Code-based cryptography: A way to secure communications

Tania Richmond, Pierre-Louis Cayrel, Viktor Fischer

▶ **To cite this version:**

Tania Richmond, Pierre-Louis Cayrel, Viktor Fischer. Code-based cryptography: A way to secure communications. womENcourage 2015, Sep 2015, Uppsala, Sweden. hal-02018870

HAL Id: hal-02018870
https://inria.hal.science/hal-02018870v1

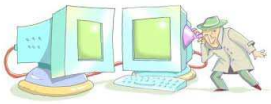
Submitted on 14 Feb 2019

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.

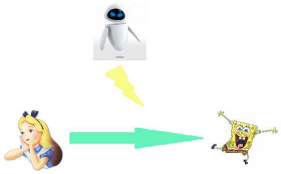
L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Code-based cryptography: A way to secure communications

Tania RICHMOND, Pierre-Louis CAYREL, Viktor FISCHER
tania.richmond@univ-st-etienne.fr



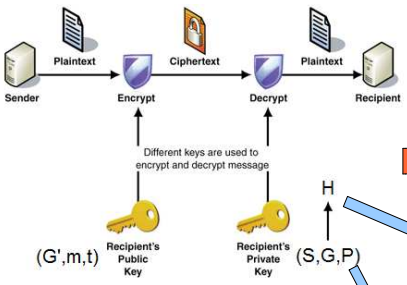
Context: Make secure communications.

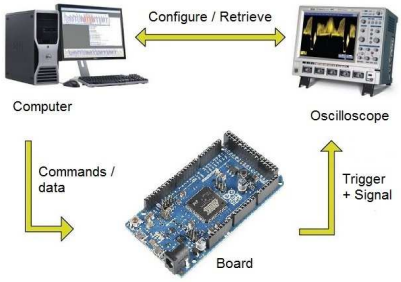


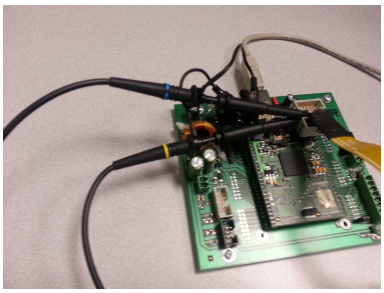
Objectives: Find an alternative to currently used methods in cryptography in order to avoid side-channel attacks.

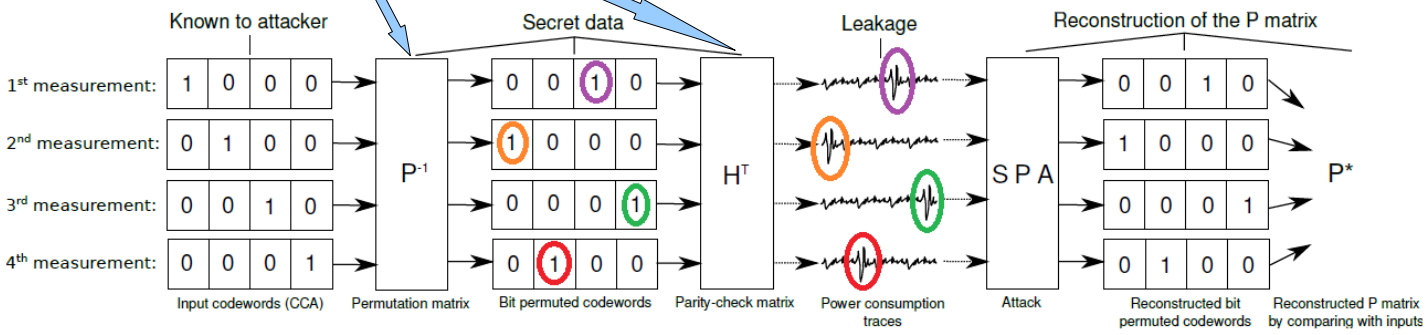
How? Implementing existing protocols and testing side-channel attacks. Then find mathematical methods to make them more secure.

Experiments:









Solution: Maintain all multiplications (also by zero) in order to avoid differences between processing zeros and ones.

Conclusion: We improved security of cryptographic protocols making them more resilient against side-channel attacks.

Perspectives: Provide a complete and secure implementation.

Publications:

M. Petrvalsky, T. Richmond, M. Drutarovsky, P.-L. Cayrel and V. Fischer. *Countermeasure against the SPA Attack on an Embedded McEliece Cryptosystem.* Accepted in MAREW 2015.

V. Dragoi, P.-L. Cayrel, B. Colombier and T. Richmond. *Polynomial structures in code-based cryptography.* In Progress in Cryptology - INDOCRYPT 2013, pp. 286-296, Springer International Publishing.