Workshop on Secure Implementation of Post-Quantum Cryptography

26-27 September 2016

Tel Aviv University

This program is available electronically at:
`http://cs.tau.ac.il/~tromer/sipqc16.pdf`

Program

Monday, September 26th

9:30-10:30	Thomas Eisenbarth *Side Channel Analysis and Protection for McEliece Implementations*
10:30-11:00	Coffee Break
11:00-11:45	Pierre-Louis Cayrel *Side Channel Analysis of the McEliece PKC Using Binary Goppa Codes*
11:45-12:15	Rainer Steinwandt *Understanding the Cost of Grover's Algorithm for Finding a Secret Key*
12:15-14:00	Lunch
14:00-15:00	David Naccache & Remi Geraud *Thrifty Zero-Knowledge When Linear Programming Meets Cryptography*
15:00-15:30	Coffee Break
15:30-16:15	Pavol Zajac *McEliece in Practice*
	Viliam Hromada *Side Channel Analysis of McEliece Cryptosystem*
16:15-17:00	Eran Tromer *Physical Side Channel Attacks on PCs*

Tuesday, September 27th

9:30-10:30	Cetin Kaya Koc *Hardware Trojans in Incompletely Specified Digital Systems*
10:30-11:00	Coffee Break
11:00-12:00	Boaz Tsaban *Nonabelian Cryptosystems, for a Change?*
12:00-14:00	Lunch
14:00-14:30	Oscar Reparaz *Side-Channel Countermeasures for Lattice-Based Post-Quantum Cryptographic Implementations*
14:30-15:00	Dorian Goldfeld *Quantum Resistant Group Theoretic Public Key Methods*

Organizing committee:

- Viktor Fischer, Jean Monnet University
- Otokar Grošek, Slovak University of Technology
- Rainer Steinwandt, Florida Atlantic University
- Eran Tromer, Tel Aviv University

Location:

Tel Aviv University, Orenstein Building room 111

WiFi: “Free-TAU” with password “free-tau”, or “TAU-CS” with password “publictau”.

Sponsors:

- Air Force Research Laboratory AFRL/RIKF Award No. FA8750-15-2-0047
- Blavatnik Interdisciplinary Cyber Research Center
- Check Point Institute for Information Security
- Leona M. & Harry B. Helmsley Charitable Trust
- NATO's Public Diplomacy Division in the Framework of "Science for Peace"
- SICPA SA

Abstracts

Thomas Eisenbarth, Worcester Polytechnic Institute:

Side Channel Analysis and Protection for McEliece Implementations

Cryptographic implementations usually process secret states that must be inaccessible to the attacker. Side channels such as power, EM or sound analysis are a common violation of this assumption, enabling an attacker with physical access to overcome the security of the implementations.

The McEliece Cryptosystem has several properties such as large keys and an unusual mixing of key and state that make its side channel analysis more challenging than other contemporary cryptosystems.

In this talk we present how side channel analysis can be applied to a state-of-the-art hardware implementation of the efficient quasi-cyclic moderate-density parity-check McEliece implementation presented at Design, Automation and Test in Europe (DATE) 2014. The cryptanalysis consists of a combination of side-channel analysis during the syndrome computation followed by an algebraic step that exploits the relation between the public key and the private key. The complete secret key is recovered after a few observed decryptions.

We further show how the implementation can be efficiently protected against these kinds of side channel analysis by applying a masking countermeasure to the implementation. The side channel resistance of the resulting design is verified by practical DPA attacks and statistical tests for leakage detection.

The presentation is based on joint work with Cong Chen, Ingo von Maurich and Rainer Steinwandt.

Pierre-Louis Cayrel, Université Jean Monnet, Saint-Étienne:

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.

In this talk, I will present the recent progress we made on code-based cryptography in our research team and especially on side-channel attacks against the McEliece cryptosystem using Goppa codes. I will also survey results we obtained on cryptanalysis (ISD and critical attacks), development of new constructions (hash-functions, stream ciphers and identification schemes) and more theoretical results (NP-completeness of some problems). I will conclude my talk in proposing future works and detail the ongoing ones.

Rainer Steinwandt, Florida Atlantic University :

Understanding the cost of Grover's algorithm for finding a secret key

Assuming the presence of large-scale quantum computers, it is natural to invoke Grover's algorithm to speed up an exhaustive key search for a block cipher of interest. In order to establish a reliable estimate for the post-quantum security margin of the target cipher, pertinent resource needs (such as number of qubits and number of gates) need to be considered. This talk discusses the cost of implementing some prominent block ciphers as a quantum circuit, as needed for Grover's algorithm, using a Clifford+T gate set.

The talk is based on joint work with Brittanney Amento, Markus Grassl, Brandon Langenberg, and Martin Roetteler.

Remi Geraud, Ecole normale supérieure de Paris (ENS):

Thrifty Zero-Knowledge When Linear Programming Meets Cryptography

We introduce "thrifty" zero-knowledge protocols, or TZK. These protocols are constructed by introducing a bias in the challenge send by the prover. This bias is chosen so as to maximize the security versus effort trade-off. We illustrate the benefits of this approach on several well-known zero-knowledge protocols.

Pavol Zajac, Slovak University of Technology:

McEliece in practice

Our talk's focus is practical experience with McEliece cryptosystem (MECS) implementations.

We summarize the current state of the BitPunch library, which is our standalone software implementation of the MECS. BitPunch's modular architecture allows us to choose between classical Goppa codes and QC-MDPC, as well as an LDGM signature scheme.

In the second part we focus on a proposal of a hybrid scheme based on MECS. We use the scheme to extend BitPunch in a "cryptobox" style. The hybrid encryption can then be used as a trasport layer for higher protocols such as key exchange.

We conclude with some remarks on the performance of MECS on Android and AVR platforms.

Viliam Hromada, Slovak University of Technology:

Side channel analysis of McEliece cryptosystem

In my talk, I will present our results from side-channel analysis of implementation of McEliece cryptosystem, known as BitPunch, developed at our department. We implemented BitPunch on three different platforms – development board STM32F407VG with ARM Cortex M4, development board Altera Cyclone SoC with ARM Cortex A9 and Raspberry Pi2 with ARM Cortex A7. By using SPA and chosen-ciphertext attack, we were able to find the secret permutation matrix of 2048-bit McEliece cryptosystem implemented on Altera Cyclone and the secret permutation matrix of 64-bit McEliece cryptosystem implemented on STM32F407VG. We also automated the whole measurement and evaluation process in MATLAB, so now we just set the parameters and “observe” the attack.

Eran Tromer, Tel Aviv University:

Physical Side Channel Attacks on PCs

Can secret information be extracted from personal computers by measuring their physical properties from the outside? What would it take to extract whole keys from such fast and complex devices? We survey numerous physical attack channels, including:

- Acoustic key extraction, using microphones to record the high-pitched noise caused by vibration of electronic circuit components during decryption.
- Electric key extraction exploiting fluctuations in the "ground" electric potential of computers. An attacker can measure this signal by touching the computer's chassis, or the shield on the remote end of Ethernet, VGA or USB cables.
- Electromagnetic key extraction, using a cheap radio to non-intrusively attack laptop computers.

Widely-deployed implementations of many cryptographic algorithms, are vulnerable to these attacks, running on common hardware such as laptops and mobile phones. We will discuss the attack principles and some countermeasures.

Joint works with Daniel Genkin, Adi Shamir, Lev Pachmanov, Itamar Pipman and Yuval Yarom. For more information see: https://cs.tau.ac.il/~tromer/leisec

Cetin Kaya Koc, University of California Santa Barbara:

Hardware Trojans in Incompletely Specified Digital Systems

There is a less studied but extremely stealth class of hardware threat: Hardware Trojans that do not rely on rare triggering conditions to stay hidden, but instead only alter the logic functions of design signals which have unspecified behavior, meaning the Trojan never violates the design specification. While formal models of such threats can be developed for analysis (detection), their impact can be studied under certain realistic scenarios. Existing Trojans generally aim to disrupt normal bus behavior and are often designed for a specific protocol and topology, but there is a general model for creating a covert Trojan communication channel between SoC components. In this channel model, which is applicable to any topology and protocol, one can create circuitry allowing information to flow covertly by altering existing bus signals only when they are unspecified. We give the specifics of this circuitry for AMBA AXI4 to quantify the overhead of the Trojan channel and illustrate the ability of our Trojans to evade a suite of protocol compliance checking assertions from ARM.

Boaz Tsaban, Bar-Ilan University:

Nonabelian cryptosystems, for a change?

Many years passed since the introduction of public key cryptography and still, very few public key cryptosystems are widely believed to be secure. Basically, these are the PKCs based on DH, the closely-related RSA, and Lattices. These trusted PKCs are all based on operations in abelian (commutative) groups.

The world of nonabelian groups is much wider and richer in computational problems than that of abelian ones. Around the beginning of the present Millenium, attempts have been made to base PKCs on nonabelian groups (and related structures). These attempts have mostly failed. Why?

I am an enthusiast of the potential of nonabelian structures in crypto, my belief is that serious cryptanalysis is necessary for gaining intuition on the promising directions. I have succeeded, with coauthors, cryptanalysing many of the proposals, and in a structural way that makes it possible for PKC designers to check some of their own proposals before releasing them.

I will discuss the methods that I developed with collaborators, and perhaps discuss my opinions on the potential of nonabelian crypto. E.g.:

1. Serious lack of manpower (equivalently, grants).
2. Presently, almost only mathematicians consider this directions. Cryptographers need to enter the field in order to bring the proposals to the standards common in crypto (this implies (2)).
3. Proposals are usually made in a raw stage, prior to serious cryptanalysis. This gives the approach a bad reputation (this implies (0)).
4. Maybe there is some big phenomenon lurking, that makes it possible to reduce the relevant nonabelian problems to abelian ones (a la Babai et al.) (And maybe not.)

I will, however, mention a very elegant nonabelian cryptographic primitive that resisted all cryptanalytic efforts (mine and many others). It has a worst case to average reduction, and performance-wise, it compares favorably with provable lattice-based candidates.

Oscar Reparaz, University of Leuven:

Side-channel countermeasures for lattice-based post-quantum cryptographic implementations

Lattice-based cryptography has been proposed as a postquantum public-key crypto system. In this talk I will describe two different side-channel countermeasures for ring-LWE (a post-quantum public-key crypto system based on lattices.)

In the first solution, we present a masked ring-LWE decryption implementation resistant to first-order side-channel attacks. Our solution has the peculiarity that the entire computation is performed in the masked domain. This is achieved thanks to a new, bespoke masked decoder implementation. The output of the ring-LWE decryption are Boolean shares suitable for derivation of a symmetric key. We have implemented a hardware architecture of the masked ring-LWE processor on a Virtex-II FPGA, and have performed side channel analysis to confirm the soundness of our approach. The area of the protected architecture is around 2000 LUTs, a 20% increase with respect to the unprotected architecture. The protected implementation takes 7478 cycles to compute, which is only a factor ×2.6 larger than the unprotected implementation. This work was presented at CHES 2015.

The second approach exploits the additively-homomorphic property of the existing ring-LWE encryption schemes and computes an additive-mask as an encryption of a random message. Our solution differs in several aspects from the previous approach; most notably we do not require a masked decoder but work with a conventional, unmasked decoder. As such, we can secure a ring-LWE implementation using additive masking with minimal changes. Our masking scheme is also very generic in the sense that it can be applied to other additively-homomorphic encryption schemes. This work was published at PQCrypto 2016.

Dorian Goldfeld, Columbia University:

Quantum Resistant Group Theoretic Public Key Methods

All widely used public-key solutions are based in number theory. This includes RSA, DH, and ECC. Of course once sufficiently large quantum computers get built all of these number-theory-based methods fall to Shor's algorithm. We believe that group theory can provide a strong basis for quantum resistant solution. While researchers have looked somewhat into lattices, we specifically believe that some hard problems in the braid group can be used. To that end we have been developing several group-theoretic public-key solutions based on various hard problems in the braid group.

In 2005 we introduced a group-theoretic one-way function called E-Multiplication that translates from the braid group to permutations and matrices over finite fields. Using E-Multiplication, combined with other hard problems in braid group theory, we have devised several quantum-resistant public-key solutions including a key agreement protocol and a digital signature solution.

Some interesting features of E-Multiplication are that it is rapidly computable, even on the tiniest of devices, its computation scales linearly with the length of the braid making it a perfect antidote to Grover's search algorithm, and because of the infinite, non-abelian, non-cyclic nature of E-Multiplication it is not subject to Shor's algorithm or the hidden subgroup problem.

In this talk we briefly recount E-Multiplication, quickly explain its quantum resistance characteristics, and then show two new public-key methods based upon it, a key agreement protocol we call KayawoodKAP, and a digital signature algorithm we call WalnutDSA. We will also discuss the security of these constructions in light of previous studies.