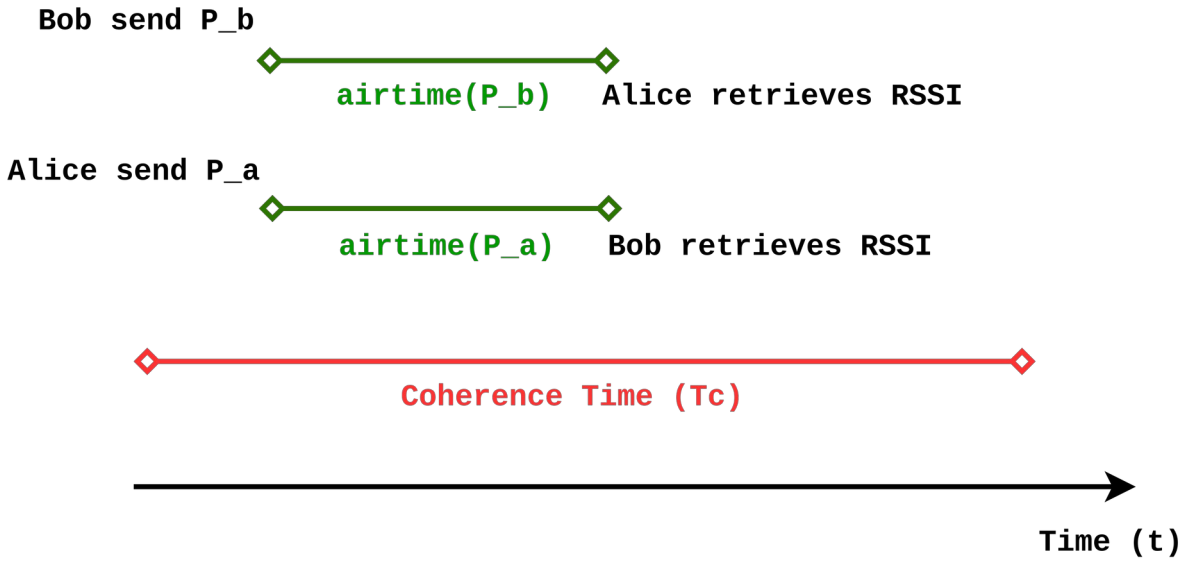
- **Noise** applied to the channel is **static** during **Tc**

Channels estimates :

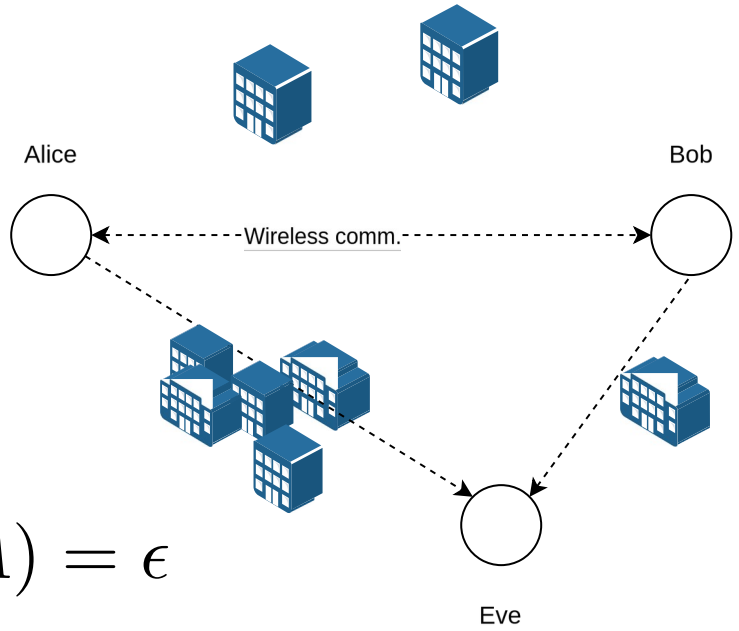
$$H_a = h_a + \epsilon$$

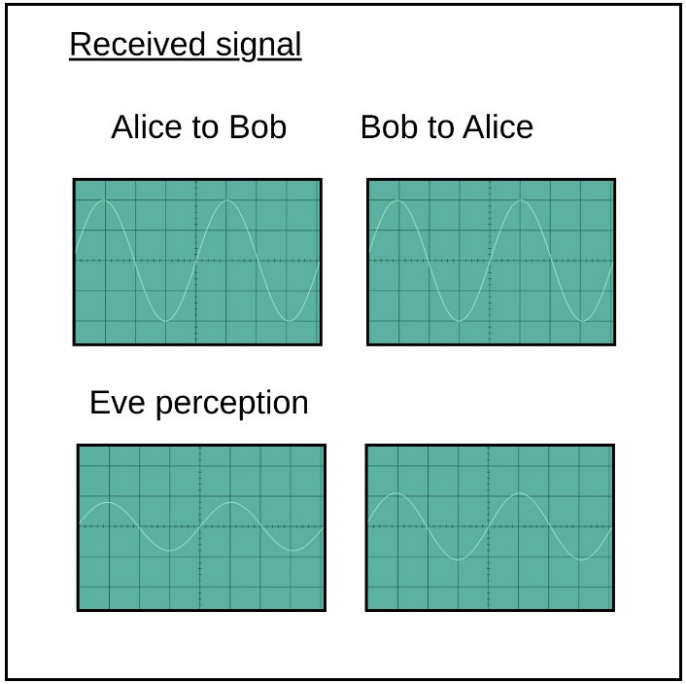
$$H_b = h_b + \epsilon$$

- A & B share a common random source ‘e’



PHYsec – Principles

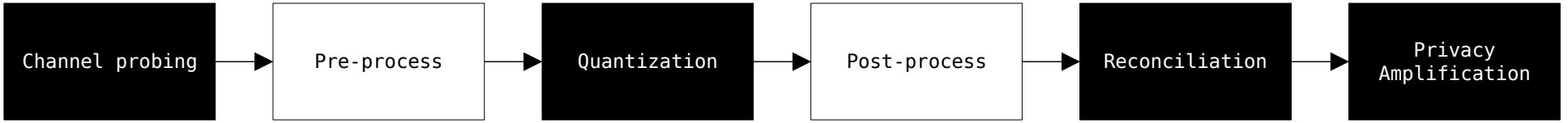




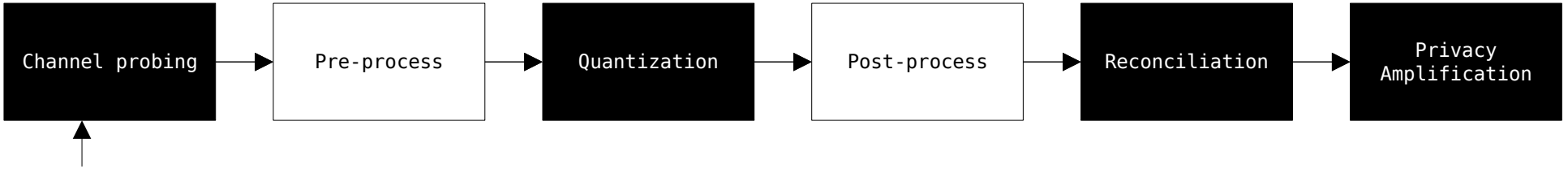
$$I(AB, BA) = \epsilon$$

$$I(AE, BE) = \epsilon'$$

PHYsec - Key Generation Procedure



PHYsec - Key Generation Procedure



Δ_{Physical}

- Half-duplex
- Unpredictable wireless environment

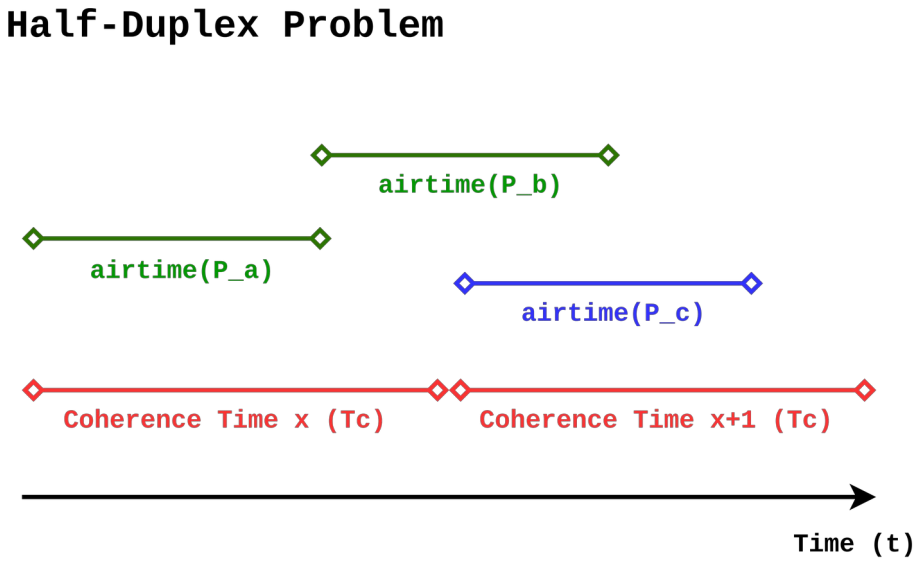
PHYsec – Acquisition & Challenges

$$H_a = h_a + \epsilon_x$$

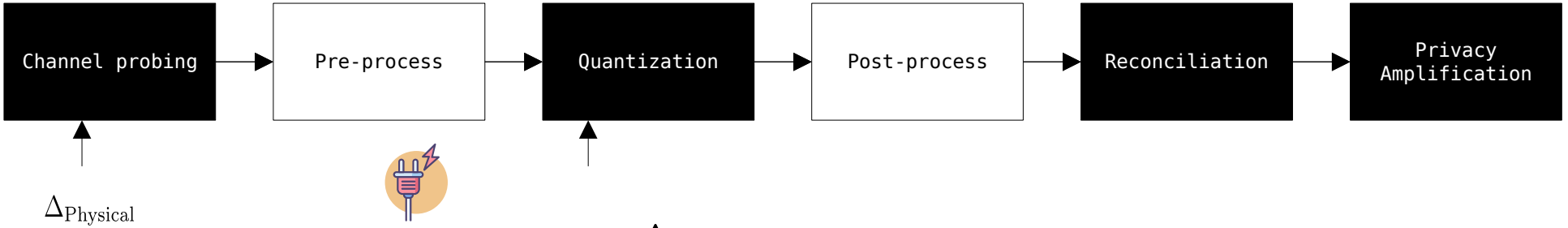
$$H_b = h_b + \epsilon_x + \epsilon_{x+1}$$

$\Delta(Physical)$

- Hardware impairments
- Half-Duplex



PHYsec - Key Generation Procedure



Δ_{Method}

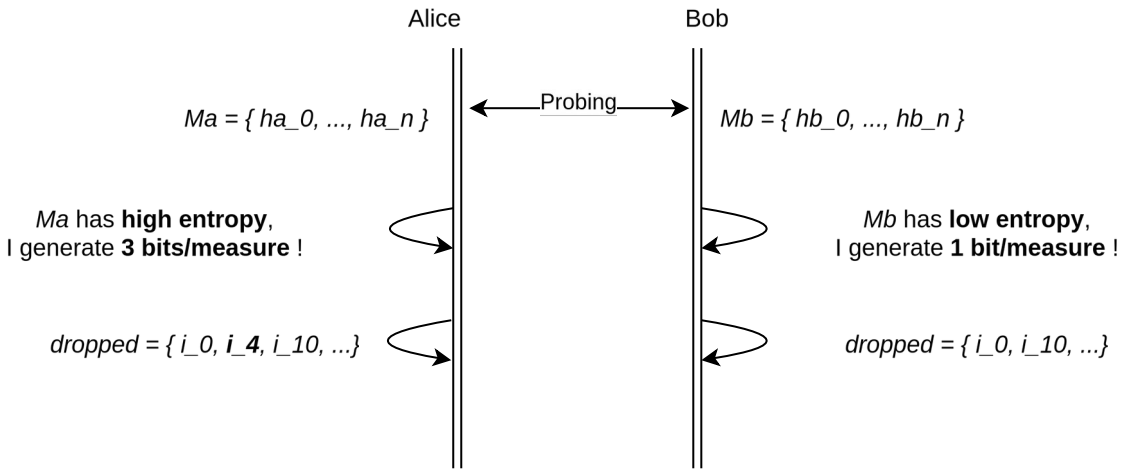
- Disagreements
- Correlation

$$\Delta = \Delta_{Physical} +$$

PHYsec – Quantization & Challenges

- different methods (Compressed Sensing, level-crossing)

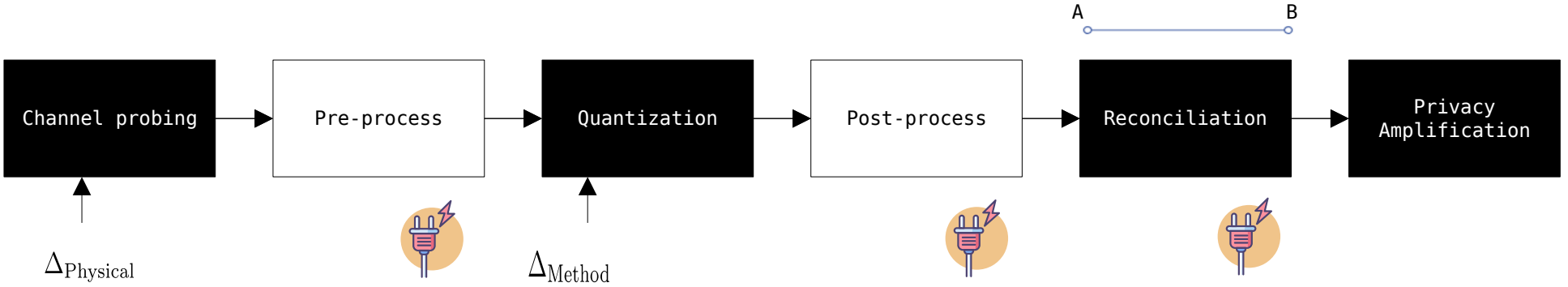
- some methods choose quantization parameters without communicating



$\Delta(Method)$

- key shift (mismatch)

PHYsec - Key Generation Procedure



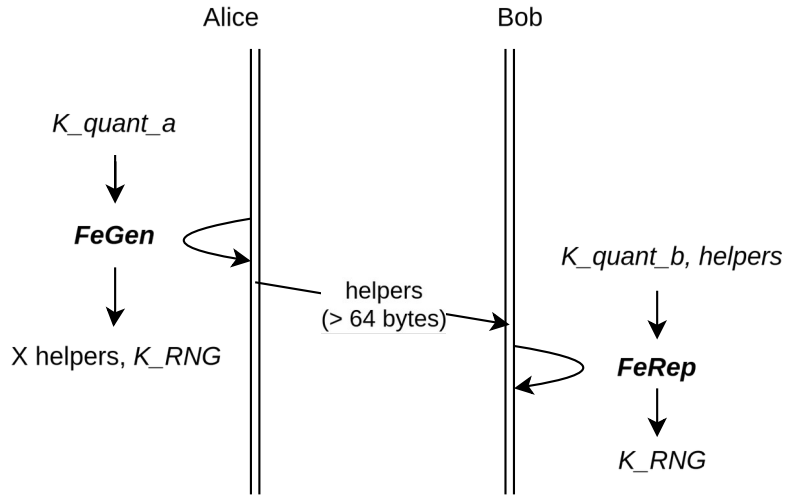
$$\Delta = \Delta_{Physical} + \Delta_{Method}$$

PHYsec – Reconciliation & Challenges

- FE can reproduce the secret (K_RNG) if K_quant_a and K_quant_b are similar

- correcting 20% err on 128 bits key => 789590193573 helpers

Fuzzy Extractors based reconciliation



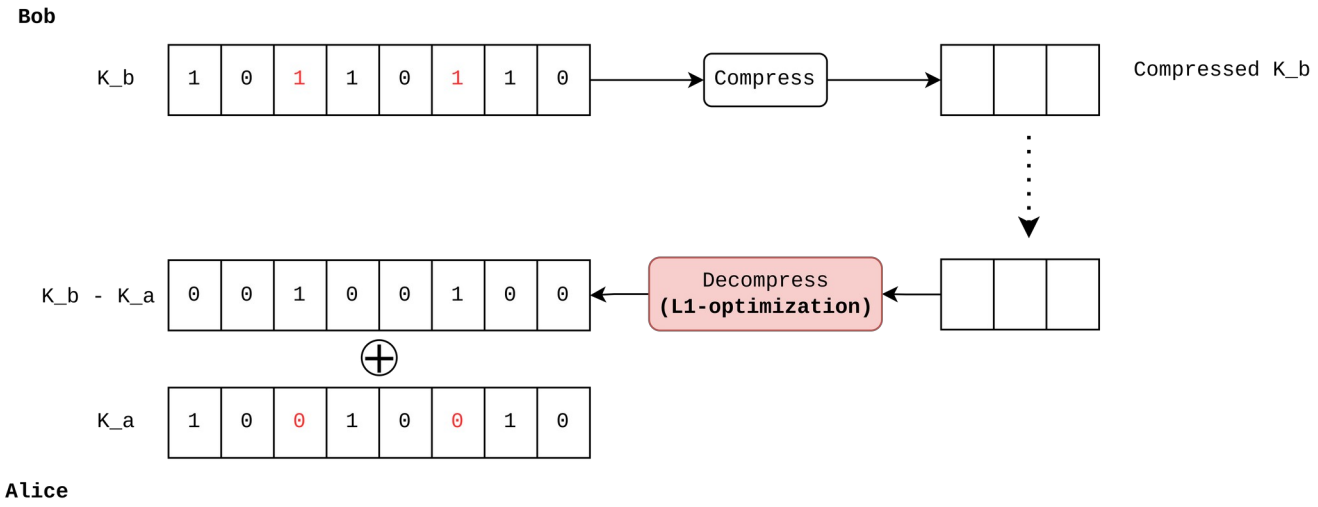
$C(Time)$

- Comms: Sending wide vectors, a lot of times, longer keygen

PHYsec – Reconciliation & Challenges

- **L1-optimization** is not implemented for low power devices

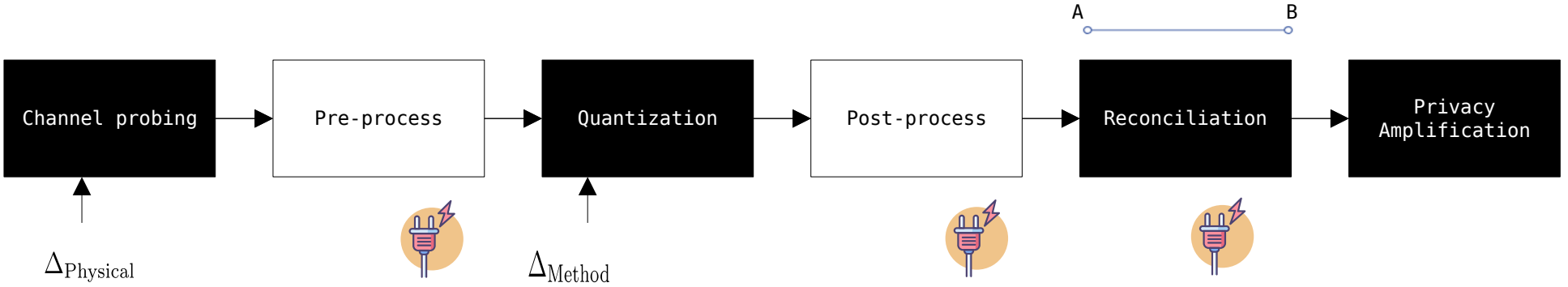
Compressed Sensing based reconciliation



$C(Time)$

- Computation: recovering (Kb-Ka) is difficult

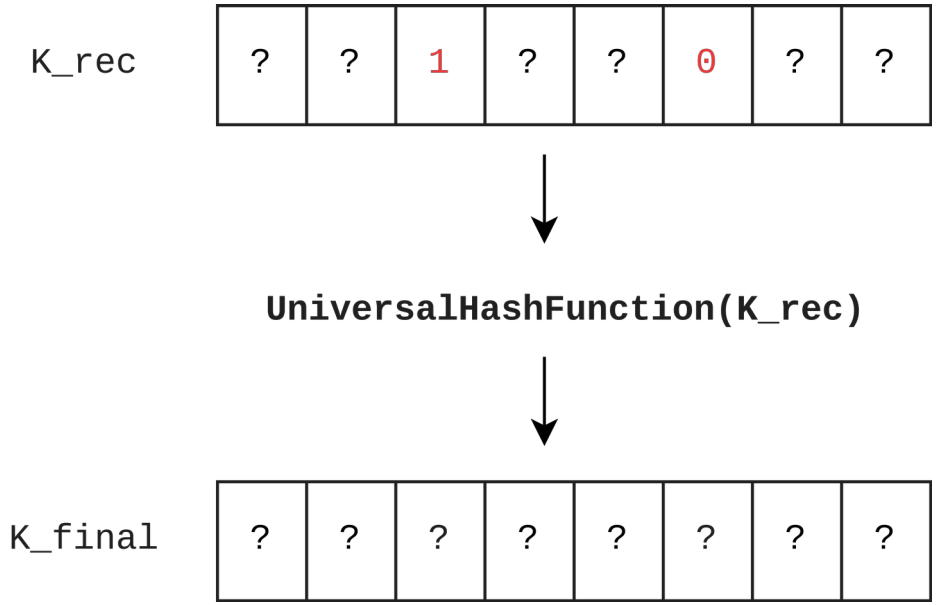
PHYsec - Key Generation Procedure



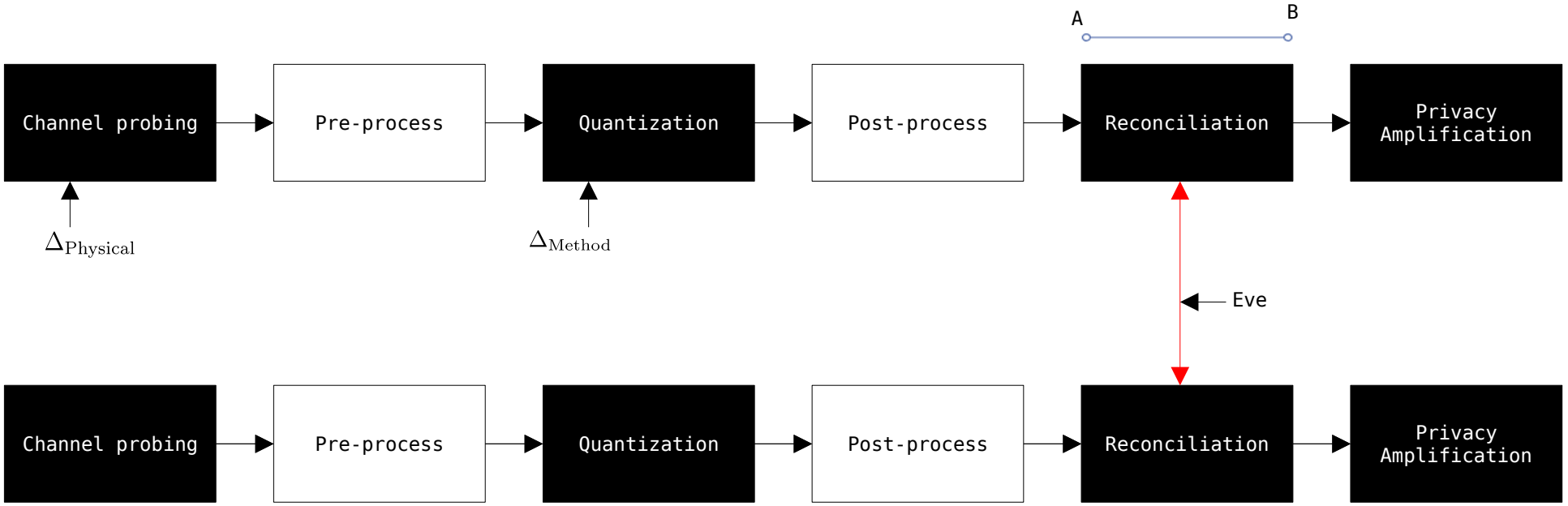
$$\Delta = \Delta_{Physical} + \Delta_{Method}$$

PHYsec – Privacy Amplification

- Distillate Eve knowledge of the K_rec key



PHYsec - Key Generation Procedure



Conclusion / Perspectives

- PHYsec could improve LPWAN security (resilience, privacy, device-to-device)

- Research challenges
  - address issues before reconciliation
  - energy efficiency

We're hiring !

Open positions (a lot) : PhDs, Postdocs, engineers !

Send mail stephane.delbruel@labri.fr