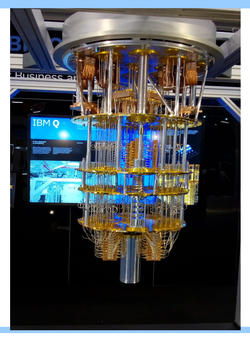
Side-Channel Analysis of Post-Quantum Cryptography

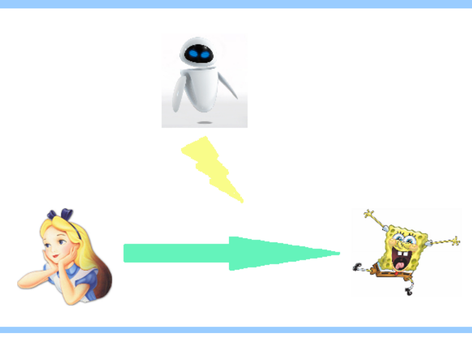
Tania Richmond, Annelie Heuser, Benoit Gérard

Side-Channel Analysis of Post-Quantum Cryptography

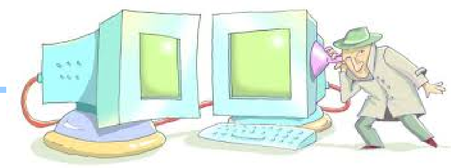
Tania RICHMOND, Annelie HEUSER, Benoît GÉRARD
Univ Rennes, Inria, CNRS, IRISA, Rennes, France

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



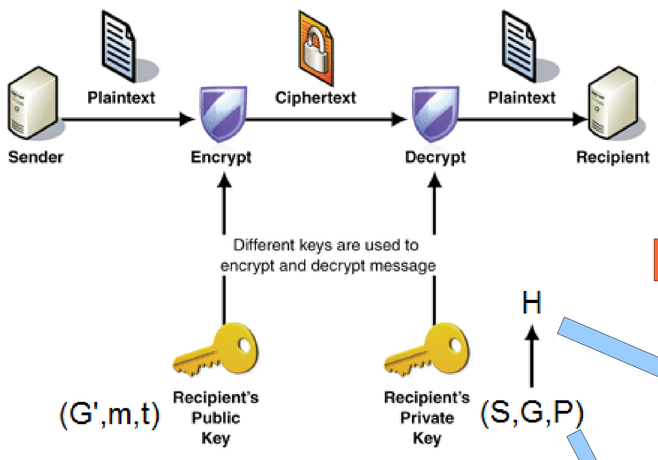


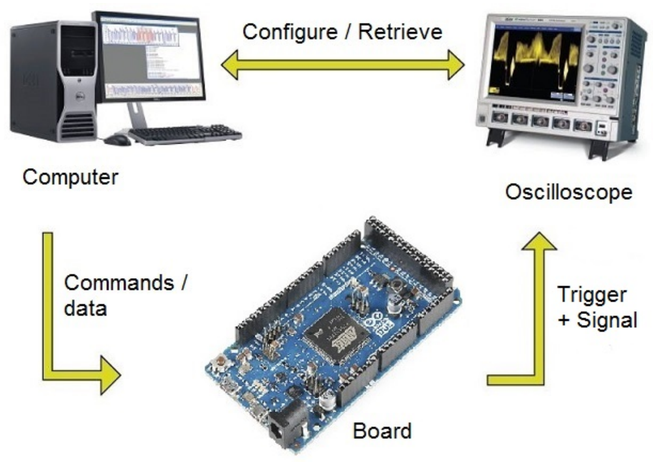
Goals: Side-channel analysis of NIST candidates/schemes

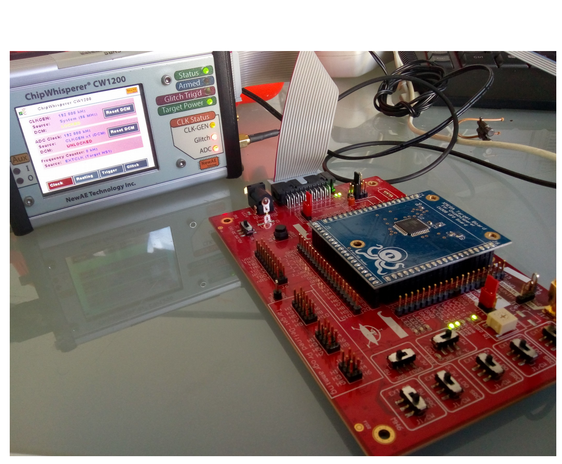


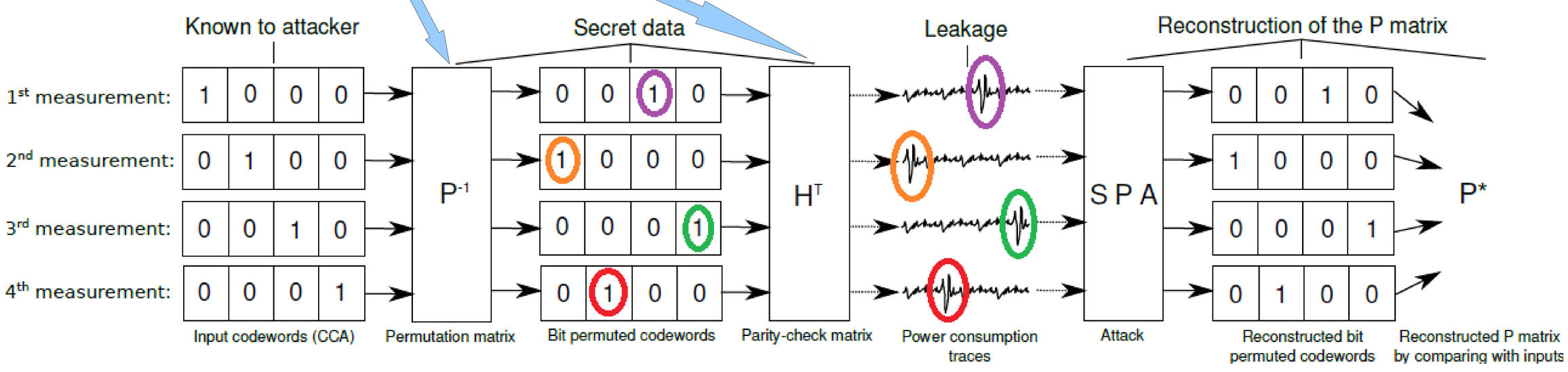
How? Finding theoretical leakages in Time/Power/EM: interactions between Maths (Number Theory, Probabilities/Statistics), Computer Science (Programming) and Electronics (Embedded Devices).

Experimental tests:



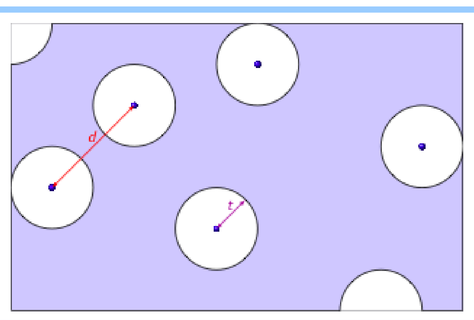






Current focus: Code-Based Cryptography

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



Perspectives: Enhancing the security of post-quantum secure cryptographic protocols by improving resiliance 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.