NATO SfP Project 984520

Status Report U.S. Partner Sep 2014

Research foci

- Quantum cryptanalysis
  - completed: quantum-related key attack (w/ colleague at Microsoft Research)
  - ongoing: improved quantum binary field arithmetic
  - not found so far: new structural attacks against McEliece
- Parameter choice in McEliece
  - ongoing: provable guarantees for CFS-style signature (w/ colleague at Kyushu Univ.)
  - ongoing: analyze performance of McEliece with Goppa codes vs. QC-MDPC
- Experimental work
  - DPA of QC-MDPC McEliece (w/ colleagues at WPI, incl. project expert, Univ. Bochum):
    → secret key recovery for DATE 2014 implementation on Xilinx XC6SLX4

Usage of project funding

- Agreement between Magma Group and Simons Foundation made purchase of budgeted software (Magma) unnecessary
  - convenient test installations under Linux and Windows
  - synergies with FAU funding for technology upgrade

  $\rightarrow$ convenient Magma access for graduate students

- Acquisition of the major equipment item for U.S. partner initiated
  - Dell PowerEdge T620 with 384 GB RAM, 2 CPUs, NVIDIA Tesla K20C GPU
  - currently working with Dell on payment details to adhere to NATO SfP guidelines

Opportunities for visibility

- Approved Dagstuhl Seminar 15371 Quantum Cryptanalysis (Sep 2015)
  - co-organized w/ M. Mosca, M. Roetteler, N. Sendrier
  - outreach to post-quantum crypto and quantum computing communities

- PQCrypto 2014
  - participation in program committee
  - planned: presentation to steering committee

- 9th Int. Workshop on Coding and Cryptography – WCC 2015
  - participation in program committee
  - opportunity to submit project results