aviesan
alliance nationale
pour les sciences de la vie et de la santé

Institut Thématique Multi-Organismes
Technologies pour la santé

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

SECURE PROCESSING OF STREAM CIPHER ENCRYPTED DATA ISSUED FROM IOT: APPLICATION TO A CONNECTED KNEE PROSTHESIS

L@TIM

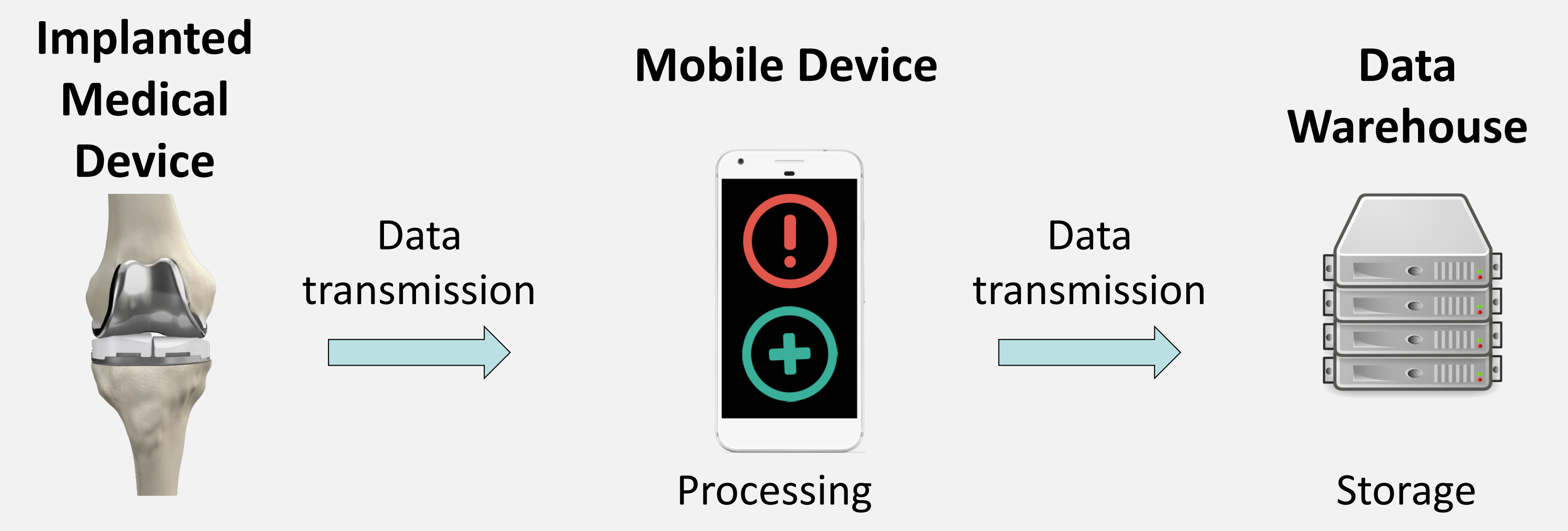
Inserm

M. Pistono[1,2], R. Bellafqira[1,2] , G. Coatrieux[1,2]

1. IMT Atlantique Bretagne Pays De La Loire, Dpt ITI, Brest 29238, France; 2. INSERM U1011, LaTIM, Brest 29238, France

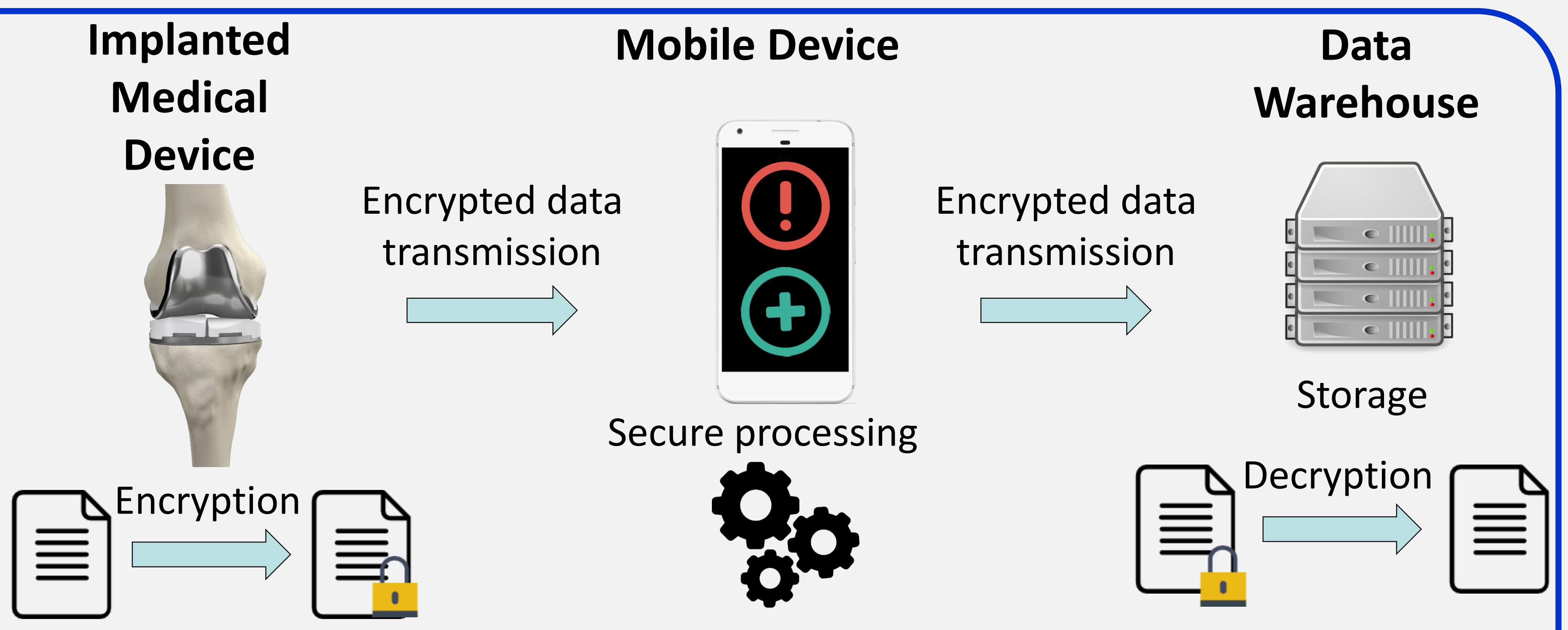
❖ Objectives/Solution/Results: Allow an honest but curious Mobile to process encrypted data issued from an Implanted Medical Device so as to raise an alarm in case of anomaly but without decrypting data / Our solution takes advantage of homomorphic encryption (HE), CLCG encryption, a cryptosystem conversion technique and a data packing strategy / We evaluate the realistic performance of our solution in the case of a connected knee prosthesis.

1. Framework



- ❖ **Main security concerns**: **confidentiality** and **privacy** of medical data.
- ❖ **Mains constraints**: low computational, memory and bandwidth capabilities of the IMD

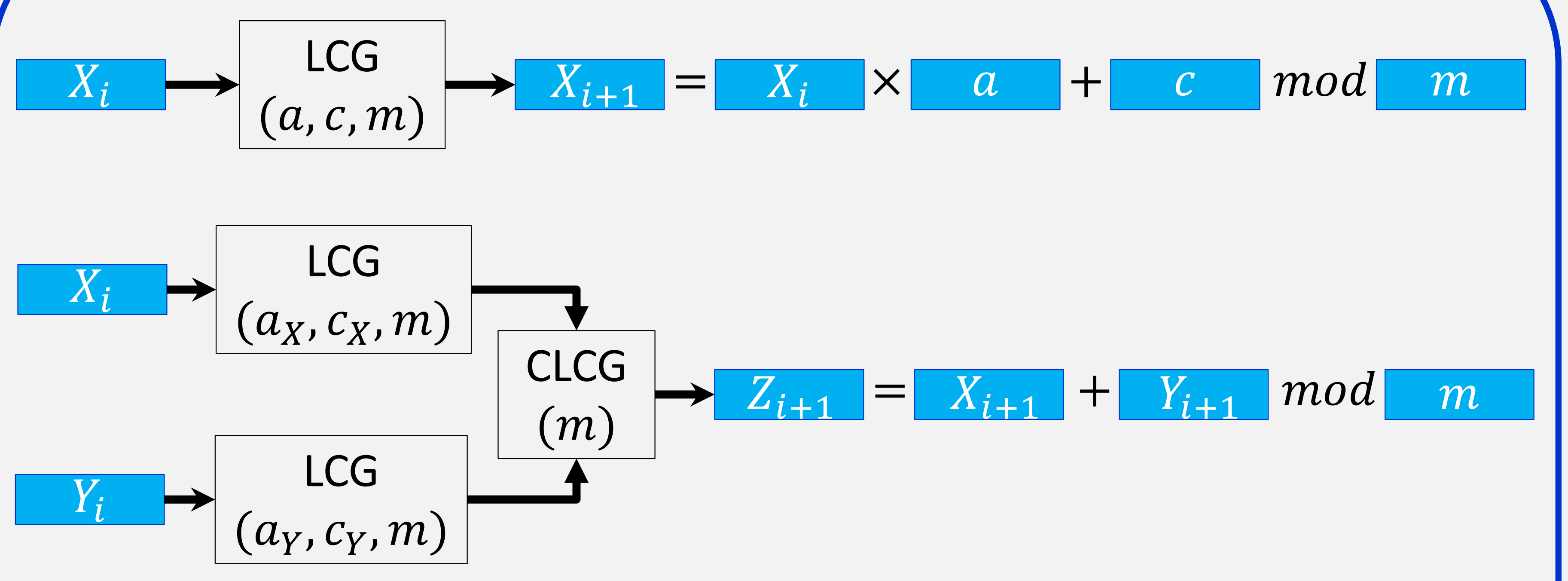
2. Secure framework



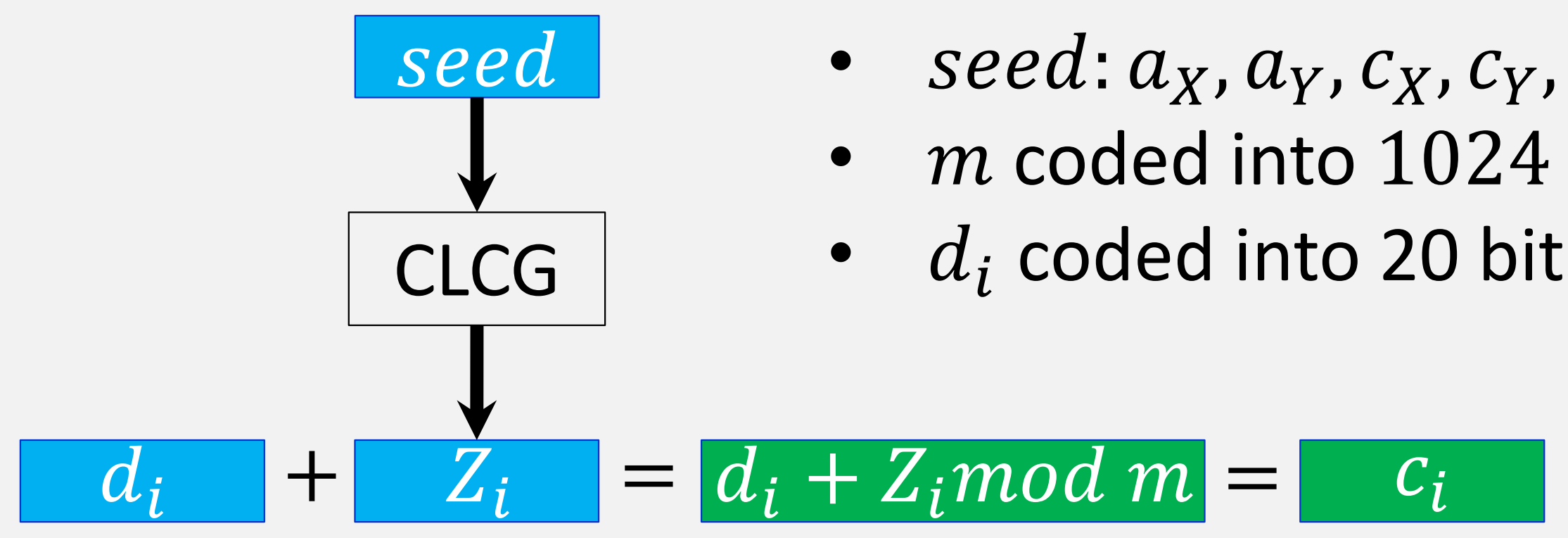
- ❖ **Solution:** Lightweight encryption, homomorphic encryption (HE) and crypto-system conversion.

3. Lightweight encryption and Packing

❖ **CLCG**: Combined linear congruential generator

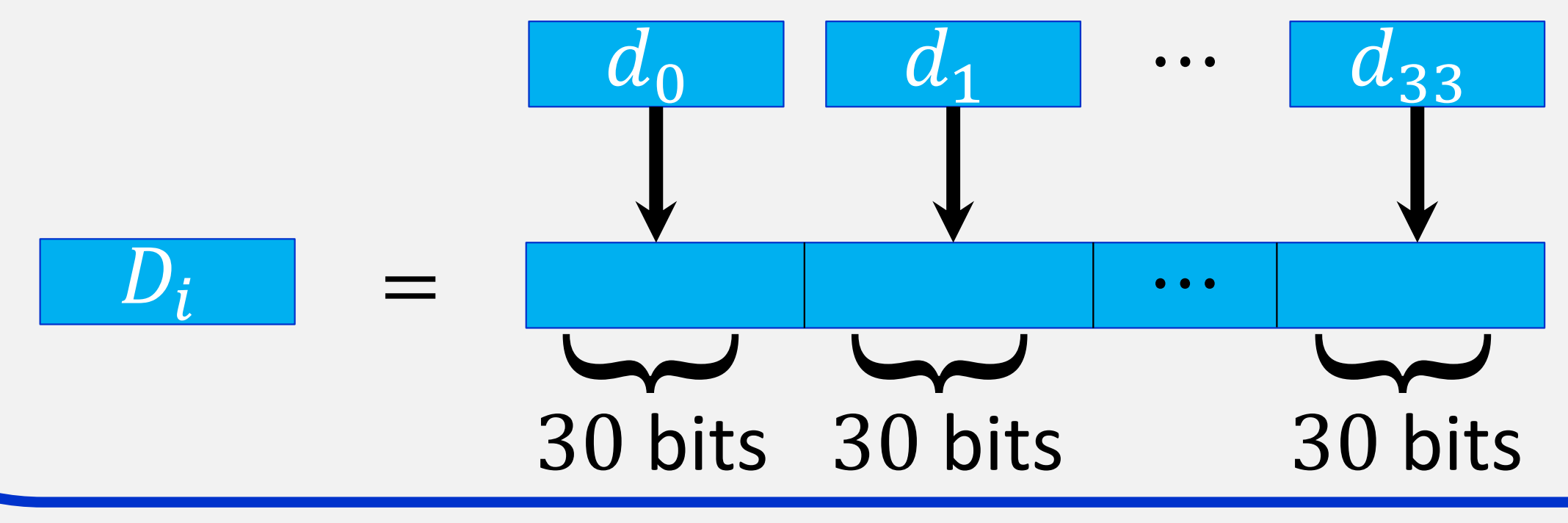

X_i
LCG
(a,c,m)
$X_{i+1} = X_i \times a + c \; mod \; m$
X_i
LCG
(a_X, c_X, m)
Y_i
LCG
(a_Y, c_Y, m)
CLCG
(m)
$Z_{i+1} = X_{i+1} + Y_{i+1} \; mod \; m$

❖ **CLCG encryption**: **Secure data transmission**



- $seed: a_X, a_Y, c_X, c_Y, X_0, Y_0, m.$
- m coded into 1024 bits.
- d_i coded into 20 bits.

❖ **Packing strategy**: **Reduce communication cost**



- $D_i = \sum_{i=0}^{33} d_i 2^{30i}$

4. Cryptosystem conversion & Secure data processing

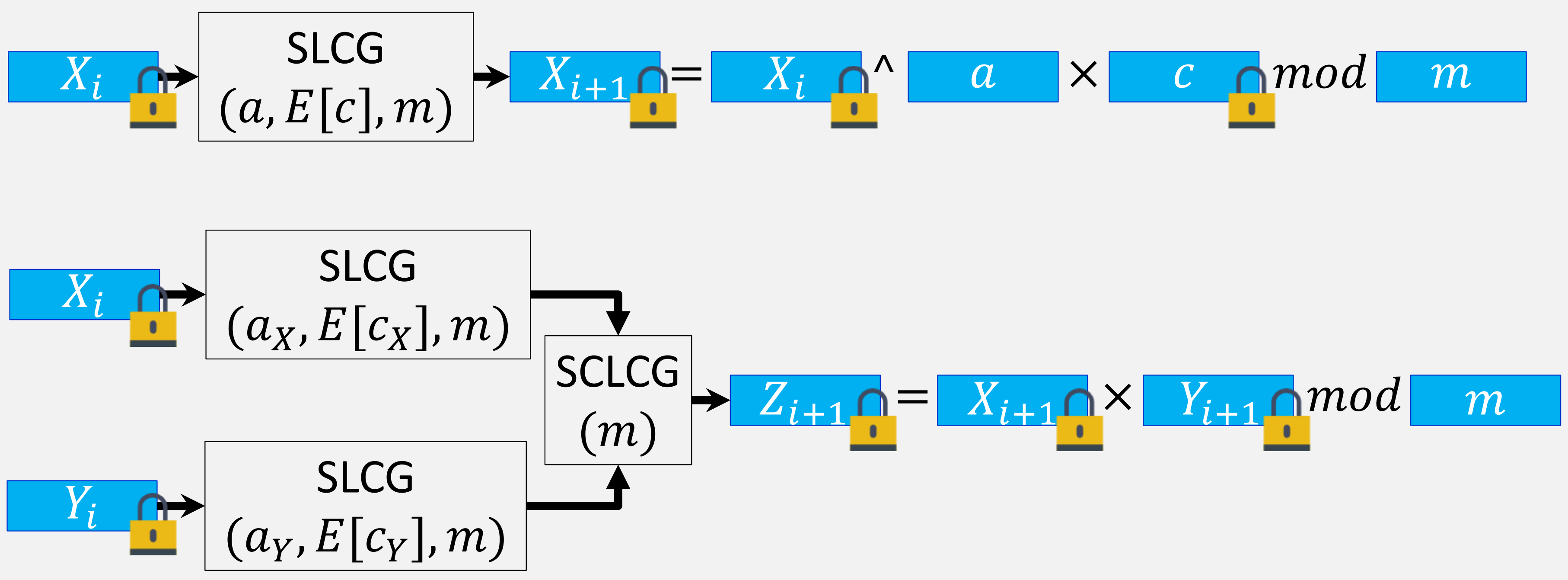
❖ **HE Damgard-Jurik cryptosystem properties**:

1) $E[m_1, r_1]E[m_2, r_2] = E[m_1 + m_2, r_1 r_2]$ 2) $E[m_1, r_1]^{m_2} = E\left[m_1, r_1^{m_2}\right]$

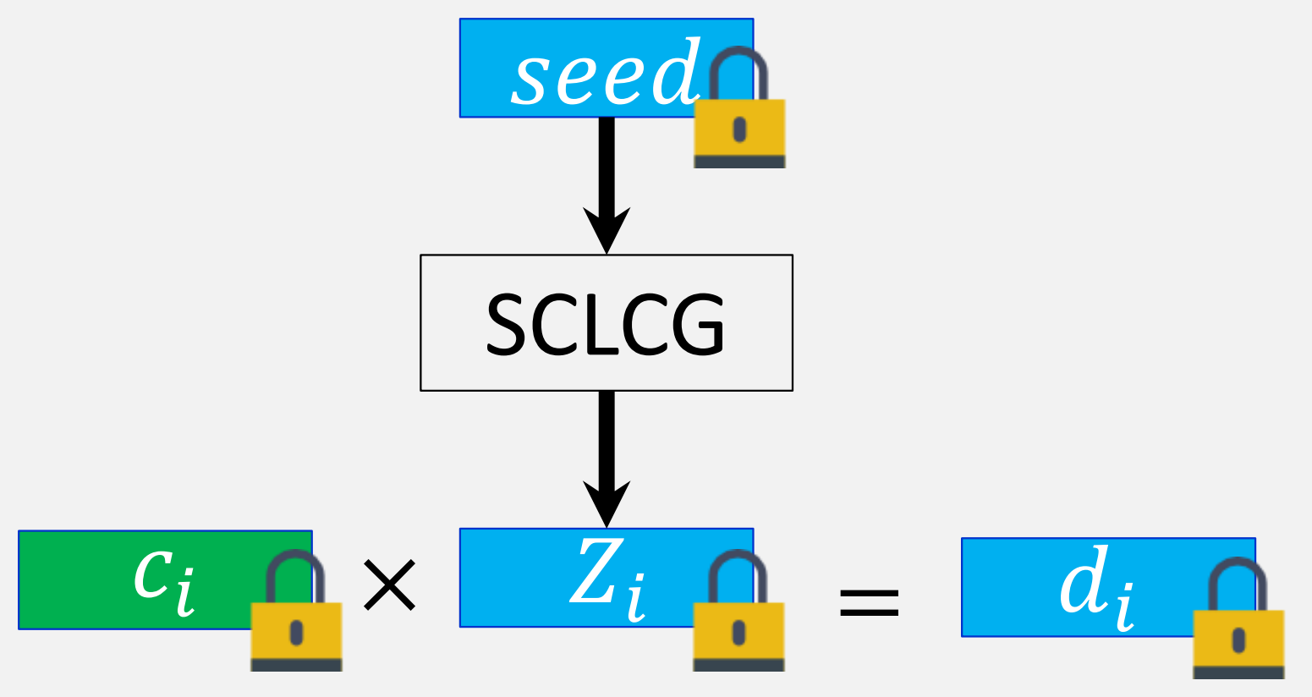
3) $F(E[m_1, r], E[m_2, r]) = m_1 - m_2$

- $E[d_i, r] =$ d_i

❖ **Secured CLCG (in the encrypted domain):**


X_i
SLCG
$(a, E[c], m)$
$X_{i+1} = X_i$ ^ $a \times c \; mod \; m$
X_i
SLCG
$(a_X, E[c_X], m)$
Y_i
SLCG
$(a_Y, E[c_Y], m)$
SCLCG
(m)
$Z_{i+1} = X_{i+1} \times Y_{i+1} \; mod \; m$

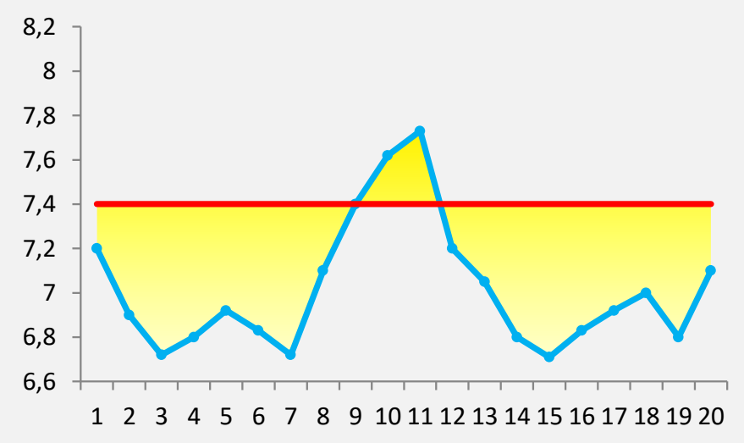
❖ **Cryptosystem conversion:**



❖ **Secure data filtering & tresholding**:

$$\sum_i w_i d_i \lessgtr S$$

Filtering weights: w_i



$F(\sum w_i d_i , S) = \sum w_i d_i - S$

$\sum w_i d_i = \prod_{i=0}^{10}(d_i$ ^ $w_i)$

Objective: secure monitoring of patient

5. Experimental simulation

❖ Experimental conditions/results: We simulate Mobile with a virtual machine equipped of one 1,3 Ghz CPU and 1GB memory (equivalent to IPhone 5). The prosthesis has 34 sensors and uses our packing strategy. Finally the Mobile filtering weights are of length 10 bits.

❖ Experimental results: 125 secure data filtering and tresholding operations can be made in less than 1 second.

6. Conclusion and future works

❖ Conclusion: We propose an original cryptosystem conversion strategy which allows the conversion of CLCG encrypted data into homomorphically Damgard-jurik encrypted data. Using CLCG encryption severely reduces computation complexity in the prosthesis while HE encryption makes possible to process data by a mobile device, like a smartphone. In order to gain in performance, we have introduced a new packing strategy. This one drastically diminishes communication costs. Beyond the fact our solution is practical in real application contrarily to the state of the art solutions based on fully homomorphic cryptosystem, the protocol presented in this work can be implemented in any IOT (Internet Of Things) devices that has enough capability to implement a CLCG cryptosystem.

❖ Future Work: Enforce security assumption by considering Mobile as a malicious adversary instead of as honest but curious.

[1] Bellafqira Reda et al., Proxy Re-Encryption Based on Homomorphic Encryption. *Proceedings of the 33rd Annual Computer Security Applications Conference*

[2] Damgård, Ivan and Jurik, Mads, A Length-Flexible Threshold Cryptosystem with Applications. *Information Security and Privacy*

11ème journées ITS – 2 & 3 octobre 2019 – Rennes – https://its.aviesan.fr

Contact: {maxime.pistono, reda.bellafqira, gouenou.coatrieux}@imt-atlantique.fr - https://www.imt-atlantique.fr/fr