Secure processing of data issued from a connected knee prosthesis

M. PISTONO, R. BELLAFQIRA, G. COATRIEUX

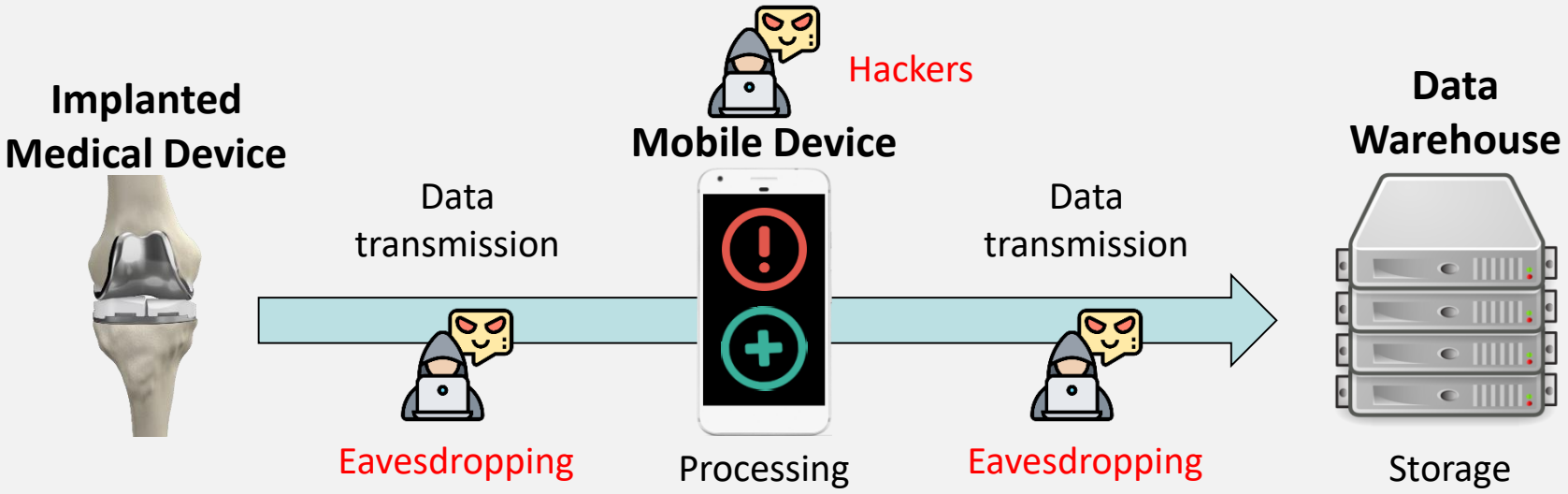
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Follow Knee

Inserm
La science pour la santé
From science to health

L@TIM

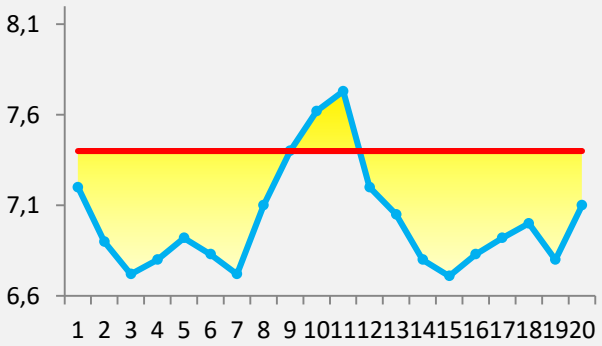
Context



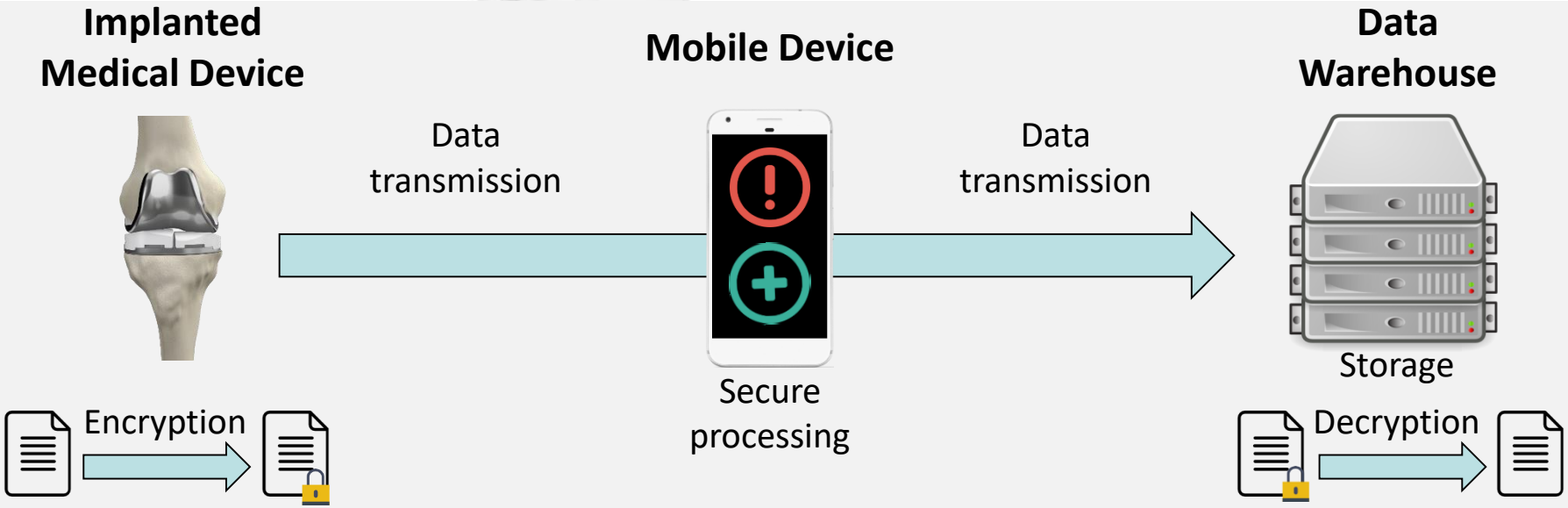
Processing: filtering and thresholding operations.

- Medical data: m_i
- Filter weights: w_i
- Threshold: S

$$\sum w_i m_i \lessgtr S$$



- **Objective**: ensure **data confidentiality** and **secure processing**.
- **Constraints**: **low computation** and **communication capabilities of IMD**.



- **Combined Linear Congruential Generator (CLCG)**: stream cipher (low complexity).

$$CLCG(m) = m + Z$$

- **Homomorphic encryption (HE)**: perform linear operations over encrypted data (high complexity).

$$HE[m_1] \times HE[m_2] = HE[m_1 + m_2] \qquad Comp(HE[m_1], HE[m_2]) = m_1 \lessgtr m_2$$

- **Cryptosystem conversion (CrC)**: from stream cipher to HE.

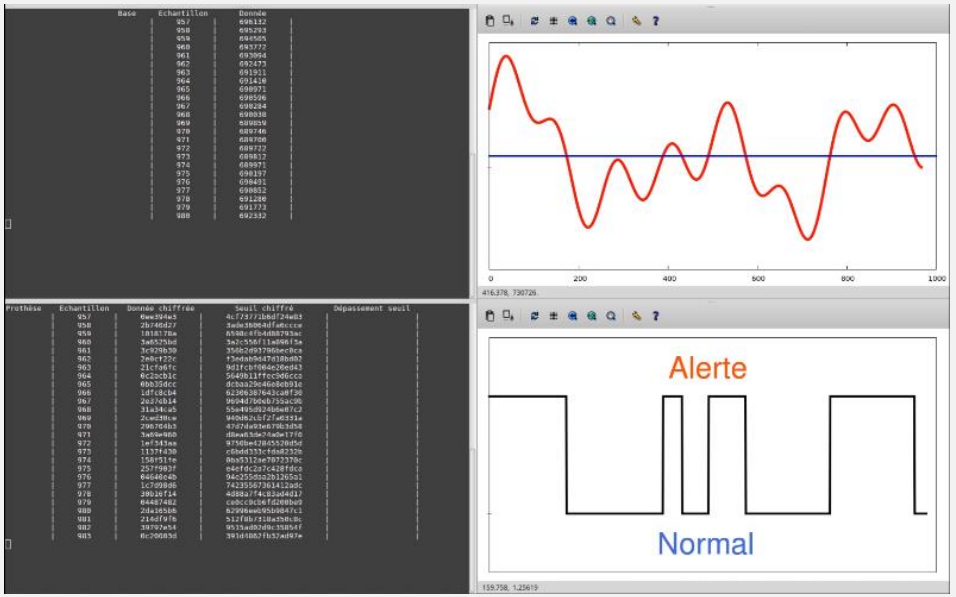
$$CLCG(m) \rightarrow \boxed{\text{CrC}} \rightarrow HE[m]$$

- **Packing**: reduce communication costs.

$$\{m_1, m_2\} \rightarrow \boxed{\text{Packing}} \rightarrow M = m_1 || m_2$$

Experimentations

- Virtual machine equipped of 1,3 GHz CPU with 1 GB memory. Equivalent to IPhone 5.
  - **125 Secure filtering operations and comparisons in less than 1 second (≈1250 samples).**



Conclusion

- We propose a new protocol which allows a honest but curious third party to process stream ciphered data issued from an IMD.
- Its originality stands on a cryptosystem conversion (CrC), secure comparison and packing.
- Our solution is practical in real application.