



**HAL**  
open science

# Side-Channel Analysis of Post-Quantum Cryptography

Tania Richmond, Annelie Heuser, Benoit Gérard

► **To cite this version:**

Tania Richmond, Annelie Heuser, Benoit Gérard. Side-Channel Analysis of Post-Quantum Cryptography. SecDays 2019 - Security Days, Jan 2019, Rennes, France. pp.1. hal-02018859

**HAL Id: hal-02018859**

**<https://inria.hal.science/hal-02018859v1>**

Submitted on 14 Feb 2019

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

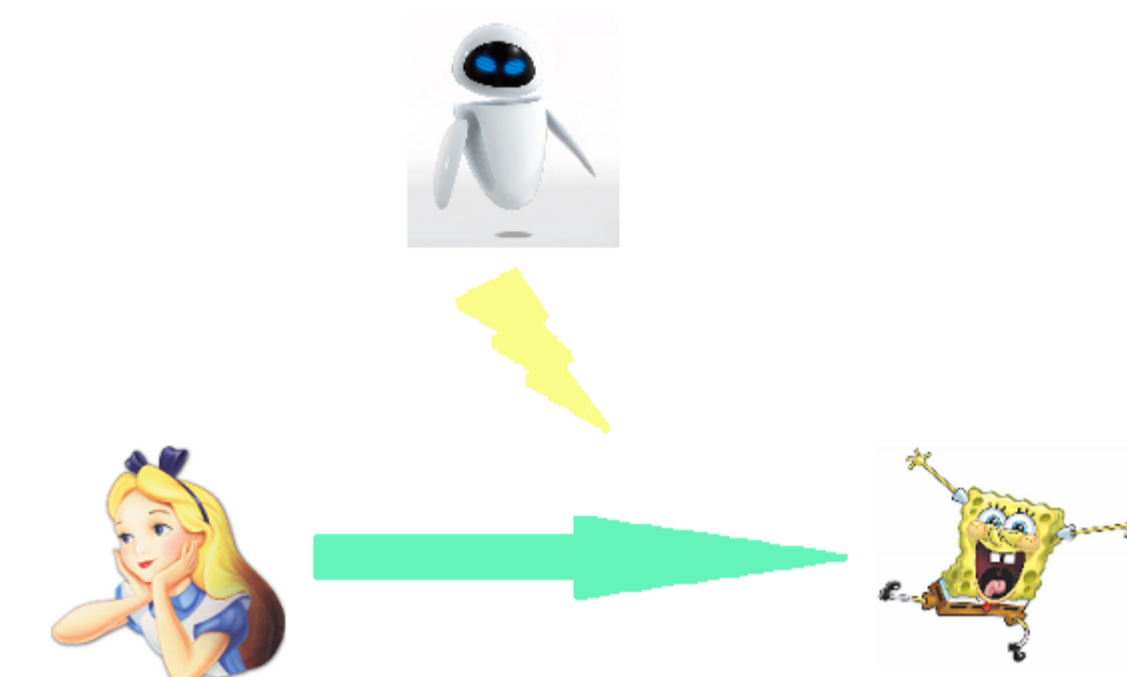
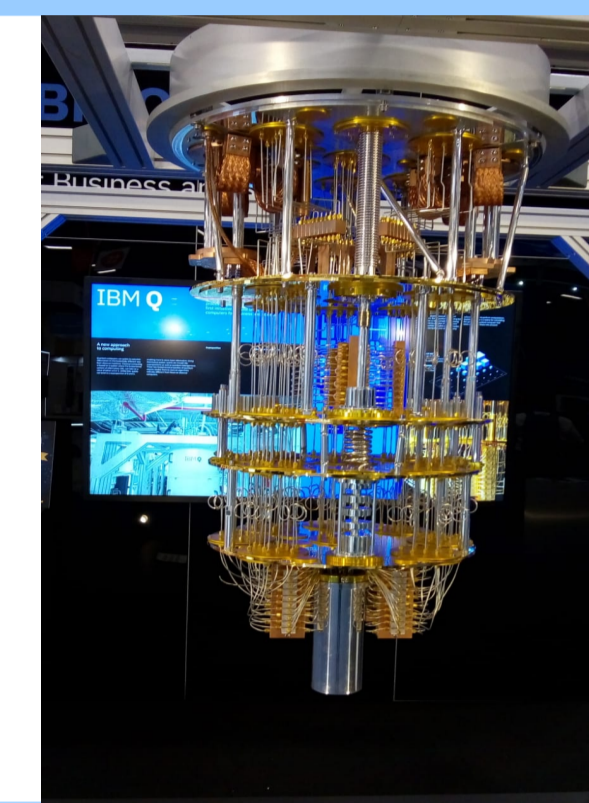
L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Side-Channel Analysis of Post-Quantum Cryptography

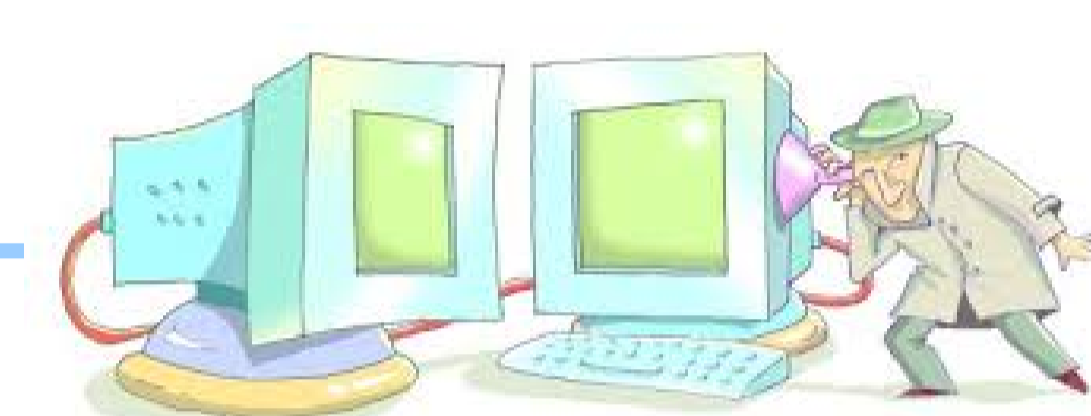
Tania RICHMOND, Annelie HEUSER, Benoît GÉRARD  
Univ Rennes, Inria, CNRS, IRISA, Rennes, France



**Context:** Quantum Computer is coming!  
Quantum secure communication is needed.  
NIST standardization is happening now.

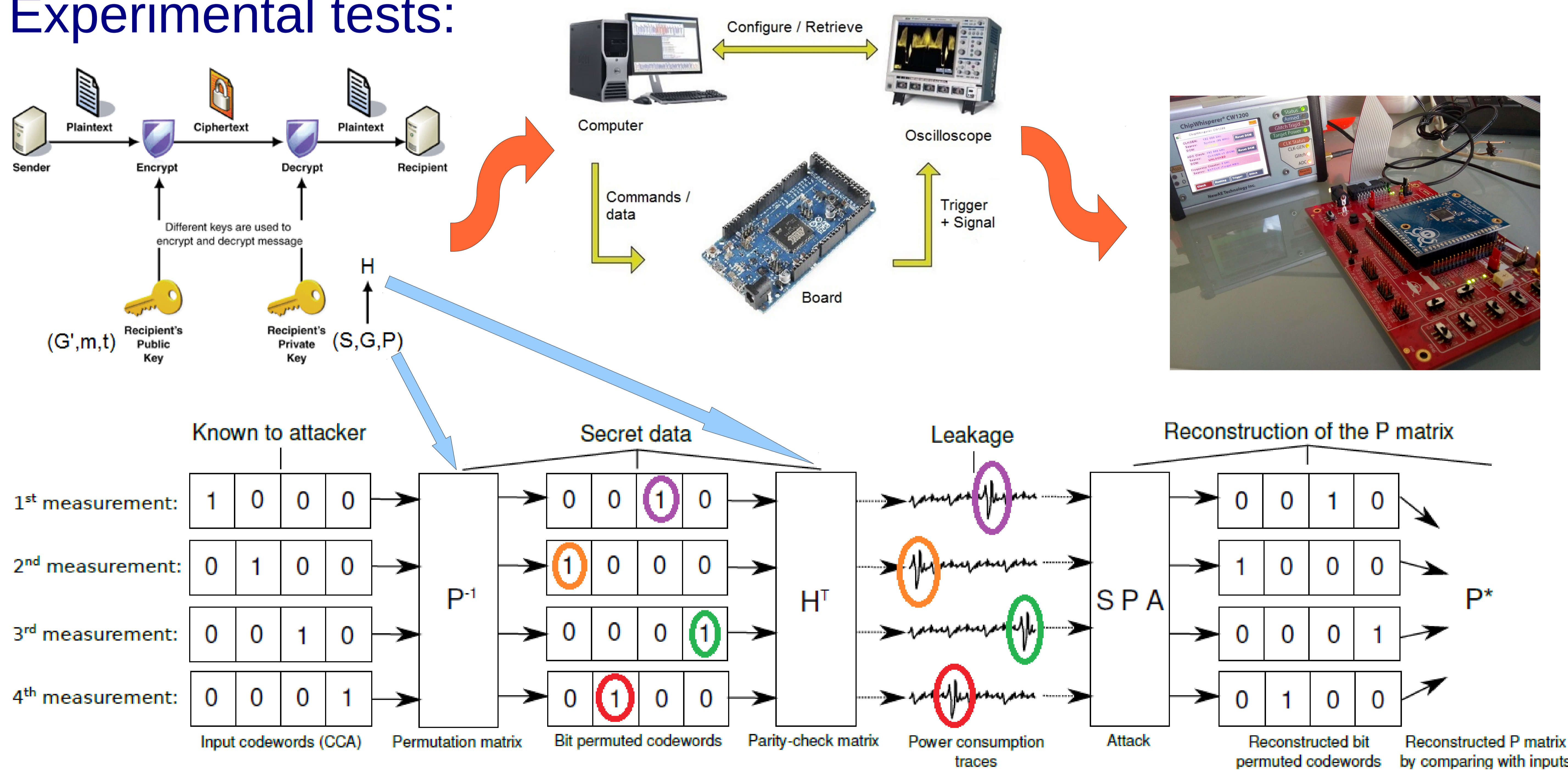


**Goals:** Side-channel analysis of NIST candidates/schemes



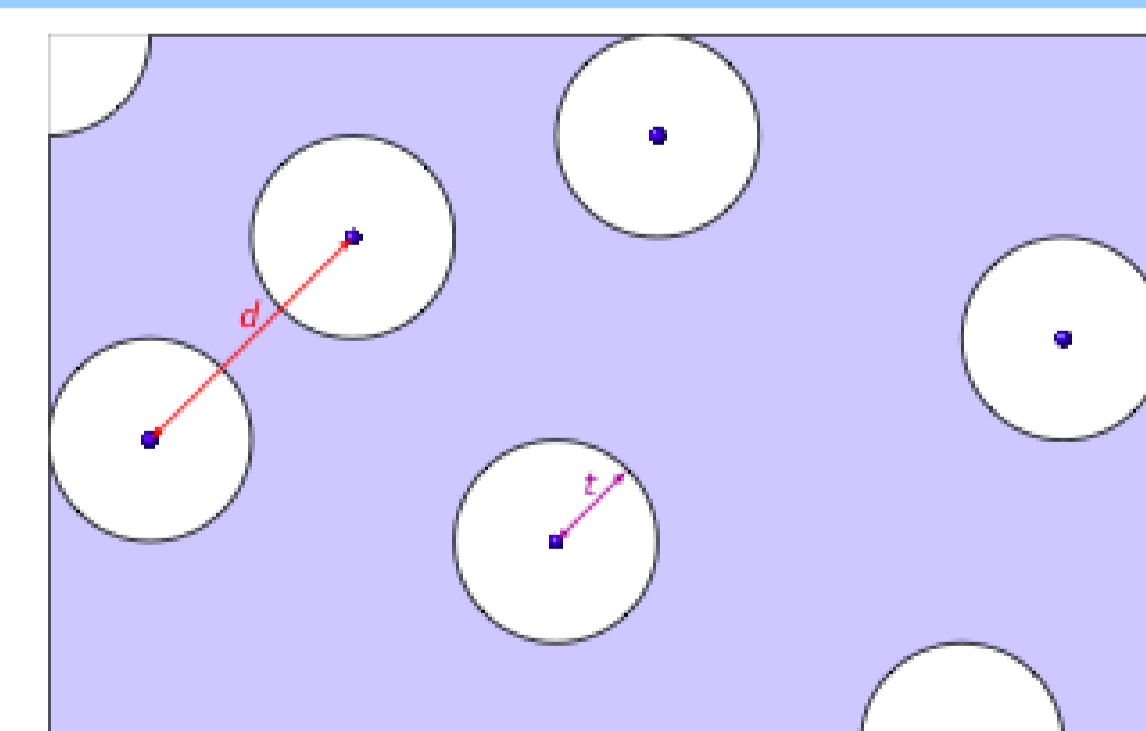
**How?** Finding theoretical leakages in Time/Power/EM:  
interactions between Maths (Number Theory, Probabilities/Statistics),  
Computer Science (Programming) and Electronics (Embedded Devices).

**Experimental tests:**



**Current focus: Code-Based Cryptography**

- McBits, QcBits;
- BIKE, QC-MDPC KEM, RankSign.



**Perspectives:** Enhancing the security of post-quantum secure cryptographic protocols by improving resilience against SCA.

**References:**

<https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions>

Tania Richmond. *Secure implementation of cryptographic protocols based on error-correcting codes*. PhD dissertation (in French), Université Jean Monnet, Saint-Etienne (France), October 2016.

