Status report — Slovakia

Secure implementation of post-quantum cryptography
SPS Project Number: 984520
3rd meeting

Otokar Grošek Pavol Zajac

T. Fabšič, A. Gulyás, V. Hromada, M. Klein, F. Uhrecký

Institute of Computer Science and Mathematics
Slovak University of Technology

This project is supported by
NATO Science for Peace and Security Programme

Outline

Bitpunch library

- Development version:
  `https://github.com/FrUh/BitPunch`
- Original version based on *A. Shoufan et. al., A Novel Processor Architecture for McEliece Cryptosystem and FPGA Platforms, 2009*
- Key generation (parametric), Encrypt, Decrypt
- Basic tests
- V1 only: Modified Pointcheval conversion (using openssl's SHA-512)

Changes in the library

MSc. thesis by F. Uhrecky:

- Code refactoring, unified convention
- New context management (mecs, code, math)
- Modular architecture (asn1, code, crypto, math, prng)
  - Ability to add new modules without significant changes (i.e. new code, conversion etc.)
- Speed optimization
- Run-time memory usage reduction (matrix operations, decryption w/ or w/o H)
- Keys import/export using ASN.1 (libtasn1)
- Reimplemented SHA-512 from PollarSSL
- Zero added to support
- Basic test enviroment

Test results — Memory usage

BitPunch	Memory usage [KiB]
1. v0.0.1	8 818
2. v0.0.3 wo. H	162
3. v0.0.3 w. H	362

- Used tool - valgrind massif
- Basic MECS, Adapted Pointcheval CCA2* (m = 11, t = 50)
- Key generation, encryption and decryption of one block
- Import/export key using ASN.1*
- * v0.0.3

Test results — Speed comparison

BitPunch	KeyGen [ms]	Enc [μs]	Dec [ms]	Shared [KiB]	Static [KiB]
1. v0.0.1	866	62	3.9	64	96
2. v0.0.3 wo. H	768	48	52	92	172
3. v0.0.3 w. H	723	48	3.6	92	172

- Basic MECS (Goppa codes w/o CCA2, m = 11, t = 50)
- CPU Intel Core i5-2430M CPU @ 2.40GHz x 4
- RAM 2 x 4GB DDR3 1333MHz
- OS Ubuntu 14.04.1 LTS, Linux 3.13.0-49-generic

Test results — Library size

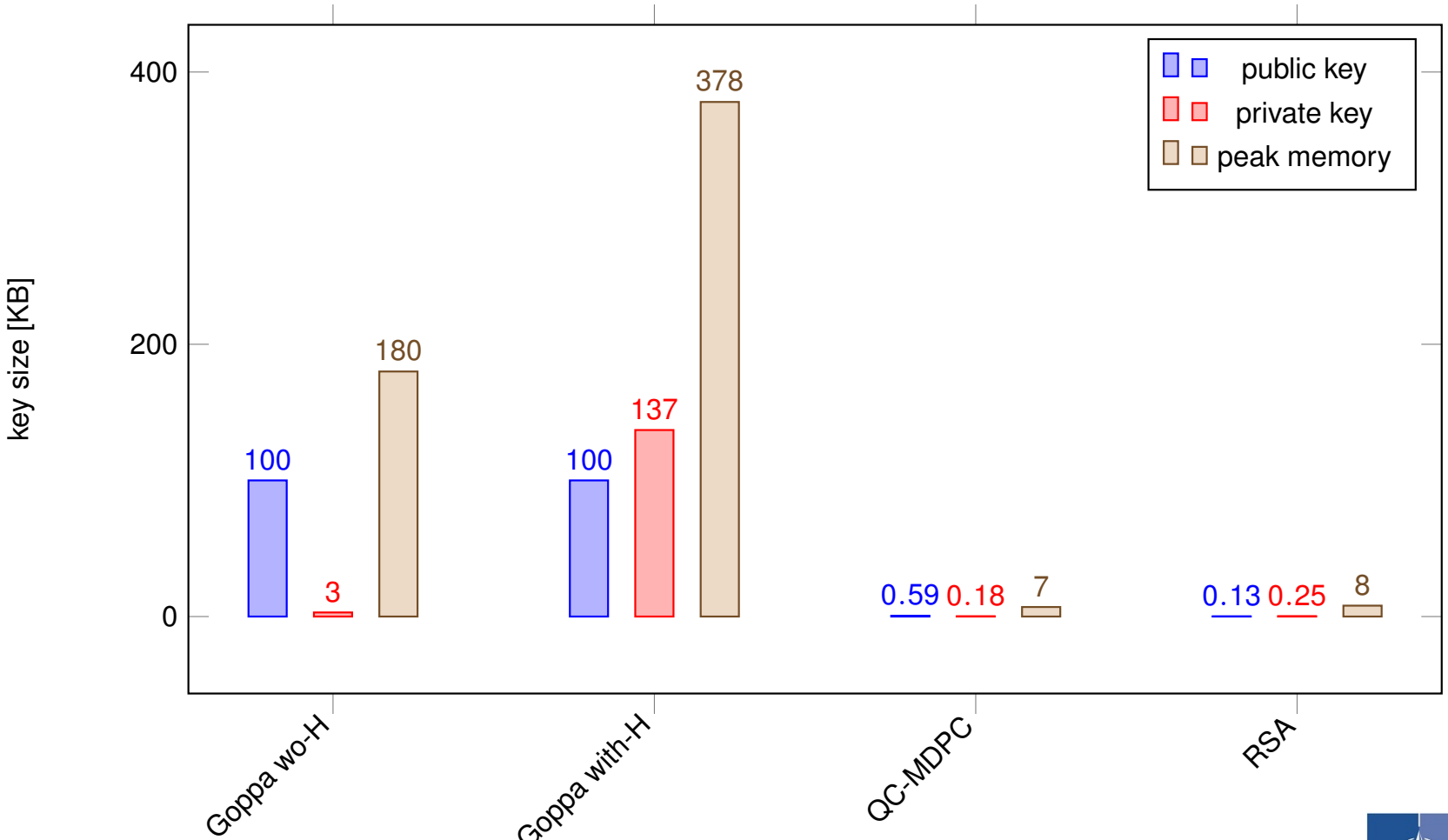
BitPunch	Shared [KiB]	Static [KiB]
1. v0.0.1 with CCA2	64**	96**
2. v0.0.3 FULL	92*	272
3. v0.0.3 FULL w/o print	68*	224
4. v0.0.3 Basic MECS w/o print	56*	208
5. v0.0.3 Basic + CCA2 w/o print	60*	212

- * + 80 for libtasn1
- ** + size of OpenSSL lcrypto (SHA-512)
- FULL - enc, dec, keygen, CCA2, ASN.1

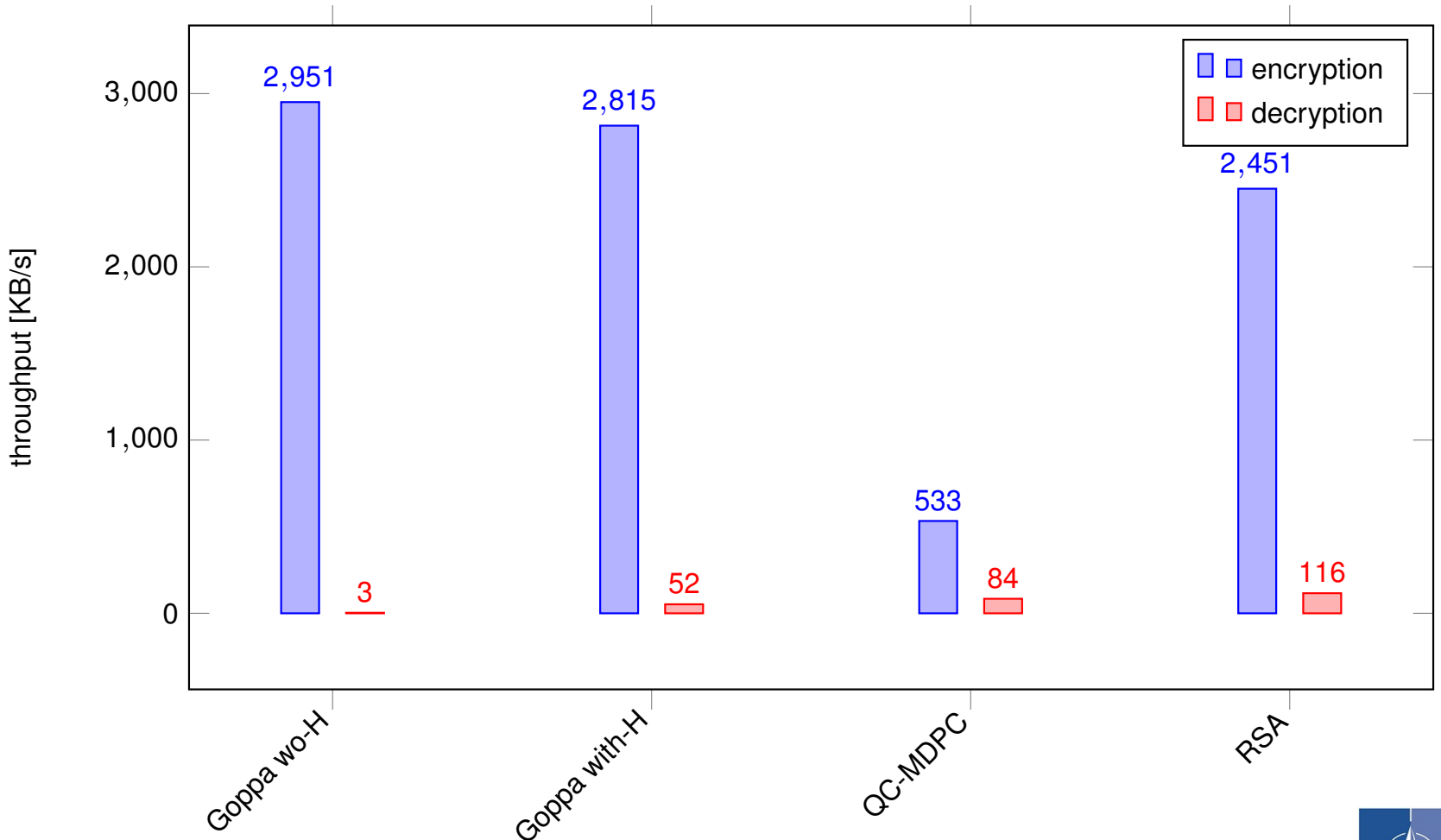
QC-MDPC codes

- MSc. thesis by A. Gulyas: Custom SW implementation of McEliece QC-MDPC codes based on BitPunch library
- Test results with:
  $n_0 = 2, n = 9602, r = 4801, w = 90, t = 84$
- No SCA countermeasures

QC-MDPC memory consumption



QC-MDPC throughput



QC-MDPC overview

cryptosystem	Goppa wo-H	Goppa with-H	QC-MDPC	RSA
mesg.len. [kB]	0.183	0.183	0.586	0.125
PK size [kB]	100	100	0.586	0.129
SK size [kB]	3	137	0.176	0.25
mem. peak [KB]	180	378	7	8
keygen [ms]	702	703	19	33
enc/mesg [ms]	0.062	0.065	1.100	0.051
enc.thr. [KB/s]	2951	2815	533	2451
dec./mesg [ms]	60	3.5	7	1.1
dec.thr. [kB/s]	3	52	84	116

Table : Comparison of cryptosystems

Timing side-channels

- Strong dependence of execution times of Patterson's decoding algorithm on number of errors
- Evaluation of error locator polynomial
- Number of XGCD steps
- Can be exploited in various ways
- MSc. thesis by M. Klein: Development of countermeasures against timing-attacks for BitPunch

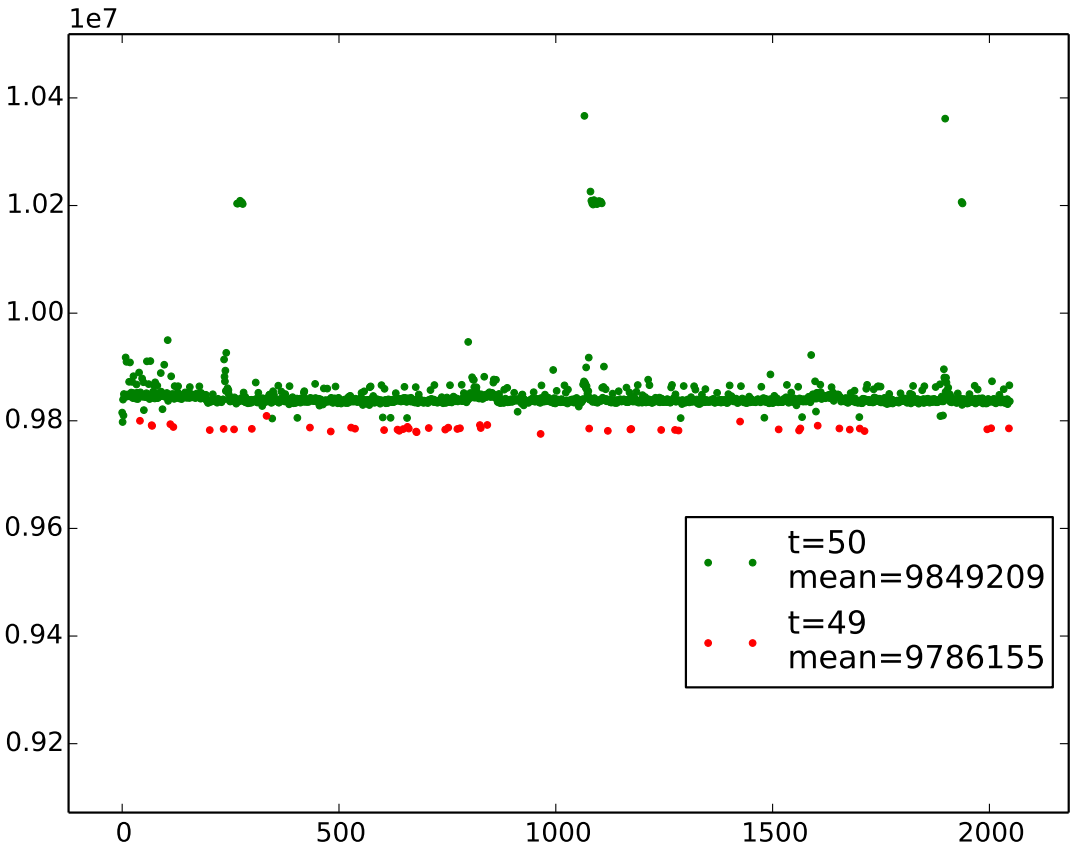
Side Channel Attacks resistance

- Original BitPunch: No SCA protection, vulnerable to various published attacks

Attack Type	t_0	t_1	Exploit type
Err.Locator Polynomial	3304830	3239563	Guess Error
Secret Permutation	140698	83	Algebraic
Syndrome Inversion	160546	95770	Algebraic

Side Channel Attacks resistance

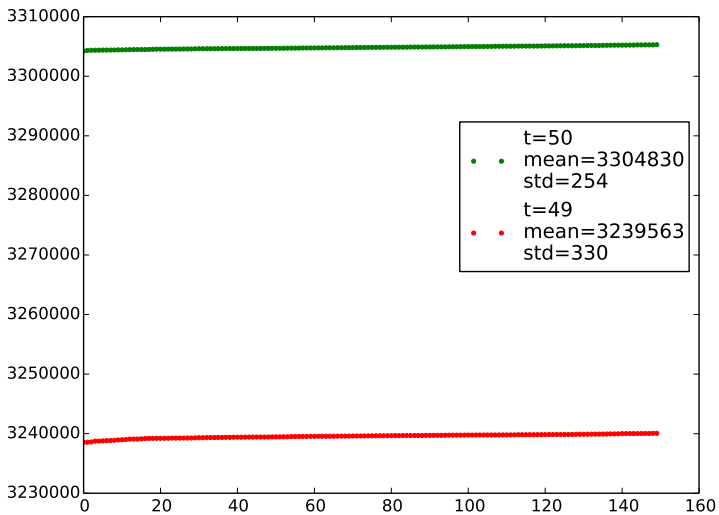
- Original BitPunch: No SCA protection, vulnerable to various published attacks



SCA countermeasures

- Currently resistant to attack on Err.Locator Polynomial
  - Time constant multiplication in finite field
  - Time constant evaluation of polynomials
  - Evaluation of ELP $\approx$ 2.5 times slower

SCA resistance



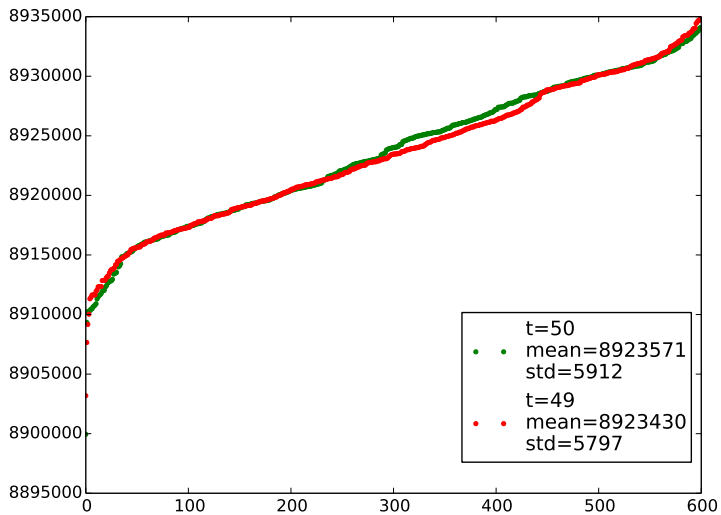
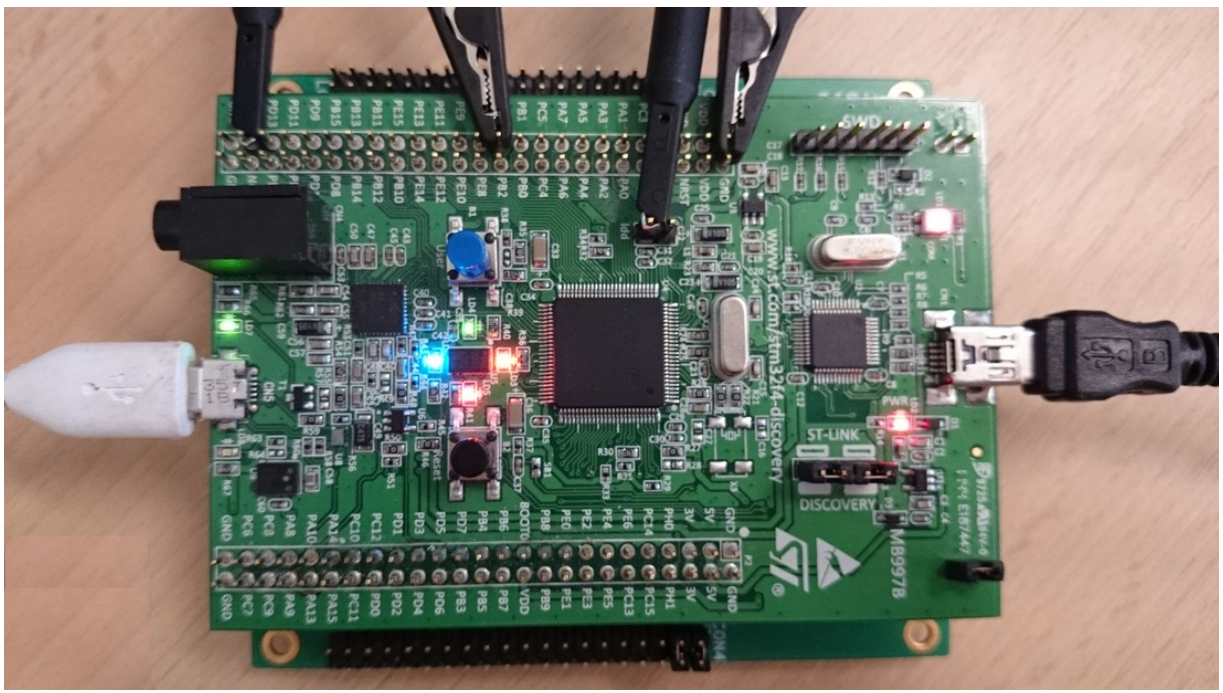


Figure : Evaluation of polynomials without (left) and with (right) countermeasures.

Power SCA on microprocessor

- Implementation of Bitpunch library on the STM32F407VG microcontroller integrated circuit.
- Due to limited memory size (192K) we are able to implement only 64-bit version of McEliece.



SCA resistance

- Our first experimental measurements of the power consumption suggest that are able to determine the permutation matrix by SPA.
- We decrypt all ciphertexts with HW one and save the corresponding power traces.
- These traces have a similar shape, but are mutually shifted by a time quantum, which corresponds to various positions of one-bits in the permutation matrix.
- We are able to determine the permutation matrix by sorting these power traces according to the execution time.

Step 6 of the project

Milestones:

M 6.1 Traces and recommendations for mounting efficient side-channel attacks:

- *Identification of secret permutation*
- *TODO: use power traces for timing attacks*

M 6.2 Capability to extract confidential data from experimental data:

- *Basic power traces (SPA) using Picoscope 6403*

Deliverables:

D 6.1 Aggregated data: *WIP*

D 6.2 Software for extracting secret data from experimental data: *WIP — Matlab scripts*

Invertible circulant matrices with prescribed weight

- We proved that an invertible circulant binary $(n \times n)$-matrix with $\frac{n^2}{2}$ ones exists if and only if $n = 2 \pmod 4$.
- For $n = 2 \pmod 4$, we developed an efficient method to construct a large set of invertible circulant binary $(n \times n)$-matrices with $\frac{n^2}{2}$ ones.
- We developed an efficient method to construct a set of invertible circulant binary $(n \times n)$-matrices with $n \times p$ ones, where p is a prime such that $\gcd(p, n) = 1$.
- We currently develop methods to construct matrices with other prescribed numbers of ones.

Publicity and Training

- March 5, 2015, Presentation at Ruhr-Universität Bochum P. Zajac et.al.: Side-Channel Resistant Implementation of Post-Quantum Cryptography.
- Written a report about the Project to the University magazin Spectrum. This contribution clearly sends the message about the importance of post-quantum cryptography in a world-wide scale along with concise description of state of the art in the particular field. Paper is available at `http://www.stuba.sk/new/docs//stu/informacie_o/diani_na_stu/spektrum/2015/201505.pdf`

Publicity Plan

- University of Washington, Tacoma, USA, June 2015
- 15-th Central European Conference on Cryptology, Klagenfurt, Austria, on July 8-10, 2015.
- University of Bergen, Norway, September 2015

Summary

- Implementation
  - New version of BitPunch
  - QC-MDPC implementation
- Research
  - Countermeasures against timing side-channels
  - Power side-channels on microprocessor
  - Further results for cyclic matrices
- Publicity: 1 presentation, 1 article