Secure implementation of post-quantum cryptography

SPS 984520

Presenters:
Karol Nemoga, NATO Evaluator

September 7, 2014, TAU

Evaluation criteria

discussion framework

- Objectives and workplan
- Project implementation and results
- Resources
- Impact
- End users
- Communication
- Young scientists
- Hihglights/strong aspects of the projects

Objectives and workplan 1

- Has the project made satisfactory technical progress?

  Publications: 8 (all partners)

  - RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis (strong public/scientific/technical impact)
  - 2 presentations/papers on CHES 2014, Korea, September 2014

-

Objectives and workplan 2

Has planned milestones and deliverables been achieved?

- Step 1 (T0 - T0+6).
- Milestone M 1.1 Project setup, equipment ordering, (T0 - T0+6), did not finished yet
  - SK Reconfigurable SoC evaluation boards - partially, PC ok
  - IS oscillosope - not realised yet, urgent
  - US PC – in 14 days
  - F Reconfigurable SoC evaluation boards, Quartus II license and a high-end PC not realised yet, urgent
- Milestone M 1.2 Kick-off Meeting o.k.
- **Deliverables:**
- D 1.1 Project WEB site o.k.

Objectives and workplan 3

Has planned milestones and deliverables been achieved?

- Step 2 (T0 - T0+9). … realization of selected algorithms in software … will be presented
- M 2.1 – Software implementations
- **Deliverables:**
- D 2.1 – Software implementations (the source code) of selected algorithms
- D 2.2 – Test vectors of functions that have to be implemented in hardware

Objectives and workplan 4

Has planned milestones and deliverables been achieved?

- Step 3 (T0+7 - T0+15) . Hardware/software co-design of selected algorithms
- M 3.1 – Selected hardware functions (described in VHDL) and the software, which will call these hardware functions, must be available before realizations of attacks in Step 5.
- **Deliverables:**
- D 3.1 – Configuration files, VHDL code and description of functions implemented in hardware
- D 3.2 – The code and executable files of the software implementing selected algorithms and running on the PC, while calling functions implemented in hardware

Objectives and workplan 5

Has planned milestones and deliverables been achieved?

We have to start

- Step 4 (T0+7 - T0+19) . Development of measuring equipment and methodology
- Step 5 (T0+9 - T0+21) . Development and simulation of cryptanalytic attack algorithms

Project implementation and results

- Effectivness of management
  - To fasten ordering, PRFs -> NPD
  - Fill in MEFs -> NPD
- Collaboration of partners
  - Experts

Resources

- project has to use its resources and budget more effectively and efficiently

Impact

- Impact is made via scientific publications and conference contributions, o.k.

End users

- End-users are involved.
- End-users likely will exploit project results.

Communication

- Project has significant visibility in the scientific/technical community.
- Project has significant public visibility (or has such potential).

Young scientists

- Young Scientists are involved in scientific activities
  - SK M. Repka, P. Zajac, M. Jokay, O. Gallo
  - IS D. Genkin, I. Pipman, L. Pachmanov, E. Shaked
  - FR T. Richmond,
  - US B. Amento
- **Training** Plan
  - **Y 1 Y2 Y3**
  - **Daniel Genkin / other 2500 2500**
  - **Itamar Pipman / other 2500 2500**
  - **Lev Pachmanov / other 2500 2500**

Thank you for your attention

Thank you for your attention!