Progress report (Slovakia)

Project meeting

Secure communication in the quantum era
SPS Project Number: G5448

Pavol Zajac, Tomáš Fabšič, Viliam Hromada,

Institute of Computer Science and Mathematics
Slovak University of Technology

March 03, 2020

Overview: activities in Slovakia

Current project focus:

- Step 1-B: Implementation security of cryptographic primitives
- Step 2-B: Identify protocol-level security mechanisms

Strong emphasis on project dissemination and student participation.

Published papers (2019)

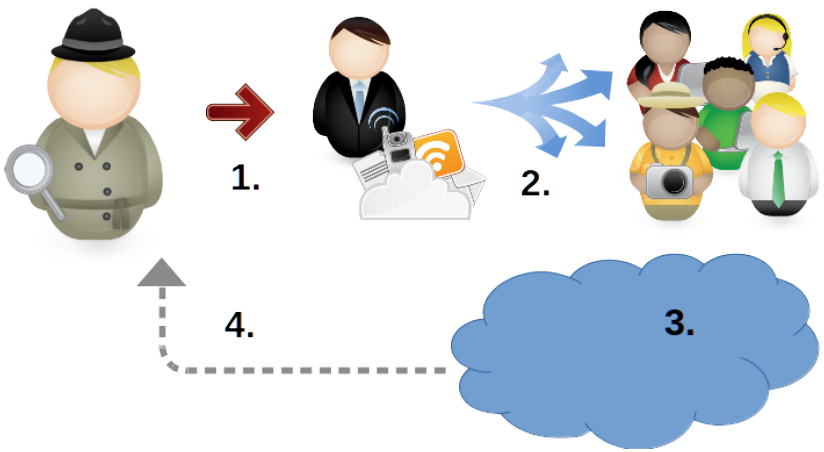
- ZAJAC, P. - ŠPAČEK, P.: Preventing potential backdoors in BIKE algorithm, Tatra Mt. Math. Publ. 73 (2019), 193–207.
- ZAJAC, P. - ŠPAČEK, P.: A New Type of Signature Scheme Derived from a MRHS Representation of a Symmetric Cipher, Infocommunications Journal 9/4, (2019), 23–30.

Conference talks (2019)

- ZAJAC, P.: Code-based signature scheme derived from a MRHS representation of an AES encryption. In Central European Conference on Cryptology 2019 : Telč, Czech Republic. June 12-14, 2019. Brno.
- HROMADA, V.: Acoustic Side-Channels in Cryptography. CYBERSEC CEE 2019 – 5th European Cybersecurity Forum. Katowice, Poland. 29. - 30. 10. 2019.
- ŠPAČEK, P. - COLOMBO, C. - VELLA, M.: Using TEE and RV in PQ-TLS Communication. CSAW'19. Department of Computer Science. University of Malta. 29. 11. 2019.
- PERNICKÝ, Ľ. - ZAJAC, P. Integration of post-quantum cryptography to Android application (in Slovak). In Santa's Crypto 2019 : proceedings. Praha, Czech Republic. 5.-6.12.2019.

Preventing potential backdoors in BIKE algorithm

Focus on preventing potential backdoors in post-quantum primitives.



1. BigBrother enforces subverted key generation.
2. Devices are distributed in free market.
3. Users communicate over the internet.
4. BigBrother eavesdrops.

Preventing potential backdoors in BIKE algorithm

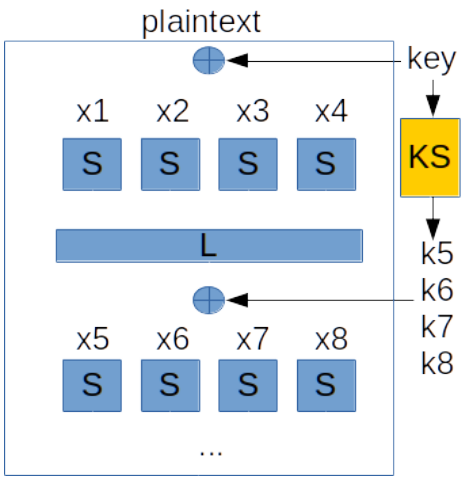
Focus on preventing potential backdoors in post-quantum primitives.

- Possible attack channel for BigBrother in BIKE: class of weak keys.
- Our solution: Verifiable secure key generation.
- Can be combined with runtime verification mechanisms...

A New Type of Signature Scheme Derived from a MRHS Representation of a Symmetric Cipher

New signature scheme design based on symmetric ciphers to overcome performance problems of proposed post-quantum schemes.

- Signatures based on MRHS equations.
- Performance comparable to symmetric encryption.
- Requires further study to provide required security guarantees.



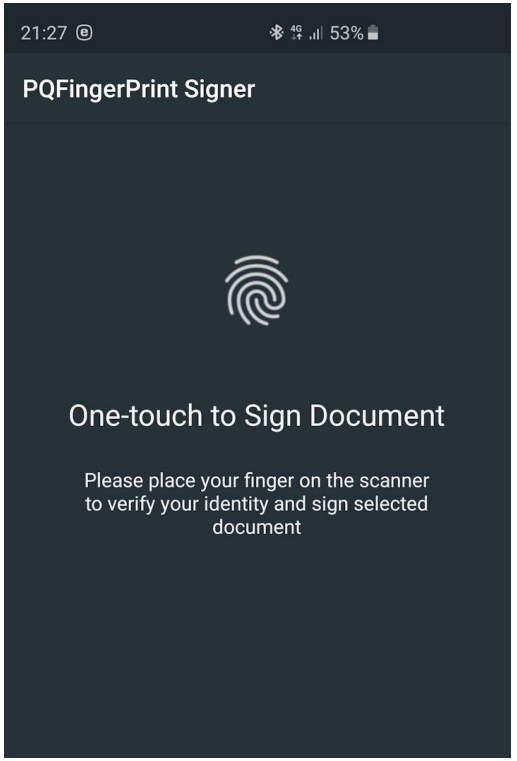
Finalized MSc. Theses (2019)

- Ľubor Pernický. Post-quantum cryptography on Android.
- Martin Novotný. Implementation of the experimental post-quantum protocol.
- Tomáš Baraniak. Decoding of QC-MDPC codes.
- Ján Kováč. Reaction attack on the QC-MDPC McEliece cryptosystem.
- Peter Kyseľ. The Implementation of HFE-cryptosystem over Finite Fields $GF(2^k)$ and $GF(p)$.
- Rastislav Páleník. The Implementation of EFC-cryptosystem over Finite Fields $GF(2^k)$ and $GF(p)$.

Integration of post-quantum cryptography to Android application

Android application that can sign PDF documents with SPHINCS algorithm.

- 500 ms to sign, 6 ms to verify signature (Samsung Galaxy S9+/S10+)
- Public Key size: 1kB,
- Signature size: 41 kB,
- Encrypted secret key unlocked with fingerprint.

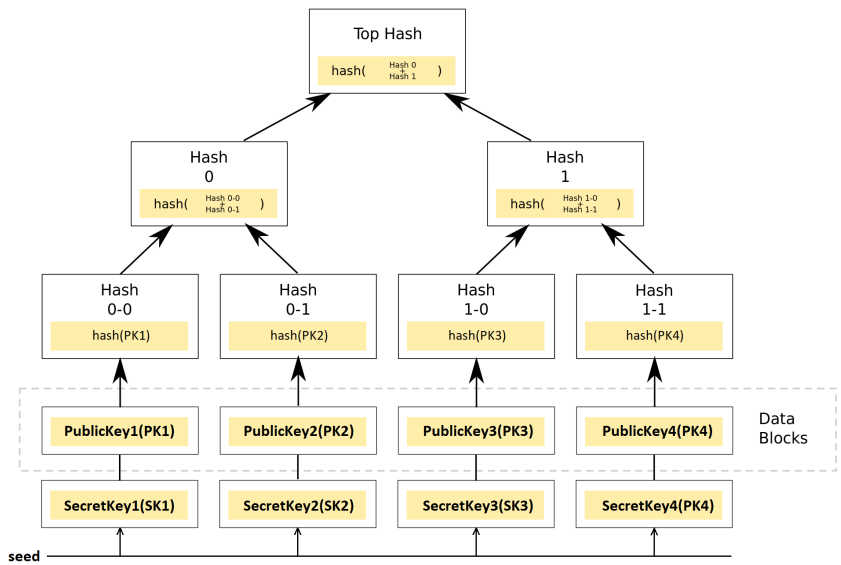


Implementation of the experimental post-quantum protocol

Efficient authentication of ephemeral keys
`https://eprint.iacr.org/2019/921`

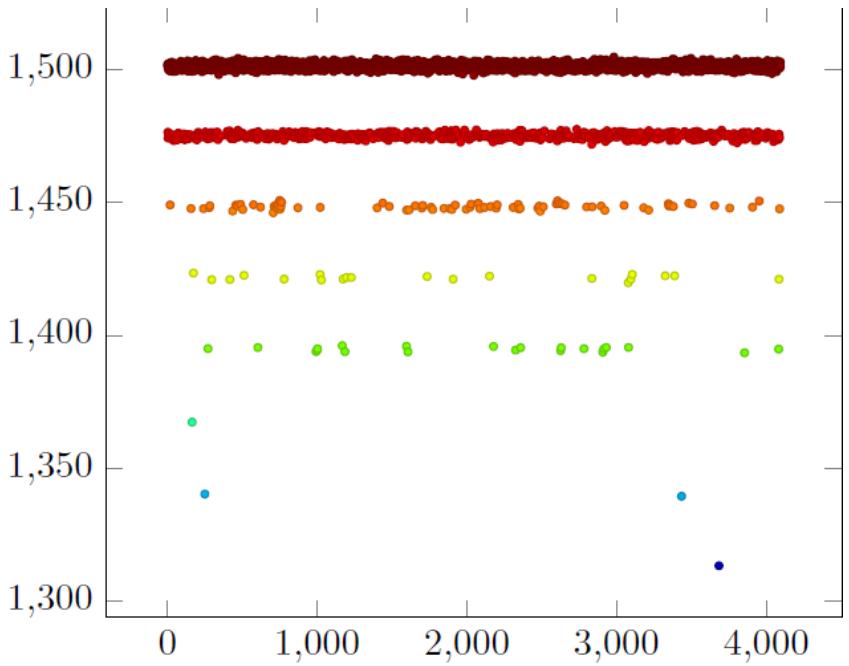
Implemented with BIKE,
2^{23} keys, per key performance:

Keygen:	$270.4\mu s$
Merkle tree:	$0.4\mu s$
Key signature:	$1.4\mu s$
Key verification:	$7.4\mu s$



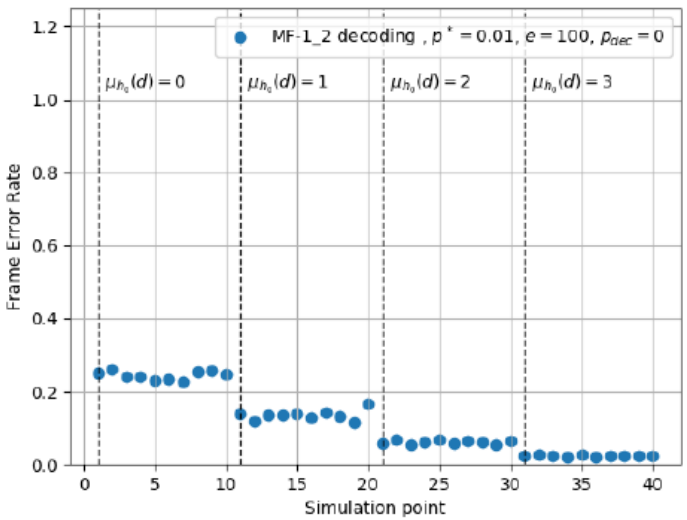
Reaction attack on the QC-MDPC McEliece cryptosystem

- Experimental reaction attack on QC-LDPC based cryptosystems, decoding errors can leak secret information (side channel).

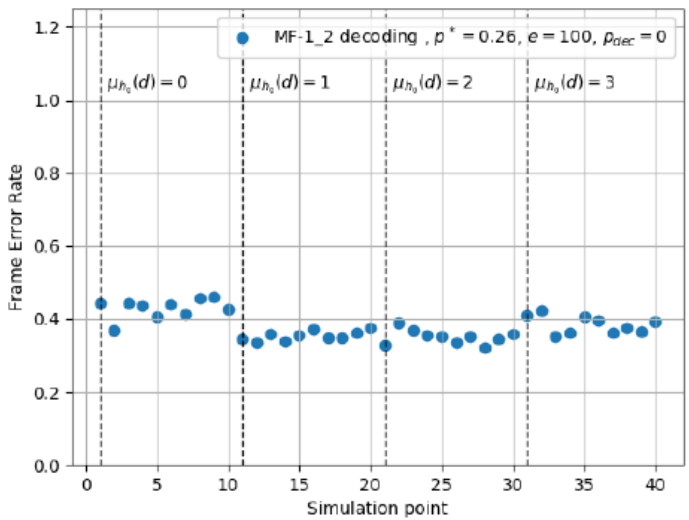


Decoding of QC-MDPC codes

- Implementation of new decoding algorithms in BitPunch library.
- Can mitigate side-channel attacks based on frame errors.



(a) $p^* = 0,01$



(b) $p^* = 0,26$

Implementations of multivariate cryptosystems

- Sagemath implementations of multivariate cryptosystems EFC, HFE.
- Batch generation of their public keys in MQ-challenge format usable in their further cryptanalysis.

```
Galois Field : GF(2)[x] / x^8 + x^4 + x^3 + x^2 + 1
Number of variables (n) : 35
Number of polynomials (m) : 70
Seed: 0
Order : graded reverse lex order

************************
008 05f 009 0df 0f5 008 0ba 014 01b 077 0fa 016 085 04c 01b 0b2 030 086 036 0ae 067 028 079 0bc 01d 0ae 072 047 068 053 089 0e4
0bb 0c1 0f1 09c 063 024 051 069 005 064 060 095 0b1 01f 050 062 0f5 095 09e 0e0 0f1 073 06a 055 045 050 051 081 0cb 010 0a0 0eb
0e6 052 0e6 0db 0c1 0be 01b 0e2 0f5 0c7 0cb 02a 01d 079 0b3 068 03c 0c6 0f3 0d8 09e 00e 049 005 04f 051 01a 036 0d0 07a 065 06c
080 079 01c 0cf 084 054 057 091 0be 01a 070 078 00e 055 0c8 001 003 0ba 039 0d3 0fe 0fb 070 06d 0b5 096 0c1 06a 05f 08e 0d6 026
03a 012 0c3 09c 011 094 0d5 0e1 067 079 0b8 008 087 08e 02f 02f 0fb 038 05d 0af 02e 0e4 02c 06e 01a 06a 060 000 0d8 006 00d 0ec
0e4 054 0f5 013 08f 05e 0f4 0b8 01f 0cb 079 05c 041 03e 0c6 00c 067 0b8 038 01c 0ce 097 0a3 0c0 033 09b 0a7 0c2 027 0cc 016 0d7
0d1 07c 039 0d8 096 048 0bd 0bd 0c7 05d 0f5 0d0 0aa 063 03f 0ff 0ee 033 097 06a 063 0c3 08c 0ef 046 004 0b9 0e6 092 0de 055 019
086 038 012 02e 06b 0f6 05f 0e3 096 05c 0a1 056 0b3 066 070 00c 08a 0c2 0ab 096 07f 0c5 005 0ad 039 0d9 0c3 04d 0c6 080 045 0ce
0c0 03f 0e4 099 0ba 087 0f0 06b 08e 078 010 0f3 08c 069 06d 051 071 05d 011 0bf 046 0cc 05a 0c3 018 04f 015 044 0e6 02a 023 0d0
09d 0a1 05d 061 02c 0d4 082 05a 086 0a4 05b 0f2 0d0 021 07c 0ec 0b9 019 04a 02b 022 05d 07c 00d 086 076 092 0f6 017 011 06d 0c5
056 0de 074 0ce 0e5 0cf 0c5 040 019 000 066 081 03d 049 07d 0f7 015 099 0b5 0f5 09a 096 089 0d6 0de 085 054 06d 05b 0e4 0fe 060
0d2 083 058 0b6 02c 0a7 04c 019 0d2 05f 089 081 069 0bc 0cd 043 0b6 076 02e 0e2 096 0a0 049 053 022 0a2 02e 0dc 03b 00e 06f 0a2
00b 0f4 0a2 0e3 067 0e4 0bb 094 0d3 081 055 054 0f0 0be 0de 080 005 03e 000 071 0c2 03a 076 0f5 099 0bd 0ec 057 0b6 0a5 0c8 0d4
0ca 05a 058 0e7 02f 09d 0eb 09a 0b2 058 07a 004 05a 017 0ea 040 0c2 0eb 089 0eb 017 067 0db 0fc 0a2 088 022 0fb 048 070 0d8 0bb
095 043 0fe 0eb 057 070 022 07b 0d7 0d8 0db 000 050 05e 0bf 0a5 0cd 055 01c 0bd 058 06a 081 0d1 06d 0f7 0c1 0d5 07e 0db 0d6 075
05c 0b8 057 05f 0b9 019 05e 06c 0b0 090 0b3 0a5 0ce 0c8 0a2 06d 0a0 0c8 0af 01a 009 037 0b0 01b 011 023 016 053 0e1 0ca 000 0c6
0d1 087 06a 08f 096 047 043 0de 0cf 0e6 016 0ef 017 002 0e3 092 0ea 0f6 03b 024 063 0da 080 098 043 017 044 04e 083 09f 0b7 081
0dd 06f 02c 0bf 080 0f5 006 03d 089 0d9 097 011 0a7 0aa 057 08e 064 0d7 0b8 076 045 05e 04e 03a 02a 020 063 039 078 07a 0e9 026
00b 043 0e3 06f 08f 006 076 0d3 040 014 0ba 000 04d 05b 0fb 0de 0f9 00c 03e 059 0fc 050 094 090 0bd 0dd 0f3 086 012 033 069 00d
```

Work in Progress

- **P. Špaček: Incorporation of post-quantum primitives into TLS.**

WIP MSc. Theses (2020)

- Implementation of post-quantum primitives:
  - Daniel Jahodka. Post-quantum signature scheme based on AES.
  - **Peter Malo. The implementation of post-quantum group key-exchange protocol.**
  - Andrej Pavlatovský. HFERP cryptosystem.

WIP MSc. Theses (2020)

- Cryptanalysis of post-quantum primitives and cryptographic schemes:
  - Nikoleta Furičková. Decoding a random linear code using an improved version of Stern's algorithm.
  - Ivana Jozeková. Reconstruction of a binary vector from its incomplete distance spectrum.
  - Juraj Karásek. The QC-LDPC McEliece cryptosystem and its resistance against the GJS attack.
  - Peter Kiska. Algorithms for decoding random linear codes.
  - Peter Radvan. Supplementary software for the analysis of MQ cryptosystems.

WIP Bc. Theses (2020)

- Samuel Orth, NIST PQC MQ-based Signature Schemes.
- Jakub Šíp, Post-quantum cryptography.
- Juraj Paška, Decoding QC-MDPC codes with a low failure rate.