FONDEMENT DES SYSTÈMES NUMERIQUES

SPACES: Security evaluations of Physically Attacked Cryptoprocessors in Embedded System

Program: ANR/JST-2010

AGENCE NATIONALE DE LA RECHERCHE ANR

SPACES

Security evaluation of Physically Attacked Cryptoprocessors in Embedded Systems

PROJECT OBJECTIVES

Aims to establish a novel security-evaluation methodology to assess crypto-modules in embedded systems, precisely:

1. Study and develop a trustworthy **SPACES Simulator** for evaluating crypto-circuits against side-channel attacks before their fabrication.
2. Develop **evaluation platforms** for validation: FPGA/smartcard platform + ASIC prototype chip.
3. Study of new attacks for a better **understanding of leakages and faults**, in particular by the ElectroMagnetic channel.

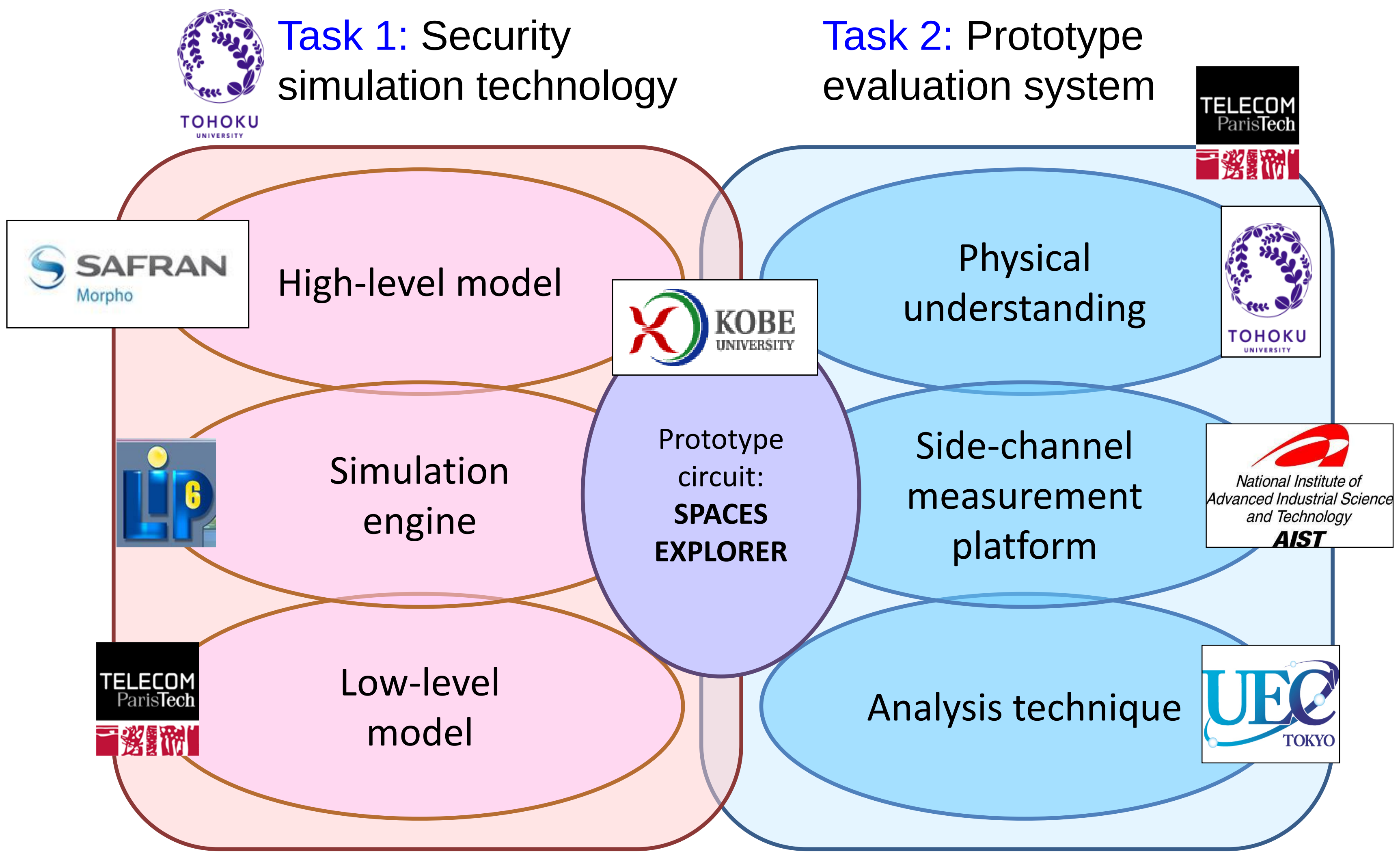
Task 1: Security simulation technology
Task 2: Prototype evaluation system
TOHOKU UNIVERSITY
SAFRAN Morpho
High-level model
LIP6
Simulation engine
TELECOM ParisTech
Low-level model
KOBE UNIVERSITY
Prototype circuit: SPACES EXPLORER
Physical understanding
Side-channel measurement platform
Analysis technique
TELECOM ParisTech
TOHOKU UNIVERSITY
National Institute of Advanced Industrial Science and Technology AIST
UEC TOKYO

Fig 1: Project structure

METHODOLOGY and RESULTS

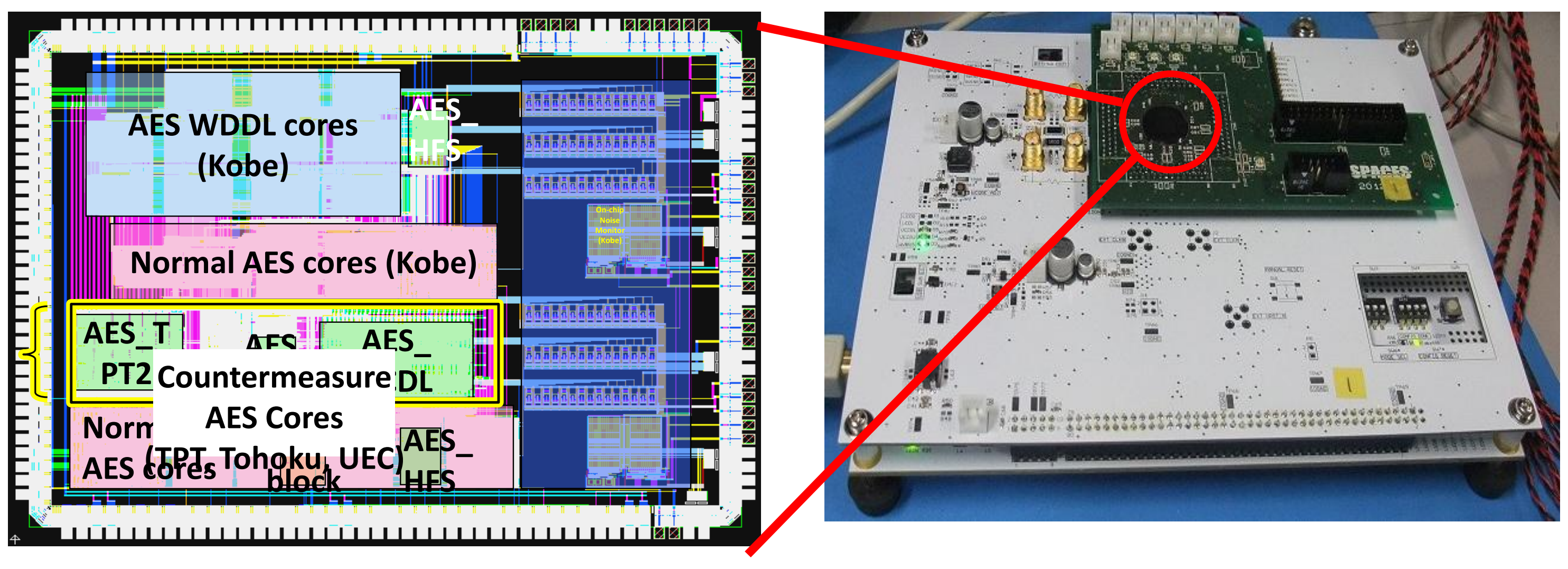

Fig 2: SPACES Explorer mounted on SASEBO-W

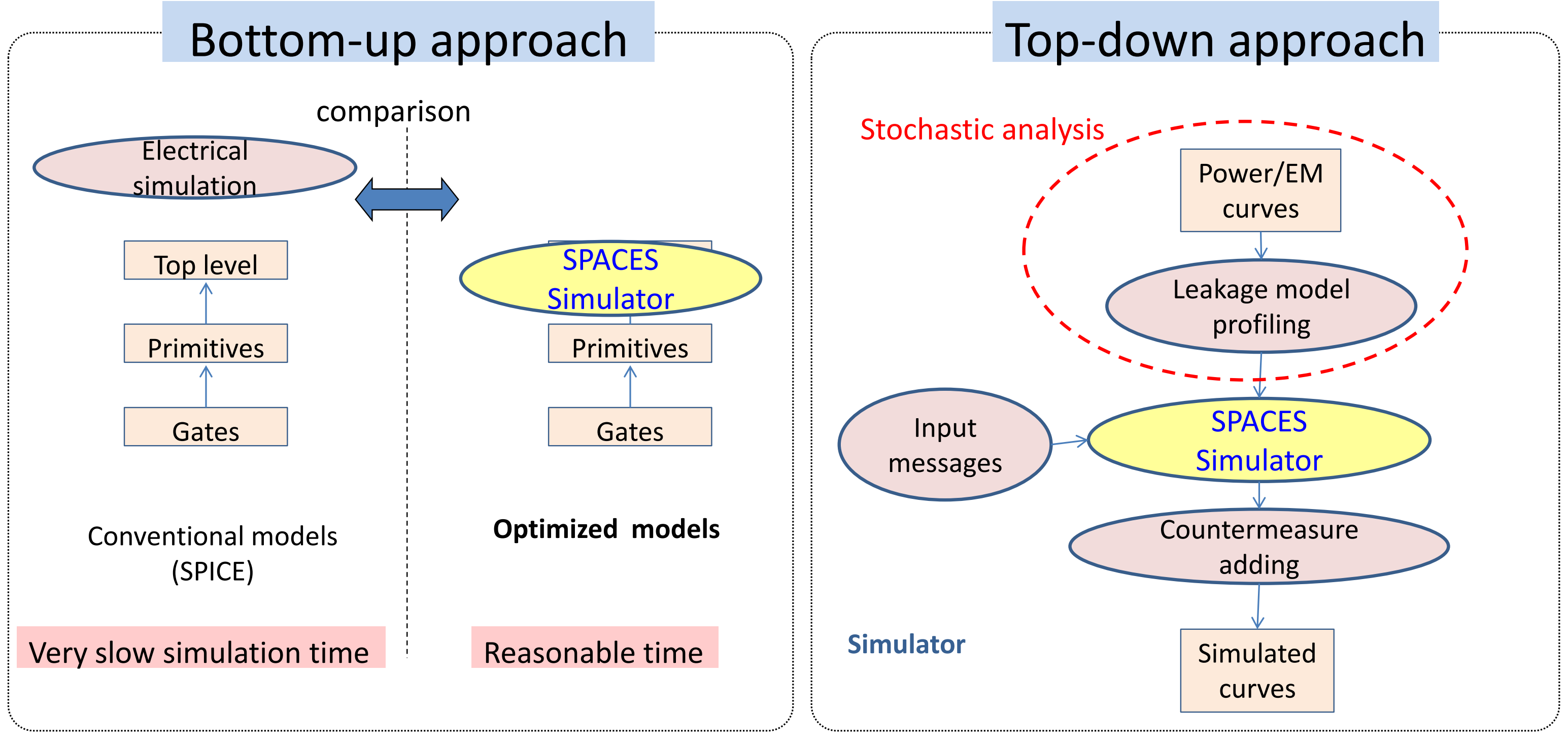

Fig 3: Simulation approaches

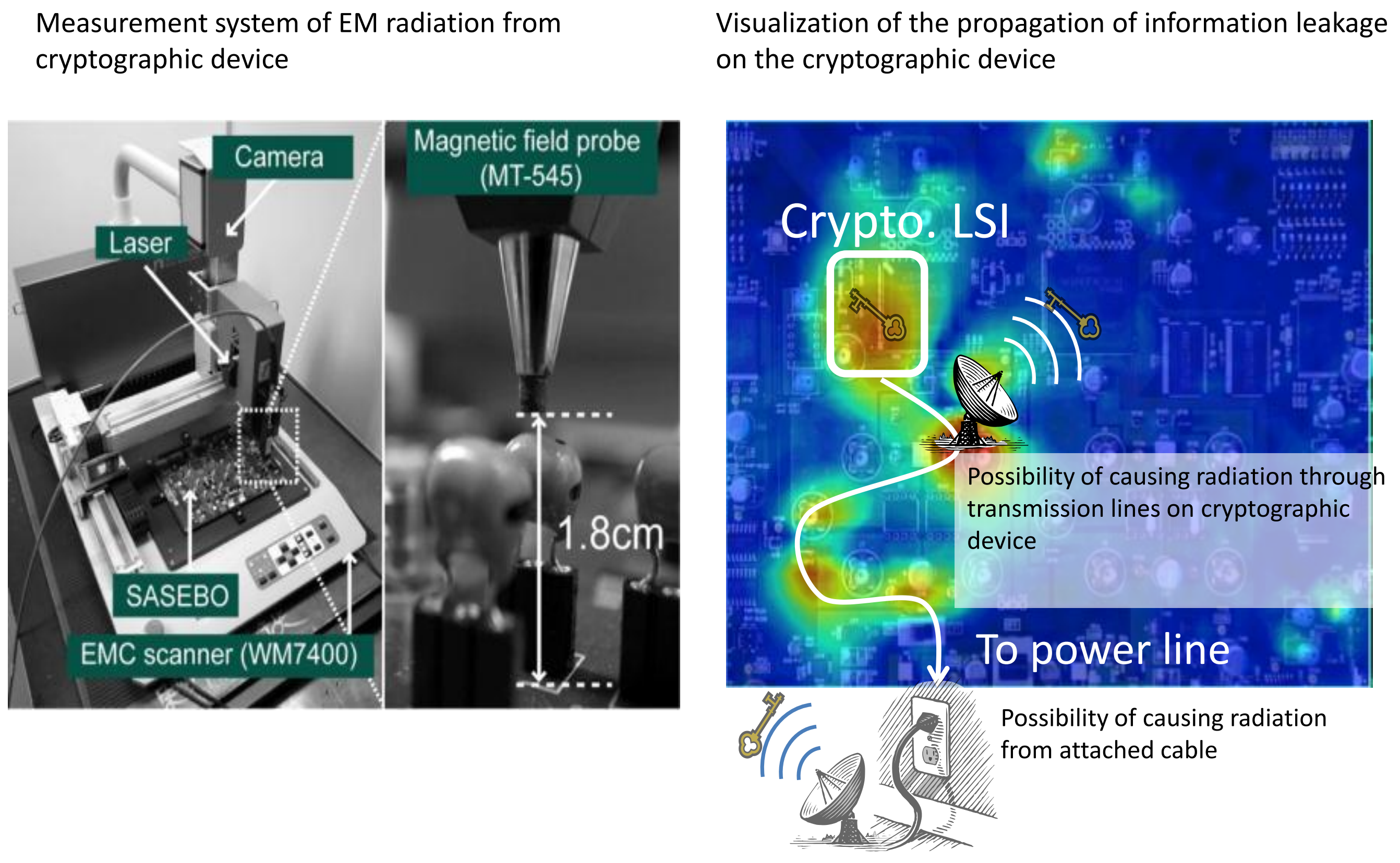
Measurement system of EM radiation from cryptographic device
Visualization of the propagation of information leakage on the cryptographic device
Camera
Laser
SASEBO
EMC scanner (WM7400)
Magnetic field probe (MT-545)
1.8cm
Crypto. LSI
Possibility of causing radiation through transmission lines on cryptographic device
To power line
Possibility of causing radiation from attached cable

Fig 4: EM Analysis platform

The following results have been obtained:

1. A prototype chip **"SPACES Explorer" successfully taped-out and tested** with 20 crypto-cores in TSMC 65nm technology
2. A new FPGA board **SASEBO-W** for smartcard and prototypes evaluation against side-channel attacks
3. A functional **High-speed Simulator** for side-channel assessment
4. An **EM analysis platform** for both side-channel and fault attack understanding
5. A new attack type study: **Fault Sensitivity Analysis**

CONCLUSIONS AND PERSPECTIVES

- Very close collaboration between french/japonese partners
- Many results: prototypes, software tools, new attacks, international publications(>20)
- SPACES explorer functionally tested, under security evaluation
- Perspectives to continue with the same team in another framework

COORDINATORs: Télécom Paristech, Tohuku University
JST PARTNERS: Tohoku University, Kobe University, UEC, AIST
ANR PARTNERS: Télécom Paristech, Paris 6 (LIP6), Safran Morpho

SPACES

Security evaluation of Physically Attacked Cryptoprocessors in Embedded Systems

http://spaces.enst.fr

CONTACT :
danger@telecom.paristech.fr
homma@aoki.ecei.tohoku.ac.jp

TELECOM ParisTech · LIP6 · SAFRAN Morpho · National Institute of Advanced Industrial Science and Technology AIST · TOHOKU UNIVERSITY · KOBE UNIVERSITY · UEC TOKYO

LES RENCONTRES DU NUMÉRIQUE
17 et 18 avril 2013