SPS Programme Multi-Year Project Final Report

SPS internal use

Progress Report Received	SPS Reference:	SfP G4520

Emerging Security Challenges Division

Science for Peace and Security Programme

Multi-Year Project Final Report

insert project title

Post-quantum Cryptography

submit completed report in **Microsoft Word format** to sps.admin@hq.nato.int

Project Start Date	Project Duration	Date of this Report
11 December 2013	36 month	11 December 2016

Project Co-Directors

	Title and Name	Institution	Country	email
N P D	**Prof. Otokar Grošek**	**Institute of Computer Science and Mathematics, Slovak University of Technology, Bratislava**	**Slovakia**	**otokar.grosek @stuba.sk**
P P D	**Dr. Eran Tromer**	**School of Computer Science, Tel Aviv University, Tel Aviv**	**Israel**	**tromer@cs.tau.ac.il**
	Prof. Viktor Fischer	**Hubert Curien Laboratory, Jean Monnet University, Saint Etienne**	**France**	**fischer@univ-st-etienne.fr**
	Dr. Rainer Steinwandt	**Department of Mathematical Sciences, Florida Atlantic University, Boca Raton, FL**	**USA**	**rsteinwa@fau.edu**

Abstract & Current Status

provide an abstract of the project and its accomplishments (no more than one-half page)

Project results were published in 46 scientific papers, and presented in 27 conference contributions.

This project sets out to identify secure parameter sets, relevant attack vectors for side-channel analyses, and secure implementations for asymmetric cryptographic schemes in a post-quantum setting:

- On the algorithmic side, we identified cryptographic schemes and secure parameters, offering strong (provable) guarantees against quantum algorithms. At the same time, the performance is competitive with deployed solutions.
- On the cryptanalytic side, we identified plausible attack power traces and methods against implementations of a post-quantum cryptographic scheme, and we also empirically demonstrated side-channel attacks against implementations in software and hardware.

On the implementation side we identified some of the necessary secure implementation conditions of a post-quantum cryptographic scheme that can withstand common side-channel attacks.

Project Goals

summarize the major goals and objectives of the project; highlight any changes from the project plan or previous reports (this is unusual)

- On the cryptanalytic side, our objective was to identify realistic assumptions and parameter sets that can withstand a well-funded attacker, capable of running dedicated

and highly optimized cryptanalytic devices. While for discrete logarithm problems on elliptic curves and for integer factorization the use of cryptanalytic hardware has been explored in the literature, for fast lattice reduction or for decoding linear codes the potential of highly optimized cryptanalytic engines (e.g., in the form a FPGA cluster) was not clear.

- On the implementation side, our objective was to provide implementations which can withstand common side-channel attacks, including physical (power analysis, electromagnetic analysis, etc.) and software-based (e.g., cache analysis). This requires the identification and application of appropriate leakage models, and also concrete experiments with implementations on different platforms.—A purely theoretical side-channel analysis is not reliable enough for such implementation-specific attacks, and placing practical counter-measures “only” heuristically, offers no acceptable security guarantees either.

Summary of Accomplishments

summarize accomplishments under these goals

During the project we have obtained a wide range of scientific results related to the main project goals.

From the cryptanalytic perspective, the most important result include the first successful Differential Power Analysis against a modern FPGA implementation of McEliece, a precise estimate of the cost of Grover’s attack against AES on a quantum computer (number and type of gates, number of qubits, circuit depth), and we provided improvements for implementing Shor’s algorithm on a quantum computer against particular elliptic curves. We have also studied different capabilities of quantum attackers, including the first quantum related-key attack, which applies to a large class of block ciphers. Other theoretical results include the detailed study of the security of variants of the McEliece cryptosystem, including the analysis of a McEliece-type signature scheme in a formal security model. As the most important result we can mark the proof of NP-completeness of the coset-weight problem for quasi-dyadic codes. We have also studied how to apply the theoretical results to practice, including new proposals of pseudo-random generators with a security reduction to hard quantum-resistant problems.

On the implementation side, we have focused on two main topics: Secure implementation of the McEliece cryptosystem, including side-channel resistance. We have prepared several implementations of the system, including a standalone open source project called BitPunch that supports Goppa based, QC-MDPC and QC-LDPC McEliece variants. We have published several papers documenting side-channel attacks on McEliece variants, including software timing attacks on Goppa variants, hardware DPA on QC-MDPC, and power analysis attacks that identify the secret permutation. We also developed a masked FPGA implementation of QC-MDPC and experimentally validated its security against first-order DPA.

The second main topic focused on a new category of side-channel attacks, so called *low bandwidth attacks*, including acoustic cryptanalysis. These attacks are very powerful, as they can extract secret keys from running PCs in practice, even over distance. Most of the published papers focus on classical algorithms (RSA, ECDSA), but we have also identified a potential vulnerability of the McEliece system (this research is still in progress).

From a broader perspective, our project has been important in preparing young scientists for post-quantum research, which is now gaining momentum in the scientific community. Our results and implementations can be used in the already initiated NIST process to standardize post-quantum cryptographic primitives.

Accomplishments

detail accomplishments and progress achieved by this project

Detailed accomplishments by year and country

Slovakia

Bitpunch team (a team of MSc. students: F. Uhrecky, M. Klein, A. Gulyas, F. Machovec, J. Kudlac, supervised by Pavol Zajac) prepared a standalone implementation of the McEliece cryptosystem in the C programming language. The implementation does not use external libraries for the core McEliece functions. Instead, they are implemented in specific modules, from the basic field arithmetic, through support function, McEliece primitive routines (key generation, encryption, and decryption) up to CCA2-conversions. The bitpunch implementation uses OpenSSL library to provide SHA-512 implementation required for the CCA2-conversion, but this dependency can easily be removed or replaced by other suitable code.
The Bitpunch implementation of the McEliece cryptosystem provides a modular lightweight library that can be used as a basis of a hardware/software codesign solution. The library is split into several modules, operating on different levels of abstraction (e.g., the basic arithmetic, support functions, core McEliece, etc.). The individual modules can be replaced by dedicated hardware functions to speed-up the solution or provide other desired benefits (such as side-channel countermeasures).
Pavol Zajac has prepared a short note (eprint article) http://eprint.iacr.org/2014/651 that discusses the issue of security for some of the proposed CCA2 conversions. If a specific version of Pointcheval's generic conversion is used with McEliece cryptosystem, additional parameter (the length of message, or the length of the hash output, respectively) enters the calculation of security level (instead of just the traditional n, k, t). If an incorrect parameter is used, the security of the system can be compromised via a subtle flaw in the padding construction. However, the conditions for the attack are artificial, and in a typical parametric setting do not influence the system. On the other hand, if the parameter choice is not checked, it can open a potential side-channel exploitable by the attacker.
Version 0.0.4 of the BitPunch library includes ASN.1 serialization for interoperability. Moreover, a new implementation of McEliece based on QC-MDPC codes was integrated into BitPunch as an alternative to basic McEliece based on Goppa codes.
BitPunch library was also tested in the embedded environment: on Microsemi SmartFusion2 development board, and on the commercial microprocessor board STM32F4.

New results in Lee codes were published by P. Horak, O. Grošek: A new approach towards the Golomb-Welch conjecture. In this paper there is described a different view of Lee Codes using homomorphisms. They published new theoretical results on the non-existence of linear PL(n;2) codes for $12 \geq n$, and the first quasi-perfect Lee codes for dimension n =3. For fixed n, they also proved that there are only finitely many quasi-perfect Lee codes over Z. Unfortunately, for the time being, application to MECS is an open question.

Slovakian partner has developed a new fast algorithm for extracting pth roots in extended finite fields of prime characteristic $p \geq 2$. This paper has been published in Electronics Letters, Volume 52, Issue 9.
Slovakian partner also studied the problem how to efficiently generate circulant binary matrices with a prescribed number of ones which are invertible over Z_2. The paper was presented at ArcticCrypt 2016.
Slovakian team has finished five software implementation tasks, as well as experiments with power analysis. The first finished implementation was the extension of the original BitBunch library. We have called this extension a "McEliece cryptobox". Cryptobox implements a hybrid encryption, which means that long message is encrypted by a symmetric cipher under random session key, which is encrypted with McEliece cryptosystem. Testing shows that for large messages a cryptobox style hybrid encryption is more efficient than using a separate key encryption and data encryption.

The second project was an implementation of LDGM signature scheme. We have successfully implemented this scheme into the BitPunch branch. LDGM system is an efficient post-quantum signature scheme, but unfortunately, it is not secure (the attacks were found during the development of the scheme).
The third project was a standalone specialized implementation of QC-MDPC cryptosystem on AVR microchips called uEliece. Unlike BitPunch library, this system is monolithic, has a fixed size parameters and a fixed Kobara-Imai beta conversion (modified to support messages of variable length and streaming encryption). The experimental code proved too slow in practice, but the issue is mostly with the symmetric encryption part. We continue this project in the present, trying to employ the new standard XOF function SHAKE instead of SHA-3 based PRNG in Kobara-Imai conversion.
The fourth implementation project was concerned about using McEliece cryptosystem in smartphones. We have created an implementation of messenger application that uses McEliece (implemented in BouncyCastle library) to initiate communication sessions. A modified Needham-Schroeder protocol is used to ensure the forward secrecy of communication. Our test shows that while encryption and decryption with McEliece cryptosystem is quite practical, key generation (of ephemeral keys needed for forward secrecy) is too slow.
The fifth implementation was another extension of the BitPunch library. We have implemented the quasi-cyclic low-density parity check (QC-LDPC) codes into the BitPunch library. QC-LDPC are an alternative to Goppa codes since the corresponding public and private keys are smaller, which makes these codes interesting for implementation on devices with limited memory.
Students Andrej Boledovič and Juraj Varga presented on 16th Central European Conference on Cryptology (CECC 2016), June 22-24, Piešťany, Slovakia, “Practical Implementation of McEliece Cryptosystem on Android”. Mobile operating system Android is the most commonly used mobile OS in the world. Since the first version of this OS, Android contains embedded cryptographic library to use by the developers. However, this library does not contain ciphers belonging to so called post-quantum cryptography (PQC). In our work we implemented McEliece algorithm as a representative of PQC in messenger application in OS Android.
O. Grošek and V. Hromada presented at 16th Central European Conference on Cryptology (CECC 2016), June 22-24, Piešťany, Slovakia, equivalence classes of binary vectors with regards to their rotation by using an algebraic approach based on the theory of linear feedback shift registers. They are used in quasi-cyclic codes, e.g. QC-LDPC (low-density parity-check codes) as proposed by Baldi et. al. Another interesting example, where equivalence classes of rotation of binary vectors are studied, is the rotational cryptanalysis of various cryptosystems. They stated the necessary and sufficient condition for existence of an equivalence class with given cardinality and provide two formulas. The first represents the sharp distribution of cardinalities for given length and Hamming weight of binary vectors and the second enables us to determine the number of different classes with the same cardinality.

United States of America

On the side of quantum cryptanalysis, a graduate student in the U.S.--group developed a method to automatically generate efficient quantum circuits for GF(2^n)-multiplication. Using a Python/Sage-based implementation, we have been able to synthesize quantum circuits for binary field multiplication with a drastically lower T-gate complexity than the best designs available in the literature so far. The number of T-gates needed is one of the most critical complexity parameters for quantum circuits. The paper by S. Kepley and R. Steinwandt containing these results appeared in *Quantum Information Processing* (vol. 14, no. 7, pp. 2373-2386). Moreover, in the U.S. group efficiency improvements for quantum circuits as needed for a quantum attack against a popular type of elliptic curve cryptography have been achieved; the corresponding paper by P. Budhathoki and R. Steinwandt has appeared in the journal *Quantum Information Processing* (vol. 14, no. 1, pp. 201–216, 2015). A (record) low-depth implementation of Shor’s algorithm for a particular type of elliptic curves has been identified and published by M. Rötteler and R. Steinwandt (Quantum Information & Computation, vol. 14, pp. 888-900, 2014). Further, a quantum related-key attack against a wide class of block ciphers has been identified by M. Roetteler and R. Steinwandt. The

corresponding paper has appeared in *Information Processing Letters* (vol. 115, no. 1, pp. 40-44, 2015.).

Different code-based signature schemes and encryption schemes and corresponding hardness assumptions for their security analysis have been reviewed. With Goppa codes a main issue is the availability of an efficient distinguishing attack which invalidates an assumption in an available provable security reduction for a popular code-based signature design. Exploring this algebraic attack more closely has been the topic a Master's thesis during the project (by Hai Pham: *Distinguishability of public keys and experimental validation: the McEliece public-key cryptosystem)*. To cope with the problem of key size, structured generator matrices have been proposed, but most recent results suggest that this imposed key structure reduces the security margin. Medium-Density-Parity-Check (MDPC) codes appeared a promising alternative to Goppa codes—lacking the algebraic structure of a Goppa code, distinguishing attacks appeared harder. The U.S. partner mounted in collaboration with colleagues at Worcester Polytechnic Institute (Thomas Eisenbarth, an expert for this project, and Cong a successful Differential Power Analysis attack against an MDPC-based McEliece implementation. These results are documented in a conference paper by C. Chen, T. Eisenbarth, I. von Maurich and R. Steinwandt (*Differential Power Analysis of a McEliece Cryptosystem*, Proceedings of 13th International Conference on Applied Cryptography and Network Security ACNS 2015, vol. 9092 of Lecture Notes in Computer Science, pp. 538-556, Springer, 2015) and a journal paper by C. Chen, T. Eisenbarth, I. von Maurich, and R. Steinwandt (*Horizontal and Vertical Side Channel Analysis of a McEliece Cryptosystem*, IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, 1093-1105, 2016).

The US-partner developed, in collaboration with an expert and other scientists the first masked QC-MDPC McEliece implementation on an FPGA. Suitable masking techniques had to be developed and implemented, and an experimental validation of security against 1st order DPA has been conducted. This work has been presented in a paper by C. Chen, T. Eisenbarth, I. von Maurich and R. Steinwandt (*Masking Large Keys in Hardware: A Masked Implementation of McEliece*, Proceedings of Selected Areas in Cryptography SAC 2015, vol. 9566 of Lecture Notes in Computer Science, pp. 293-309, Springer, 2016). Regrettably, at the very end of the project, new theoretical results became available that render suggested QC-MDPC codes insecure. While the developed DPA techniques and countermeasures remain valid, for practical deployment QC-MDPC codes do not seem suitable anymore at this point.

The U.S. partner advanced the quantum cryptanalytic toolbox, too—when implementing a full-fledged hybrid encryption, (KEM-DEM) in addition to McEliece (with Goppa codes) as key encapsulation mechanism, one would commonly use a symmetric cipher for the complementing DEM part. Building on AES would be a typical choice, and we quantified the quantum resources needed to attack that part with a Grover-based key search. This included in particular work on implementing the AES S-box as a quantum circuit. Our findings have been presented at invited presentations in Canada and Waterloo, and a more complete analysis has been published at PQCrypto 2016 in a paper by M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt (*Applying Grover's Algorithm to AES: Quantum Resource Estimates*, Proceedings of Post-Quantum Cryptography 2016, vol. 9606 of Lecture Notes in Computer Science, pp. 29-43, Springer, 2016). A Grover-based quantum cryptanalysis of two other prominent block ciphers (Serpent and MARS) has been worked on as well. This is joint work with a colleague in Germany and two Ph.D. students. The analysis of Serpent is part of a Ph.D. thesis that has been completed during this project by Brittanney Amento, and the work on MARS is currently in the final phase. We expect a paper submission with these results to be ready in early 2017.

Most recently, work has been initiated to deal with fault induction attacks – unlike for passive-side channel attacks, here modifications of internal data is possible. We initiated this exploration with work on a symmetric cipher in collaboration with a project expert (Thomas

Eisenbarth), however this is still research in progress. We have also collaborated with colleagues in Japan on establishing strong provable guarantees for a variant of the (code-based) CFS signature. Initial thoughts have been presented by a co-author from Japan at a Dagstuhl seminar, and we hope that a paper will be published over the course of 2017.

Israel

Israeli team demonstrated the extraction of secret decryption keys from laptop computers, by nonintrusively measuring electromagnetic emanations for a few seconds from a distance of 50 cm. The attack can be executed using cheap and readily-available equipment: a consumer-grade radio receiver or a Software Defined Radio USB dongle. The setup is compact and can operate untethered; it can be easily concealed, e.g., inside pita bread. Common laptops, and popular implementations of RSA and ElGamal encryptions, are vulnerable to this attack, including those that implement the decryption using modern exponentiation algorithms such as sliding-window, or even its side-channel resistant variant, fixed-window (m-ary) exponentiation.
We successfully extracted keys from laptops of various models running GnuPG (popular open source encryption software, implementing the OpenPGP standard), within a few seconds. The attack sends a few carefully-crafted ciphertexts, and when these are decrypted by the target computer, they trigger the occurrence of specially-structured values inside the decryption software. These special values cause observable fluctuations in the electromagnetic field surrounding the laptop, in a way that depends on the pattern of key bits (specifically, the key-bits window in the exponentiation routine). The secret key can be deduced from these fluctuations, through signal processing and cryptanalysis. [“RSA key extraction via low-bandwidth acoustic cryptanalysis” (CRYPTO’14), “Get your hands off my laptop: physical side-channel key-extraction attacks on PCs” (CHES’14),*Stealing keys from PCs using a radio: cheap electromagnetic attacks on windowed exponentiation*, Daniel Genkin, Lev Pachmanov, Itamar Pipman, Eran Tromer, CHES 2015].

The Israeli team also extended the low-bandwidth attacks reported in the past, and detailed technical accounts of these attacks, to facilitate full reproducibility for future evaluators, are accepted for publication in prestigious journals. [*Acoustic cryptanalysis*, Daniel Genkin, Adi Shamir, Eran Tromer, Journal of Cryptology, 2016] [*Get your hands off my laptop: physical side-channel key-extraction attacks on PCs (extended version)*, Daniel Genkin, Itamar Pipman, Eran Tromer, Journal of Cryptographic Engineering, 2015]

In a complementary line of research, the Israeli group published a paper on methods for protecting implementations from tampering attacks, “Circuits resilient to additive attacks with applications to secure computation” (STOC, 14).
Also, they demonstrated key-recovery attacks on common cryptographic software implementations of Elliptic Curve Diffie Hellman encryption, as specified in the NIST SP800-56A standard, and implemented in GnuPG. This is the first published physical side-channel attack on elliptic curve cryptography running on a PC. By measuring the target's electromagnetic emanations, the attack extracts the secret decryption key within seconds, from a target located in an adjacent room across a wall. The attack utilizes a single carefully chosen ciphertext, and tailored time-frequency signal analysis techniques, to achieve full key extraction. We have disclosed our attack to GnuPG developers under CVE-2015-7511 and worked with the developers to implement countermeasures. GnuPG's Libgcrypt 1.6.5, containing these countermeasures and resistant to the key-extraction attack described here, was released concurrently with the public posting of these results. [Daniel Genkin, Lev Pachmanov, Itamar Pipman, Eran Tromer, ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs, proc. RSA Conference Cryptographers' Track (CT-RSA) 2016, LNCS 9610, 219-235, Springer, 2016].
The Israeli team, with collaborators, also demonstrated a new software-based side-channel attack that exploits information leaks through cache-bank conflicts in Intel processors. By detecting cache-bank conflicts via minute timing variations, we are able to recover information about victim processes running on the same machine. Our attack is able to recover both 2048-

bit and 4096-bit RSA secret keys from OpenSSL 1.0.2f running on modern Intel processors. This is despite the fact that OpenSSL's RSA implementation was carefully designed to be constant time in order to protect against cache-based (and other) side-channel attacks. This work is under submission.

Israeli partners (Daniel Genkin, Lev Pachmanov, Itamar Pipman, Adi Shamir, Eran Tromer, Yuval Yarom) published in Communications of the ACM, vol. 59 no. 6, 70-79, 2016 a paper about "Physical key extraction attacks on PCs" where they studied direct attacks against state-of-the-art cryptographic software.

Israeli partners (Yuval Yarom, Daniel Genkin, Nadia Heninger) presented a CHES 2016 their contribution to "CacheBleed: a timing attack on OpenSSL constant time RSA" (to appear in proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2016). The scatter-gather technique is a commonly-implemented approach to prevent cache-based timing attacks. In this paper they showed that scatter-gather is not constant-time. They implemented a cache timing attack against the scatter-gather implementation used in the modular exponentiation routine in OpenSSL version 1.0.2f. This attack exploits cache-bank conflicts on the Sandy Bridge microarchitecture. They have tested the attack on an Intel Xeon E5-2430 processor. For 4096-bit RSA this attack can fully recover the private key after observing 16,000 decryptions.

France

On the French side, we have worked on the theoretical and practical side of side-channel analysis against the post-quantum public key cryptosystems. We have developed theoretical studies of timing attacks, power analysis attacks and differential power analysis attack against the secret decoding algorithm used in McEliece (namely the Patterson algorithm). We have developed secure countermeasures and implemented them on specific devices. We also proposed new schemes for pseudo random generation, hashing and encryption. All our results have been published in international journals or international conferences with peer reviews.

More precisely, we found a novel countermeasure against a simple power analysis based side channel attack on a software implementation of the McEliece public key cryptosystem. First, we attacked a straightforward C implementation of the Goppa codes based McEliece decryption running on an ARM Cortex-M3 microprocessor. Next, we demonstrated on a realistic example that using a "chosen ciphertext attack" method, it is possible to recover the complete secret permutation matrix. We showed that this matrix can be completely recovered by an analysis of a dynamic power consumption of the microprocessor. Then, we estimated the brute-force attack complexity reduction depending on the knowledge of the permutation matrix. Finally, we proposed an efficient software countermeasure having low computational complexity. Of course, we provided all the necessary details regarding the attack implementation and all the consequences of the proposed countermeasure especially in terms of power consumption. [Countermeasure against the SPA Attack on an Embedded McEliece Cryptosystem. M. Petrvalsky, T. Richmond, M. Drutarovsky, P.-L. Cayrel and V. Fischer. Proceedings of MAREW 2015, IEEE, 2015]

A thorough analysis of the state of the art, we pointed out a missing solution for embedded devices to secure the syndrome computation. We showed that this weakness can open the door to a side-channel attack targeting the secret permutation. Indeed, brute-force attack iterations are dramatically decreased when the secret permutation is recovered. We demonstrated the feasibility of this attack against the McEliece cryptosystem implemented on an ARM Cortex-M3 microprocessor using Goppa codes. We explained how to recover the secret permutation on a toy example. Finally, we proposed a promising countermeasure, which can be implemented in embedded devices to prevent this attack. [A Side-Channel Attack Against the Secret Permutation on an Embedded McEliece Cryptosystem. T. Richmond, M. Petrvalsky and M. Drutarovsky TRUDEVICE 2015, Grenoble (France), Mars 2015.]

We also analysed the security and performance of two recent RFID authentication protocols based on two different schemes of code-based cryptography. The first was proposed by Malek and Miri based on randomized McEliece cryptosystem. The second was proposed by Li et al.

based on McEliece cryptosystem using Quasi Cyclic-Medium Density Parity Check (QC-MDPC) codes. We provided enough evidence to prove these two RFID authentication protocols are not secure. [Weaknesses in Two RFID Authentication Protocols. N. Chikouche, F. Cherif, P.-L. Cayrel and M. Benmohammed Proceedings of C2SI 2015, LNCS, Springer-Verlag, 2015.]

In 4 published papers in ICCC 2015, a wide variety of code-based cryptography aspects were studied. First we have proposed a new way to instantiate the McEliece cryptosystem using rank metric (called GPT) and using the well-known (u|u+v) construction. This approach offers a different security resistance (compare to the SD problem) and owns interesting performance features. The paper is untitled New GPT cryptosystem based on the (u|u+v)-construction codes by H. Moufek, R. Mahdjoubi, P.-L. Cayrel and K. Guenda ICCC 2015.

Second, we have proven the NP-completeness of the coset weight problem for a specific family of codes namely the quasi-dyadic codes. This theoretical result confirms the previous assumptions made in the literature. The paper is untitled NP-completeness of the coset weight problem for quasi-dyadic codes by P.-L. Cayrel, K. Diagne and C. T.Gueye in ICCC 2015.

Third, we have developed an efficient pseudo-random number generator based on worst case lattice problems (which is also an interesting candidate for the post-quantum era). We realised the implantation of the scheme on GPU and shown the efficiency of this construction compare to AES. The paper is untitled A pseudorandom number generator based on worst-case lattice problems by P.-L. Cayrel, M. Meziani, O. Ndiaye, R. Lindner and R. Silva in ICCC 2015.

Fourth, we have proposed a new fast and provably secure code-based stream cipher that we named SBS. This scheme is faster than the previous proposed schemes and keeps the same security level. We also implemented this scheme efficiently. The paper is untitled SBS: A Fast and Provably Secure Code-Based Stream Cipher by P.-L. Cayrel, M. Meziani and O. Ndiaye in ICCC 2015.

We have provided security arguments for signature schemes (which are useful for non post-quantum cryptosystems too) in the journal Design codes and cryptography (DCC 2016).

We have detailed several critical attacks against the McEliece PKC in the International Journal of Information and Coding Theory 2015.

We have also improved existing RFID Authentication Protocol based on Randomized McEliece Cryptosystem in the International Journal of Network Security.

We also developed DPA attacks on the Secure Bit Permutation in the McEliece PKC in RADIOELEKTRONIKA 2016.

French team published two papers (Inter. Journal of Information and Coding Theory (IJoICT) and Applicable Algebra in Engineering, Communication and Computing (AAECC)). The first one is dealing with lower bounds for Information Set Decoding over Fq and on the effect of Partial Knowledge. That topic is specially in the choice of the parameters for code-based cryptosystems. They proposed in this context lower bounds of the complexity for the ISD for codes defined over Fq.

The second one is a Pseudorandom Number Generator Based on Worst-Case Lattice Problems. Lattice problem are also post-quantum secure and the design of provably secure PRNG is an open problem for which we propose an answer in this publication.

Overview of the published results

According to the project goals we can split the results into theoretical results (related to cryptanalysis and parameters) and practical results (implementation, side channels). Due to the scientific nature of the project, there are also additional related results, akin to "a side product" of the main research. Note that some of the results cover both of the main categories. We will describe the accomplished results in more focused categories.

Theoretical results that focus on capabilities of quantum attacker include the following publications.

- M. Rötteler and R. Steinwandt: **A quantum circuit to find discrete logarithms on ordinary binary elliptic curves in depth O(log^2 n)**, Quantum Information & Computation, vol. 14, pp. 888-900, 2014.

- S. Kepley and R. Steinwandt: **Quantum circuits for F_{2^n}-multiplication with subquadratic gate count**, Quantum Information Processing, vol. 14, no. 7, pp. 2373-2386.
- P. Budhathoki and R. Steinwandt: **Automatic synthesis of quantum circuits for point addition on ordinary binary elliptic curves**, Quantum Information Processing, vol. 14, no. 1, pp. 201–216, 2015.
- M. Roetteler and R. Steinwandt: **A note on quantum related-key attacks**, Information Processing Letters, vol. 115, no. 1, pp. 40-44, 2015.
- M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt: **Applying Grover's Algorithm to AES: Quantum Resource Estimates**, Proceedings of Post-Quantum Cryptography 2016, vol. 9606 of Lecture Notes in Computer Science, pp. 29-43, Springer, 2016.

The focus of these articles is a deeper study of the cryptanalytic possibilities of the attacker that has a quantum computer available. The first three articles explore how quantum attacks on classical elliptic curve discrete logarithms can be improved by better quantum circuits. Furthermore, the goal is to automate the circuit synthesis process. The subsequent two articles focus on quantum attacks on symmetric ciphers. The research shows that quantum related-key attacks can be a very powerful tool for cryptanalysis. This attack has however strong requirements on superposition access to the block cipher. On the other hand, the last article shows that attacks that use Grover's algorithm are not straightforward as one might naively expect. In particular, for all three variants of AES (key size 128, 192, and 256 bit) that are standardized in FIPS-PUB 197, we establish precise bounds for the number of qubits and the number of elementary logical quantum gates that are sufficient to implement Grover's quantum algorithm to extract the key from a small number of AES plaintext-ciphertext pairs.

Theoretical security and parameters of lattice and code based schemes were studied in the following papers:

Ö. Dagdelen, D. Galindo, P. Véron, M. El Yousfi Alaoui and P.-L. Cayrel: **Extended Security Arguments for Signature Schemes,** Designs, Codes and Cryptography 78 (2016), 441-461.

In this paper we study generic signature schemes based on Fiat-Shamir transform, which can be instantiated by post-quantum schemes.

Vlad Dragoi, Pierre-Louis Cayrel , Brice Colombier and Tania Richmond: **Polynomial structures in code-based cryptography,** LNCS 8250, Springer-Verlag. Indocrypt 2013, Berlin, 2013, pp.286-296.
P.-L. Cayrel, K. Diagne and C. T.Gueye: **NP-completeness of the coset weight problem for quasi-dyadic codes, I**CCC **2015**, the Sixth International Conference on Computational Creativity (ICCC 2015). Park City, Utah, June 29 – July 2, 2015.
R.Niebuhr, E. Persichetti, P. - L. Cayrel, S. Bulygin and J. Buchmann, On lower bounds for Information Set Decoding over Fq and on the effect of Partial Knowledge, Inter. Journal of Information and Coding Theory, 2016.

These papers presents in more details theoretical results related to the security of code-based schemes. In the first paper, we show that the structure of polynomials with exactly t different roots is very dense and the probability that this type of polynomials has at least one coefficient equal to zero is extremely low. This leads to natural countermeasures to a timing attack against the polynomial evaluation in McEliece cryptosystem implementations. The second paper proves that coset weight problem for a family of quasi-dyadic codes is NP-complete. Thus, using these types of codes in post-quantum cryptography is as secure as using random linear codes. Finally, in the last paper, we give lower bounds for ISD over Fq. Our results allow to compute conservative parameters for cryptographic applications.

Otokar Grošek and Viliam Hromada: **On Generation of Error Vectors,** 16th Central European Conference on Cryptology (CECC 2016), June 22-24, Piešťany, Slovakia, to appear Tatra Mt. Math, Publ. 2016.

This paper presents new results from the study of error vector generation for McEliece cryptosystems. We summarize different techniques and propose more efficient methods based on equivalence classes of specific types of error vectors.

We have also published survey papers that summarize the security related features of the code based post-quantum systems:

P.-L. Cayrel, C. T. Gueye, O. Ndiaye and R. Niebuhr: **Critical attacks in code-based cryptography,** Internat. J. Information and Coding Theory 3 (2015), 158-176.
Repka, Marek, and Pavol Zajac. "Overview of the Mceliece Cryptosystem and its Security." Tatra Mountains Mathematical Publications 60.1 (2014): 57-83.

The first paper summarizes various specific attacks on various code-based systems, such as: Broadcast, Known Partial plaintext, Message-resend, Related-message, Chosen ciphertext, Lunchtime, Reaction attack and Malleability. The second paper summarizes the known facts about McEliece cryptosystem and its security, including the selection of parameters, existing implementations and side-channel attacks.

We have also studied, how to apply the post-quantum problems (decoding problem, lattice problems) to constructions of symmetric primitives:

P.-L. Cayrel, M. Meziani, O. Ndiaye et Q. Santos: **Efficient Software Implementations of Code-based Hash Functions and Stream-Ciphers,** Proceedings of WAIFI 2014, *LNCS 9061*, Springer-Verlag, Berlin, 2015, pp.187-203.
P.-L. Cayrel, M. Meziani and O. Ndiaye: **SBS : A Fast and Provably Secure Code-Based Stream Cipher,** ICCC 2015, pages 137-149
P.-L. Cayrel, M. Meziani, O. Ndiaye, R. Lindner and R. Silva: **A Pseudorandom Number Generator Based on Worst-Case Lattice Problem,** ICCC 2015 and to appear in Applicable Algebra in Engineering, Communication and Computing, 2016

The first paper is a survey of code based hash and stream ciphers (FSB, SFSB, RFSB, SYND, 2SC and XSYND). We also tried to improve their performances as software implementations which are done in C language by Using XMM registers from Streaming SIMD Extensions (SSE). The implementation provides a fair comparison of those primitives in the same platform. The next two papers are proposals of a new code-based stream cipher and lattice based pseudorandom generator. The advantage over standard primitives is an explicit reduction to hard computational problems.

From the implementation side, we were mostly working with various versions of the McEliece cryptosystem (MECS). MECS is an asymmetric cryptosystem as old as RSA, but with a main disadvantage of large keys. Our published implementations include:

Marek Repka: **McEliece PKC Calculator,** Journal of Electrical Engineering (65) 2014, 342-348.
Bitpunch team: **McEliece PKC Implementation,** https://github.com/FrUh/BitPunch
Andrej Boledovič and Juraj Varga: **Practical Implementation of McEliece Cryptosystem on Android,** 16th Central European Conference on Cryptology (CECC 2016), June 22-24, Piešťany, Slovakia, to appear Tatra Mt. Math, Publ. 2016.

The first paper describes an initial schoolbook implementation using NTL library that is useful for study of the system and generating of experimental and testing data. Our main

implementation is the BitPunch library, which is standalone C implementation of the McEliece cryptosystem. The modular architecture allows to use various codes (currently we have implemented Goppa codes and QC-MDPC codes in the main branch, and QC-LDPC codes in experimental branch). BitPunch library was used in further side-channel experiments (described later). We have also tried to implement a working messenger-type application that employs MECS on Android devices. The results are described in the last paper of this group: the encryption and decryption is fast, but problematic (as expected) is the key management (including ephemeral keys generation required for forward secrecy). Except these published implementations, we have laboratory versions of working MECS (or its core subsystem) implementations used in side-channel attacks (described later).

Marek Repka: **Note On Modular Reduction In Extended Finite Fields And Polynomial Rings For Simple Hardware, J**ournal of Electrical Engineering 67 (2016), 56-60.
Marek Repka: **Computing *p*th roots in extended finite fields of prime characteristic** $p \geq 2$, Electronics Letters 52 (2015), 718 –719.

The above two papers describe some of the techniques usable in MECS implementations.

A main focus of the project was the study of side-channel attacks against post-quantum systems. Our main object of the study was the McEliece cryptosystem. We have examined several attack vectors:

Marek Klein: **Side Channels in SW Implementation of the McEliece PKC,** *INFOCOMMUNICATIONS JOURNAL* 8.1 (2016): 10-16
This paper summarized results of a master thesis focused on study of SW timing attacks on McEliece cryptosystem. Experiments were performed with the BitPunch library. The most significant source of the leakage was the evaluation of the error locator polynomial. The paper describes several countermeasures that can improve the resistance against timing attacks, but at the cost of overall performance.

D. Bucerzan, P. - L. Cayrel, V. Dragoi and T. Richmond, Improved Timing Attacks against the Secret Permutation in the McEliece PKC, Inter. Journal of Computers Communications & Control, 12(1) 7-25, 2016

Another study of timing based attacks, with focus on recovering the secret permutation in the system. Provides two new timing attacks based on correlation between different steps of the decoding algorithm.

T. Richmond, M. Petrvalsky and M. Drutarovsky: **A Side-Channel Attack Against the Secret Permutation on an Embedded McEliece Cryptosystem,** TRUDEVICE 2015, Grenoble (France), Mars 2015, Electronically only at https://www.date-conference.com/proceedings1/2015/.
M. Petrvalsky, T. Richmond, M. Drutarovsky, P.-L. Cayrel and V. Fischer: **Countermeasure against the SPA Attack on an Embedded McEliece Cryptosystem,** Radioelektronika 2015, 25th International Conference, IEEE **Conference Publications**, 2015, pp. 462-466.

The above papers present a study of simple power analysis based attacks to reveal secret permutation of the McEliece system. The second paper expands on the possible countermeasures and their efficiency.

Cong Chen, Thomas Eisenbarth, Ingo von Maurich, Rainer Steinwandt: **Differential Power Analysis of a McEliece Cryptosystem**, Proc. ACNS 2015, LNCS 9062, Springer-Verlag, Berlin 2015. Pp. 538-556.

C. Chen, T. Eisenbarth, I. von Maurich, and R. Steinwandt: **Horizontal and Vertical Side Channel Analysis of a McEliece Cryptosystem**, IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, 1093-1105, 2016.
Cong Chen, Thomas Eisenbarth, Ingo von Maurich and Rainer Steinwandt: **Masking Large Keys in Hardware: A Masked Implementation of McEliece,** 22nd International Conference on Selected Areas in Cryptography (SAC 2015), LNCS 9566, Springer, Berlin 2016, pp. 293-309.
M. Petrvalsky, T. Richmond, M. Drutarovsky, P.-L. Cayrel and V. Fischer: **DPA on the Secure Bit Permutation in the McEliece PKC,** RADIOELEKTRONIKA 2016, IEEE, to appear

Finally, we conducted the first practical DPA attack on a McEliece cryptosystem that employs QC-MDPC codes. In the third paper we proposed and validate countermeasures to first-order DPA attacks. Finally, we also applied DPA techniques to recover the secret permutation (when using Goppa codes).

Marek Repka, Michal Varchola: **Correlation Power Analysis using Measured and Simulated Power Traces based on Hamming Distance Power Model – Attacking 16-bit Integer Multiplier in FPGA, I**nternational Journal of Computer Network and Information Security 7 (2015), 10-16.
Marek Repka, Michal Varchola and Miloš Drutarovský: **Improving CPA Attack Against DSA and ECDSA,** Journal of Electrical Engineering 66 (2015),159-163.

These additional papers apply the learned techniques also to standard platforms (with goal to attack DSA and ECDSA implementations). The attack on the multiplier can be useful for any implementation of the cryptosystem that uses an FPGA multiplier with protected data.

In the recent years, a lot of attention was obtained by acoustic attack presented by the Israeli team. During the project, a lot of new progress was done in this area, including extending these results to a new research area of low bandwidth side channel attacks. We summarize results from selected papers presenting the research progress:

Daniel Genkin, Adi Shamir, Eran Tromer: **RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis,** Advances in Cryptology - CRYPTO 2014/1, LNCS 8616, Springer-Verlag, Berlin, 2014, pp. 444-461.
Daniel Genkin, Adi Shamir, Eran Tromer: **Acoustic cryptanalysis, J**ournal of Cryptology 29 (2016), 1-52.

The original and extended version of the article describing acoustic cryptanalysis. We have been able to reproduce acoustic attacks also in Slovakia, and later on study stay in United States we have also studied acoustic channels in protected computers (still work in progress).

Daniel Genkin, Itamar Pipman and Eran Tromer: **Get your hands off my laptop: physical side-channel key-extraction attacks on PCs,** CHES 2014, LNCS 8731, Springer-Verlag, Berlin, 2014, pp. 242-260.
Daniel Genkin, Lev Pachmanov, Itamar Pipman, Eran Tromer: **Stealing keys from PCs using a radio: cheap electromagnetic attacks on windowed exponentiation, Proc.** CHES 2015, LNCS 9293, Springer, Berlin, pp. 207-228.
Daniel Genkin, Itamar Pipman, Eran Tromer: **Get your hands off my laptop: physical side-channel key-extraction attacks on PCs (extended version),** Journal of Cryptographic Engineering 5 (2015), 95-112.
Daniel Genkin, Lev Pachmanov, Itamar Pipman, Eran Tromer: r**ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs,** Proc. RSA Conference Cryptographers' Track (CT-RSA) 2016, LNCS 9610, Springer, Berlin, 2016, pp. 219-235
Daniel Genkin, Lev Pachmanov, Itamar Pipman, Adi Shamir, Eran Tromer, Yuval Yarom: **Physical key extraction attacks on PCs,** Communications of the ACM 59 (2016), 70-79.

These papers build on techniques learned from acoustic attacks and generalize the technique to so called low bandwidth cryptanalysis. The source side channel attack can be sampled with low frequency over various channels (electrical/network cables, even in short distance electromagnetic emanations). The technique is applied to RSA system, but can be generalized to post-quantum systems as well.

Yuval Yarom, Daniel Genkin, Nadia Heninger: **CacheBleed: a timing attack on OpenSSL constant time RSA,** Workshop on Cryptographic Hardware and Embedded Systems CHES 2016, LNCS 9813, Springer, Berlin, pp. 346-367.

Another source of vulnerabilities are timing attacks based on timing variations in cache accesses. This paper presents results from RSA system, but we also observed cache timing variations in BitPunch implementation (see thesis by M. Klein).

During the project, several papers were inspired by ideas discussed in the project, even if they do not directly solve the project problems:

Daniel Genkin, Yuval Ishai, Manoj M. Prabhakaran, Amit Sahai, Eran Tromer: **Circuits resilient to additive attacks with applications to secure computation,** 2014 ACM Symposium on Theory of Computing, STOC '14, ACM, 2014, pp. 495-504.

Peter Horak, Otokar Grošek: **A new approach towards the Golomb–Welch conjecture** , European Journal of Combinatorics 38 (2014), 12–22.

N. Chikouche, F. Cherif, P.-L. Cayrel and M. Benmohammed: **Weaknesses in Two RFID Authentication Protocols,** Proceedings of C2SI 2015, LNCS 9084, LNCS, Springer-Verlag, Berlin, 2015, pp. 162-172.
N. Chikouche, F. Cherif, P.-L. Cayrel and M. Benmohammed: **A Secure Code-Based Authentication Scheme for RFID Systems ,** Internat. J. Computer Network and Information Security 9 (2015), 1-9.
N. Chikouche, F. Cherif, P.-L. Cayrel and M. Benmohammed: **Improved RFID Authentication Protocol based on Randomized McEliece Cryptosystem,** nternational J. Network Security 17 (2015), 413-422.
H. Moufek, R. Mahdjoubi, P.-L. Cayrel and K. Guenda, **New GPT cryptosystem based on the (u|u+v)-construction codes,** ICCC **2015**, **I**CCC **2015**, the Sixth International Conference on Computational Creativity (ICCC 2015). Park City, Utah, June 29 – July 2, 2015.

Collaboration

detail the collaboration and consultation among co-directors and their groups

During the whole period of the Project all teams collaborated regularly, there were 5 fruitful meetings at TAU, and also there were many two side meetings on various international conferences. See also Project Participants and Roles.

Milestones & Deliverables

list project milestones and deliverables their current status; if they are not complete, explain and detail the impact on the project outcomes

Milestones:
M 1.1 Project setup, equipment ordering
M 1.2 Kick-off meeting
Deliverables:
D 1.1 Project WEB site

Milestones:
M 2.1 – Software implementations of selected algorithms are expected to be available for generating test vectors necessary for hardware testing before Step 3 will start. The test vectors must correspond to intermediate results on a step-by-step basis for both simplified and complete versions of functions which should be implemented in hardware.
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

Milestones:
M 3.1 – Selected hardware functions (described in VHDL) and the software, which will call these hardware functions are available for Step 5.
Deliverables:
D 3.1 – Configuration files, VHDL code and description of functions implemented in hardware are available for Step 5.
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 are available for Step 5.

Milestones:
M 4.1 – Fully operational setup to measure and process side-channel information such as power consumption are available for Step 5.
Deliverables:
D 4.1 – The code and executable files of the software aimed at controlling the measuring equipment are available for Step 5.

Milestones:
M 5.1 – We developed methods to carry out side-channel attacks against algorithms chosen in Step 2, based on simulated leakage.
Deliverables:
D 5.1 – We developed software to perform side-channel attacks based on simulated leakage

Milestones:
M 6.1 Traces and recommendations for mounting efficient side-channel attacks. These attacks are possible on some hardware configuration only. The results for TEMPEST computer are in progress.
M 6.2 Capability to extract confidential data from experimental data. This process will be automated.
Deliverables:
D 6.1. Aggregated data (traces for recommended parameter choice)
D 6.2. Software for extracting secret data from experimental data

Milestones:
M 7.1. Dissemination of results to a broader audience in a conference organized by the project partners.
Deliverables:
D 7.1. Workshop on Secure Implementation of Post-Quantum Cryptography took place at Tel Aviv University, Israel, on Sep 26 – 27, 2016. Here, the actual state of the art was presented by top ranking experts in the field. The whole program including presentations is available on the web page of our Project http://re-search.info/
Results of the project were also presented at the

- 16th Central European Conference on Cryptology that took place in Piestany, Slovakia, on June 22 – 24, Conference WEB: http://www.uim.elf.stuba.sk/cecc16/
- Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2016, http://www.chesworkshop.org/
- RSA Conference Cryptographers' Track (CT-RSA) 2016, https://jpn.nec.com/rd/event/ct-rsa16.html
- ArcticCrypt 2016, http://arcticcrypt.b.uib.no/
- 22nd Conference on Selected Areas in Cryptography (SAC 2015), http://mta.ca/sac2015/
- Post-Quantum Cryptography 2016, https://pqcrypto2016.jp/

Training & Professional Development

detail training and professional development activities

Several young scientists and students were involved in the Project on the French side. First of all, T. Richmond (who defended her PhD in October 2016), was the leader of the young research team containing two other students from Slovakia: Marek Klein and Martin Petrvalsky. Both were (is still be) working on implementation of side-channel attacks on the McEliece system.
One of the main aims of our Project was to involve young scientists and Master students to solve some partial problems of the Project. In Slovakia, 3 students were involved in development of BitPunch library during their master thesis: Andrej Gulyás (implementation of QC-MDPC codes), Marek Klein (timing attacks), and František Uhrecký (general BitPunch development and integration). Furthermore, two teams of first-year MSc. students (10 students) learned to work with microprocessor boards, side-channel measurements and BitPunch library led by our young post-docs Viliam Hromada and Ondrej Gallo, and our PhD. student Tomáš Fabšič.
The project SfP G4520 was working as a great motivation for students in Slovakia to focus on research topics during their study of information security. In the study year 2015/16, we have realized the following bachelor and master theses related to the project:
Andrej Boledovic (MSc. thesis) - Using McEliece cryptosystem in OS Android
Pavol Dobrocka (MSc. thesis) - Signature schemes in post-quantum cryptography
Martin Orem (MSc. thesis) - Secure implementation of McEliece cryptosystem
Radovan Bezak (Bc. thesis) - QC-MDPC McEliece on microprocessor
We also involved a team of 5 first-year MSc. students that implemented the QC-LDPC codes into the BitPunch cryptographic library.
In the academic year 2016/17 we have another team of 5 first-year MSc. students, this time their goal is to continue in the work of their colleagues from the previous year and adapt the aforementioned attack on QC-MDPC codes on the QC-LDPC codes implemented in BitPunch.

Also in line with this goal, the collaboration of the U.S. partner with WPI and Univ. Bochum has involved young scientists, who have not completed their Ph.D. thesis yet. For the development of the masked McEliece implementation, the contributions of a Ph.D. student were essential.
A known algebraic (distinguishing) attack against McEliece when using Goppa Codes was explored by the student Hai Pham working on his Master's thesis (using the computer algebra system Magma as convenient platform). The thesis has been defended successfully. Moreover, another Ph.D. student at the U.S. partner institution played a key role in analyzing the quantum resources for attacking the symmetric component of a hybrid scheme when using AES (Brandon Langenberg). Two Ph.D. students (Brandon Langenberg and Brittanney Amento) were involved in the quantum cryptanalysis of Serpent and MARS, and we are pleased to report that one of them (Brittanney Amento) completed her Ph.D. thesis during this project, with her quantum cryptanalytic findings being part of the Ph.D. thesis.
For the work on quantum circuits related to elliptic curve arithmetic, the graduate students Shane Kepley and Parshuram Budhathoki were involved.

In the Israeli team, 6 young scientists (graduate students and research assistants) are involved in the research. Of these, 3 are already authors of published or forthcoming papers. We have also upgraded some of these from part-time research assistants to full-time graduate students, for deeper training.

Several young scientists and students were involved in the Project on the French side. First of all, T. Richmond, which is the leader of the young research team containing at the moment two other students from Slovakia: Marek Klein and Martin Petrvalsky. Both are working on implementation of side-channel attacks on the McEliece system.

The Israeli team has integrated some of this project's results into undergraduate and graduate teaching curriculum, educating hundreds of students about the risk of physical and software side-channel attacks, and mitigation approach.

On June 25-27, 2014 in Slovakia we organized a course Best Practices in Cryptology and Information Security for 4 US and 10 Slovakian students on the topic close to this Project.
.
8 Norwegian students and 8 Slovakian students participated in Bratislava-Crypt, November 09-13, 2015. This intensive course covered some basic topics in cryptography including side-channel attacks, with practical examples of attacks against public key cryptosystems.
From 20th to 23rd October, Rainer Steinwandt, Ondrej Gallo and Tomas Fabsic visited the Worcester Polytechnic Institute, Massachusetts, USA as guests of one of our experts Thomas Eisenbarth. The aim of the visit was to conduct the first known analysis of the vulnerability of a Tempest computer against low-frequency side channel attacks.
Low-frequency side channel attacks were invented by Daniel Genkin, Adi Shamir, Eran Tromer and Itamar Pipman and were presented in papers RSA key extraction via low-bandwidth acoustic cryptanalysis and Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks On PCs in 2014. Unlike traditional physical side channel attacks, low-frequency side channel attacks exploit signals at much lower frequencies. Relevant signals for low-frequency side channel attacks include acoustic signals from a laptop, electric potential signals from a laptop chassis and electromagnetic signals from a laptop. By a careful examination of these signals, Genkin, Shamir, Tromer and Pipman were able to extract the secret key from implementations of RSA and El Gamal running on various commercial laptops. These results have been successfully repeated at STU in Bratislava. However, no low-frequency attacks on Tempest computers have been published in the literature.
The novelty of low-frequency side channel attacks lead Dr. Steinwandt, Dr. Eisenbarth, Dr. Gallo and Mr. Fabsic to the hypothesis that even Tempest computers may be vulnerable to low-frequency side channel attacks. The analysis conducted during their stay at the Worcester Polytechnic Institute confirms this hypothesis. During their stay Dr. Steinwandt, Dr. Eisenbarth, Dr. Gallo and Mr. Fabsic conducted measurements of acoustic and electric potential signals

from a Tempest laptop. They concluded that in both types of signal it is clearly distinguishable when the laptop performs an RSA decryption and when it is at rest. During their experiments, Dr. Steinwandt, Dr. Eisenbarth, Dr. Gallo and Mr. Fabsic were assisted by inventors of low-frequency attacks, Daniel Genkin and Eran Tromer, with whom they consulted their experimental setup and their observations via email.

Impact

describe the impact of the project on the scientific community and the public

The theoretical insights helped to advance quantum cryptanalysis. In particular, our results made the scientific community aware that for symmetric cryptography the implications of quantum computing are significantly more subtle than just “double all key lengths.” Gate-level analysis of cryptographic algorithms has received more attention by now – just recently work on hash functions has been published by colleagues not involved in this project. Our experimental results were ground-breaking in the sense that we had for the first time an implementation of a DPA against a post-quantum proposal that was not known to be vulnerable to this type of attack. Our work on low-bandwidth side-channels opened up a completely new line of work in side-channel attacks – the attacks resulted in strong reactions from popular press and actually deployed software has been updated such that the attack is not immediately applicable.

Implementation

detail how the results of this project have been, are being, and will be implemented

It is expected that results on McEliece from this project will inform the post-quantum standardization process – cf. the NIST initiative in the U.S. We provided practical attack implementations and implemented countermeasures in an academic/lab settings. To what extent some of the results will influence products in a wider/commercial market is likely to depend on the outcome of standardization efforts. If a McEliece variant will be standardized, our results have a good chance of helping with the development of secure implementations for a broader market. Our work on low-bandwidth side-channels already resulted in an update of deployed cryptographic software.

Project Participants and Roles

list the participants in the project and the rough fraction of their time spent on it; describe briefly how each contributed to the project; add or subtract rows as needed

The joint research was carried out by four teams, who collaborated in this constellation the first time, but earlier bilateral collaborations ensured a smooth start, and based on the prior experiences. An efficient handling of the diverse tasks in this project was done smoothly. All involved teams had an extensive background in cryptology, and in their collaboration covered all project-specific competences, ranging from quantum cryptanalysis to soft- and hardware implementations and experimental work with side-channel attacks.

The main share of the implementation work was done mostly at Tel Aviv University, Jean Monnet University, and also Slovak Technical University, and Florida Atlantic University. The complementary measurement facilities in Slovakia and Israel enabled the teams to proceed in parallel on performing the research on different schemes or platforms. Both groups have substantial experience with the implementation of cryptographic schemes. Partners in Slovakia and the U.S.A. have an established track record in the theoretical analysis of cryptographic schemes aiming at a post-quantum setting.

Name	Affiliation	Position/Title	% Time	Role
Dr. Eran Tromer	TAU	Senior Lecturer	25%	PPD; technical coordination and management, kick-off meeting
Prof. Avishai Wool	TAU	Professor	15%	Cryptanalytic analysis and experimental design
Daniel Genkin	TAU	PhD student	50%	Cryptanalytic analysis and measurement control
Itamar Pipman	TAU	MSc student	25%	Hardware implementation and measurement control
Lev Pachmanov	TAU	Research assistant	25%	Software implementation
Ezra Shaked	TAU	Engineer	5%	Lab equipment construction and maintenance
Prof.Otokar Grošek	STU	Director	30%	NPD; technical and administration coordination, contact with end-users, plan, kick-off meeting implementation
Dr. Pavol Zajac	STU	Assoc. Prof.	30%	Processing measured data, design of software implementation, Software for extracting secret data from experimental data.
Dr. Michal Mikuš	STU	Senior lecturer	30%	Processing measured data, design of software implementation
Marek Repka	STU	PhD. student	60%	Processing measured data, design of software implementation, preparation of test vectors, hardware implementation
Dr. Matúš Jókay	STU	Senior lecturer	30%	Processing measured data, design of software implementation
Dr. Ondrej Gallo	STU	Senior lecturer	10%	Design of hardware implementation
Dr. Viliam Hromada	STU	Senior lecturer	10%	Design of hardware implementation
Tomáš Fabšic	STU	PhD Student	30%	Processing measured data, design of software implementation
Prof. Viktor Fischer	JMU	Professor	30%	Co-Director, Configuration files, VHDL code and description of functions implemented in hardware
Prof. Pierre – Louis Cayrel	JMU	Assoc. Prof.	20%	The code and executable files of the software implementing selected algorithms and running on the PC, while calling functions implemented in hardware
Tania Richmond	JMU	PhD Student	60%	**Software to perform side-channel attacks based on simulated leakage**
Nathalie Bochard	JMU	Engineer	20%	Aggregated data, traces for recommended parameter choice
Prof. Alain Aubert	JMU	Assoc. Prof.	20%	Hardware implementation of selected functions
Prof. Lilian Bossuet	JMU	Assoc. Prof.	10%	Evaluation of vulnerabilities to side-channel attacks against algorithms chosen in Step 2, based on simulated leakage
Dr. Rainer Steinwandt	FAU	Professor	20%	Co-Director help with technical and administration coordination, identification of methods which are able to withstand side-channel attacks
Dr. Spyros Magliveras	FAU	Professor	15%	Identification of suitable post-quantum cryptographic schemes, final conference with external participants
Brittanney Amento	FAU	PhD. student	50%	Realization of selected algorithms in software, identification of functionality
Brandon Langenberg	FAU	PhD. student	50%	Realization of selected algorithms in software, identification of functionality

Criteria for Success

list the Criteria for Success established in the Project Plan and your evaluation of their completion

Criterion	Relative Weight	Complete	Comments
Project set up and realization of kick-off meeting.	5%	5%	Kick-off meeting, December 8-11, 2013
D 2.1 – Software implementations (the source code) of selected algorithms	10%	10%	Bitpunch library McEliece PKC calculator
D 2.2 – Test vectors of functions that have to be implemented in hardware	8%	8%	Generated by "McEliece PKC Calculator ".
D 3.1 – Configuration files, VHDL code and description of functions implemented in hardware	8%	8%	Configuration files and VHDL code was developed
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	10%	10%	Code and executable files were developed in cooperation of all partners, and at various implementations. Details in published MSc. theses.
D 4.1 – The code and executable files of the software aimed at controlling the measuring equipment	8%	8%	Code and executable files were developed in cooperation of all partners, and used in further experiments.
D 5.1 – Software to perform side-channel attacks based on simulated leakage	10%	10%	Software was developed in cooperation of all partners, and used in further experiments.
D 6.1. Aggregated data (power traces for recommended parameter choice)	8%	8%	Data traces were obtained in experiments by the help of previous software tools and aggregated data presented in published papers.
D 6.2. Software for extracting secret data from experimental data	13%	13%	Key extraction software was developed both in IL and SK
D 7.1. Meeting/conference with external participants	5%	5%	Held at TAU, Tel Aviv, see WEB page
Training of young Israeli and NATO scientists.	10%	10%	Young SK and US scientists in cooperation with IL young scientists performed measurements in US.
Dissemination of results by publishing in journal and proceeding papers, and conference contributions.	5%	5%	46 papers published/ (5 in progress)
Total	100%	100%	

Products & Dissemination

please list all products and outcomes of the project

Journal articles, conference papers, book chapters, and other publications (please do not attach copies)

1. Martin Roetteler, Rainer Steinwandt: **A quantum circuit to find discrete logarithms on ordinary binary elliptic curves in depth O(log^2 n)**, Quantum Information & Computation **14** (2014), 888-900.
2. Vlad Dragoi, Pierre-Louis Cayrel , Brice Colombier and Tania Richmond: **Polynomial structures in code-based cryptography,** LNCS 8250, Springer-Verlag. Indocrypt 2013, Berlin, 2013, pp.286-296.
3. Daniel Genkin, Adi Shamir, Eran Tromer: **RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis,** Advances in Cryptology - CRYPTO 2014/1, LNCS 8616, Springer-Verlag, Berlin, 2014, pp. 444-461.
4. Peter Horak, Otokar Grošek: **A new approach towards the Golomb–Welch conjecture** , European Journal of Combinatorics **38** (2014), 12–22.
5. Marek Repka: **McEliece PKC Calculator,** Journal of Electrical Engineering (**65**) 2014, 342-348.
6. Daniel Genkin, Itamar Pipman and Eran Tromer: **Get your hands off my laptop: physical side-channel key-extraction attacks on PCs,** CHES 2014, LNCS 8731, Springer-Verlag, Berlin, 2014, pp. 242-260.

7. Bitpunch team: **McEliece PKC Implementation,** https://github.com/FrUh/BitPunch
8. Martin Roetteler and Rainer Steinwandt: **A note on quantum related-key attacks,** Information Processing Letters **115** (2015), 40–44.
9. S. Kepley and R. Steinwandt: **Quantum circuits for F_{2^n}-multiplication with subquadratic gate count**, Quantum Information Processing, vol. 14, no. 7, pp. 2373-2386.
10. P. Budhathoki and R. Steinwandt: **Automatic synthesis of quantum circuits for point addition on ordinary binary elliptic curves,** Quantum Information Processing 14 (2015), 201–216.
11. P.-L. Cayrel, M. Meziani, O. Ndiaye et Q. Santos: **Efficient Software Implementations of Code-based Hash Functions and Stream-Ciphers,** Proceedings of WAIFI 2014, LNCS 9061, Springer-Verlag, Berlin, 2015, pp.187-203.
12. C. Chen, T. Eisenbarth, I. von Maurich, and R. Steinwandt: **Horizontal and Vertical Side Channel Analysis of a McEliece Cryptosystem**, IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, 1093-1105, 2016.
13. Daniel Genkin, Yuval Ishai, Manoj M. Prabhakaran, Amit Sahai, Eran Tromer: **Circuits resilient to additive attacks with applications to secure computation,** 2014 ACM Symposium on Theory of Computing, STOC '14, ACM, 2014, pp. 495-504.
14. Cong Chen, Thomas Eisenbarth, Ingo von Maurich, Rainer Steinwandt: **Differential Power Analysis of a McEliece Cryptosystem, Proc.** ACNS 2015, LNCS 9062, Springer-Verlag, Berlin 2015. Pp. 538-556.
15. Marek Repka, Michal Varchola: **Correlation Power Analysis using Measured and Simulated Power Traces based on Hamming Distance Power Model – Attacking 16-bit Integer Multiplier in FPGA, I**nternational Journal of Computer Network and Information Security **7** (2015), 10-16.
16. Marek Repka, Michal Varchola and Miloš Drutarovský: **Improving CPA Attack Against DSA and ECDSA,** Journal of Electrical Engineering **66** (2015),159-163.
17. Cong Chen, Thomas Eisenbarth, Ingo von Maurich and Rainer Steinwandt: **Masking Large Keys in Hardware: A Masked Implementation of McEliece,** 22nd International Conference on Selected Areas in Cryptography (SAC 2015), LNCS 9566, Springer, Berlin 2016, pp. 293-309.
18. Daniel Genkin, Lev Pachmanov, Itamar Pipman, Eran Tromer: **Stealing keys from PCs using a radio: cheap electromagnetic attacks on windowed exponentiation,** Proc. CHES 2015, LNCS 9293, Springer, Berlin, pp. 207-228.
19. Daniel Genkin, Adi Shamir, Eran Tromer: **Acoustic cryptanalysis,** Journal of Cryptology **29** (2016), 1-52.
20. Daniel Genkin, Itamar Pipman, Eran Tromer: **Get your hands off my laptop: physical side-channel key-extraction attacks on PCs (extended version),** Journal of Cryptographic Engineering **5** (2015), 95-112.
21. M. Petrvalsky, T. Richmond, M. Drutarovsky, P.-L. Cayrel and V. Fischer: **Countermeasure against the SPA Attack on an Embedded McEliece Cryptosystem,** Radioelektronika 2015, 25th International Conference, IEEE Conference Publications, 2015, pp. 462-466.
22. T. Richmond, M. Petrvalsky and M. Drutarovsky: **A Side-Channel Attack Against the Secret Permutation on an Embedded McEliece Cryptosystem,** TRUDEVICE 2015, Grenoble (France), Mars 2015, Electronically only at https://www.date-conference.com/proceedings1/2015/.
23. N. Chikouche, F. Cherif, P.-L. Cayrel and M. Benmohammed: **Weaknesses in Two RFID Authentication Protocols,** Proceedings of C2SI 2015, LNCS 9084, LNCS, Springer-Verlag, Berlin, 2015, pp. 162-172.

24. Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt: **Applying Grover's algorithm to AES: quantum resource estimates,** PQCrypto 2016, LNCS 9606, Springer, Berlin, 2016, pp. 29-43.
25. Marek Repka: **Note On Modular Reduction In Extended Finite Fields And Polynomial Rings For Simple Hardware,** Journal of Electrical Engineering **67** (2016), 56-60.
26. Marek Repka: **Computing *p*th roots in extended finite fields of prime characteristic *p* ≥ 2,** Electronics Letters 52 (2015), 718 –719.
27. P.-L. Cayrel, M. Meziani and O. Ndiaye: **SBS : A Fast and Provably Secure Code-Based Stream Cipher,** ICCC 2015, pages 137-149
28. P.-L. Cayrel, M. Meziani, O. Ndiaye, R. Lindner and R. Silva: **A Pseudorandom Number Generator Based on Worst-Case Lattice Problem,** ICCC 2015 and to appear in Applicable Algebra in Engineering, Communication and Computing, 2016
29. Ö. Dagdelen, D. Galindo, P. Véron, M. El Yousfi Alaoui and P.-L. Cayre: **Extended Security Arguments for Signature Schemes,** Designs, Codes and Cryptography **78** (2016), 441-461.
30. P.-L. Cayrel, C. T. Gueye, O. Ndiaye and R. Niebuhr: **Critical attacks in code-based cryptography,** Internat. J. Information and Coding Theory **3** (2015), 158-176.
31. N. Chikouche, F. Cherif, P.-L. Cayrel and M. Benmohammed: **A Secure Code-Based Authentication Scheme for RFID Systems ,** Internat. J. Computer Network and Information Security **9** (2015), 1-9.
32. N. Chikouche, F. Cherif, P.-L. Cayrel and M. Benmohammed: **Improved RFID Authentication Protocol based on Randomized McEliece Cryptosystem,** nternational J. Network Security 17 (2015), 413-422.
33. M. Petrvalsky, T. Richmond, M. Drutarovsky, P.-L. Cayrel and V. Fischer: **DPA on the Secure Bit Permutation in the McEliece PKC,** RADIOELEKTRONIKA 2016, IEEE, to appear
34. Yuval Yarom, Daniel Genkin, Nadia Heninger: **CacheBleed: a timing attack on OpenSSL constant time RSA,** Cryptology ePrint Archive: Report 2016/224
35. Daniel Genkin, Lev Pachmanov, Itamar Pipman, Eran Trome: r**ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs,** Proc. RSA Conference Cryptographers' Track (CT-RSA) 2016, LNCS 9610, Springer, Berlin, 2016, pp. 219-235
36. Andrej Boledovič and Juraj Varga: **Practical Implementation of McEliece Cryptosystem on Android,** 16th Central European Conference on Cryptology (CECC 2016), June 22-24, Piešťany, Slovakia, to appear Tatra Mt. Math, Publ. 2016.
37. Otokar Grošek and Viliam Hromada: **On Generation of Error Vectors,** 16th Central European Conference on Cryptology (CECC 2016), June 22-24, Piešťany, Slovakia, to appear Tatra Mt. Math, Publ. 2016.
38. Daniel Genkin, Lev Pachmanov, Itamar Pipman, Adi Shamir, Eran Tromer, Yuval Yarom: **Physical key extraction attacks on PCs,** Communications of the ACM 59 (2016), 70-79.
39. Yuval Yarom, Daniel Genkin, Nadia Heninger: **CacheBleed: a timing attack on OpenSSL constant time RSA,** Workshop on Cryptographic Hardware and Embedded Systems CHES 2016, LNCS 9813, Springer, Berlin, pp. 346-367.
40. Marek Klein: **Side Channels in SW Implementation of the McEliece PKC,** *INFOCOMMUNICATIONS JOURNAL* 8.1 (2016): 10-16

41. Pavol Marák: **Post-quantum cryptography: NATO project at the FEI,** SPEKTRUM, Journal of Slovak University of Technology, Academic year 2014/2015, Volume XXI., Issue 5
42. H. Moufek, R. Mahdjoubi, P.-L. Cayrel and K. Guenda, **New GPT cryptosystem based on the (u|u+v)-construction codes,** ICCC **2015**, ICCC **2015**, the Sixth International Conference on Computational Creativity (ICCC 2015). Park City, Utah, June 29 – July 2, 2015.
43. P.-L. Cayrel, K. Diagne and C. T.Gueye: **NP-completeness of the coset weight problem for quasi-dyadic codes,** ICCC **2015**, the Sixth International Conference on Computational Creativity (ICCC 2015). Park City, Utah, June 29 – July 2, 2015.
44. D. Bucerzan, P. - L. Cayrel, V. Dragoi and T. Richmond ,**Improved Timing Attacks against the Secret Permutation in the McEliece PKC**, Inter. Journal of Computers Communications & Control, 12(1) 7-25, 2016
45. R.Niebuhr, E. Persichetti, P. - L. Cayrel, S. Bulygin and J. Buchmann, **On lower bounds for Information Set Decoding over Fq and on the effect of Partial Knowledge**,Inter. Journal of Information and Coding Theory, 2016.
46. M. Repka, P. Zajac: Overview **of the Mceliece Cryptosystem and its Security** Tatra Mt. Math. Pub., Volume 60, 2014, 57-83

Conference presentations and public lectures

1. Pierre-Louis Cayrel gave an invited lecture on **code-based cryptography** in AFRICAN MATHEMATICAL SCHOOL, Cameroon (website : http://httcbambili.com/AMS/)
2. Pierre-Louis Cayrel gave an invited lecture on **code-based cryptography** in AIMS, Senegal (website : http://www.aims-senegal.org/)
3. Vlad Dragoi, Pierre-Louis Cayrel , Brice Colombier and Tania Richmond: **Polynomial structures in code-based cryptography,** Indocrypt 2013
4. Daniel Genkin, Adi Shamir, Eran Tromer: **RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis,** Advances in Cryptology - CRYPTO 2014
5. Daniel Genkin, Itamar Pipman and Eran Tromer: **Get your hands off my laptop: physical side-channel key-extraction attacks on PCs,** CHES 2014
6. P.-L. Cayrel, M. Meziani, O. Ndiaye et Q. Santos: **Efficient Software Implementations of Code-based Hash Functions and Stream-Ciphers,** Proceedings of WAIFI 2014
7. Daniel Genkin, Yuval Ishai, Manoj M. Prabhakaran, Amit Sahai, Eran Tromer: **Circuits resilient to additive attacks with applications to secure computation,** 2014 ACM Symposium on Theory of Computing, STOC '14, ACM, 2014
8. Cong Chen, Thomas Eisenbarth, Ingo von Maurich, Rainer Steinwandt: **Differential Power Analysis of a McEliece Cryptosystem, Proc.** ACNS 2015
9. Cong Chen, Thomas Eisenbarth, Ingo von Maurich and Rainer Steinwandt: **Masking Large Keys in Hardware: A Masked Implementation of McEliece,** 22nd International Conference on Selected Areas in Cryptography (SAC 2015
10. Daniel Genkin, Lev Pachmanov, Itamar Pipman, Eran Tromer: **Stealing keys from PCs using a radio: cheap electromagnetic attacks on windowed exponentiation,** CHES 2015
11. M. Petrvalsky, T. Richmond, M. Drutarovsky, P.-L. Cayrel and V. Fischer: **Countermeasure against the SPA Attack on an Embedded McEliece Cryptosystem,** Radioelektronika 2015, 25th International IEEE Conference

12. T. Richmond, M. Petrvalsky and M. Drutarovsky: **A Side-Channel Attack Against the Secret Permutation on an Embedded McEliece Cryptosystem,** TRUDEVICE 2015, Grenoble (France), Mars 2015,
13. N. Chikouche, F. Cherif, P.-L. Cayrel and M. Benmohammed: **Weaknesses in Two RFID Authentication Protocols,** C2SI 2015,
14. Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt: **Applying Grover's algorithm to AES: quantum resource estimates,** PQCrypto 2016,
15. P.-L. Cayrel, M. Meziani and O. Ndiaye: **SBS : A Fast and Provably Secure Code-Based Stream Cipher,** ICCC 2015
16. P.-L. Cayrel, M. Meziani, O. Ndiaye, R. Lindner and R. Silva: **A Pseudorandom Number Generator Based on Worst-Case Lattice Problem,** ICCC 2015
17. Daniel Genkin, Lev Pachmanov, Itamar Pipman, Eran Trome: r**ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs,** RSA Conference Cryptographers' Track (CT-RSA) 2016,
18. Andrej Boledovič and Juraj Varga: **Practical Implementation of McEliece Cryptosystem on Android,** 16th Central European Conference on Cryptology (CECC 2016), June 22-24, Piešťany, Slovakia
19. Otokar Grošek and Viliam Hromada: **On Generation of Error Vectors,** 16th Central European Conference on Cryptology (CECC 2016), June 22-24, Piešťany, Slovakia
20. Yuval Yarom, Daniel Genkin, Nadia Heninger: **CacheBleed: a timing attack on OpenSSL constant time RSA,** Workshop on Cryptographic Hardware and Embedded Systems CHES 2016
21. H. Moufek, R. Mahdjoubi, P.-L. Cayrel and K. Guenda, **New GPT cryptosystem based on the (u|u+v)-construction codes,** ICCC **2015**, **I**CCC **2015**, the Sixth International Conference on Computational Creativity (ICCC 2015). Park City, Utah, June 29 – July 2, 2015.
22. P.-L. Cayrel, K. Diagne and C. T.Gueye: **NP-completeness of the coset weight problem for quasi-dyadic codes, I**CCC **2015**, the Sixth International Conference on Computational Creativity (ICCC 2015). Park City, Utah, June 29 – July 2, 2015.
23. Rainer Steinwandt: **Understanding the cost of Grover's algorithm for finding a secret key**, Workshop on Secure Implementation of Post-Quantum Cryptography, Tel Aviv University Israel, Sep 26 – 27, 2016
24. Pierre-Louis Cayrel: **Our results in side-channel analysis of the McEliece PKC using binary Goppa codes and more general results in code-based cryptography, software implementations and secure designs,** Workshop on Secure Implementation of Post-Quantum Cryptography, Tel Aviv University Israel, Sep 26 – 27, 2016
25. Eran Tromer: **Physical Side Channel Attacks on PCs,** Workshop on Secure Implementation of Post-Quantum Cryptography, Tel Aviv University Israel, Sep 26 – 27, 2016
26. Pavol Zajac: **McEliece in practice,** Workshop on Secure Implementation of Post-Quantum Cryptography, Tel Aviv University Israel, Sep 26 – 27, 2016
27. Viliam Hromada: **Side channel analysis of McEliece cryptosystem,** Workshop on Secure Implementation of Post-Quantum Cryptography, Tel Aviv University Israel, Sep 26 – 27, 2016

Inventions, Patents, & Licenses

N/A

Other products such as web sites, databases, etc. released to the scientific community or the public

Web site of the Project: http://re-search.info/
Web site of the French team: http://cayrel.net/?Code-based-cryptography-133

Project publicity (please attach copies of articles or reports about the project)

- A short Information about the project in a morning radio talkshow "Dobre ráno Slovensko" by O. Grošek. Rádio Slovensko, Morning radio talkshow "Dobré ráno Slovensko", 11. 03. 2016 at 06:09. Title [slovak/english] - Niektoré šifry odolávajú / Some ciphers still resist. Available at our WEB page. Information about the project in a night radio talkshow "Nočná Pyramída" by O. Grošek, Rádio Slovensko, Night radio talkshow "Nočná Pyramída", 06. 04. 2016 at 22:00 - 24:00. Available at our WEB page.
- Pavol Marák: **Post-quantum cryptography: NATO project at the FEI,** SPEKTRUM, Journal of Slovak University of Technology, Academic year 2014/2015, Volume XXI., Issue 5
- The paper Daniel Genkin, Adi Shamir, Eran Tromer: "**RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis"** has extremely large media coverage, including Forbes, The Economist, NBC News, Channel 4 News and The Telegraph, Wikipedia, etc. The paper Daniel Genkin, Itamar Pipman Eran Tromer, "Get your hands off my laptop: physical side-channel key-extraction attacks on PCs" likewise had extensive exposure, including Sky News and MIT Technology Review.
- Moreover, within Florida's State University System, a Florida Center for Cybersecurity has been established, and in the first meeting of the advisory council for this center (with representatives of all twelve member institutions of Florida's state university system), the co-director of the U.S. partner gave, as a member of this council, a presentation pointing out this project.
- Pavol Zajac and Viliam Hromada during their stay at University of Washington Tacoma gave invited talks on topics of side-channel attacks and introduced some of the goals of the project and its current results.
- The Israeli team has presented and gave live demonstrations of some of the projects results at several large conferences (CHES'14, CRYPTO'14, CHES'15, CRYPTO'15, CECC'15), industry labs (including Microsoft and Google), and university courses.
- Some our research findings have received very wide exposure (hundreds of articles) in popular media, including BBC, Business Insider, Economist, Forbes, Ha'aretz, Heise Online, Le Monde, MIT Technology Review, NBC News, NU.nl, PCWorld, Sky News, and many others. New media exposure, in this reporting period, includes: Ars Technica, VICE Motherboard, The Register and Linux Weekly News.
- The US partner gave invited presentations in Canada and Germany, presented a paper in Canada, and the quantum cryptanalysis seminar co-organized in Germany was picked up, e.g., by Nature. One paper was presented at PQCrypto 2016, and it has been approved that PQCrypto 2018 will take place in the service region of FAU, organized by the US co-director of this project. A workshop by NIST on post-quantum cryptography is anticipated to be at FAU.
- Our various papers' web sites were viewed by half a million visitors.
- The co-director of the U.S. partner gave a presentation to an advisory board which involves representatives from the private sector in the FAU service area. This should help to popularize this line of work beyond the academic sector.

- V. Fischer and T. Richmond took part in the COST Action workshop in Grenoble in March 2015, where they presented recent results of the Project.
- The US partner is currently involved in a research project with the Air Force Research Laboratory, and so the university communicates with the Air Force on a somewhat regular basis about cryptography and cybersecurity research at FAU. Results from this project (specifically about side-channel attacks and quantum cryptanalysis) are incorporated in such presentations. The US partner is currently also preparing to host PQCrypto 2018 in Ft. Lauderdale, which is to be collocated with a workshop by NIST on post-quantum cryptography.
- Since Military Intelligence Service of the Slovak Republic is one of our end-users, O. Grosek presented 24. 11. 2016 for Military Intelligence Service Oversight Special Committee of the National Council of the Slovak Republic results gained by the researchers involved in this NATO Project. (The Oversight Committee meetings are not public. The Committee shall meet at least once every quarter. Discussions must proceed in accordance with Rules of Procedure of the Committee. Convening the committee may be called for by any member of the Committee. Committee members and other persons who participate in or are present at the meeting of the Committee, once their participation is approved by members of the Committee, are obliged to maintain confidentiality about the facts learned in this proceeding and respect the protection of classified information under special regulations.)