

Symmetric Cryptography

Edited by

Frederik Armknecht¹, Tetsu Iwata², Kaisa Nyberg³, and
Bart Preneel⁴

1 Universität Mannheim, DE, armknecht@uni-mannheim.de

2 Nagoya University, JP, iwata@cse.nagoya-u.ac.jp

3 Aalto University, FI, kaisa.nyberg@aalto.fi

4 KU Leuven, BE, bart.preneel@esat.kuleuven.be

Abstract

From January 10–15, 2016, the seminar 16021 in Symmetric Cryptography was held in Schloss Dagstuhl – Leibniz Center for Informatics. It was the fifth in the series of the Dagstuhl seminars “Symmetric Cryptography” held in 2007, 2009, 2012, and 2014.

During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations were given during the seminar. The first section describes the seminar topics and goals in general.

Seminar January 10–15, 2016 – <http://www.dagstuhl.de/16021>

1998 ACM Subject Classification E.3 Data Encryption, H.2.0 General – Security, Integrity, and Protection, K.6.5 Security and Protection

Keywords and phrases authenticity, block ciphers, confidentiality, cryptanalysis, hash functions, integrity, lightweight cryptography, provable security, stream ciphers

Digital Object Identifier 10.4230/DagRep.6.1.34

1 Executive Summary

Frederik Armknecht

Tetsu Iwata

Kaisa Nyberg

Bart Preneel

License © Creative Commons BY 3.0 Unported license
© Frederik Armknecht, Tetsu Iwata, Kaisa Nyberg, and Bart Preneel

One lesson learned from the Snowden leaks is that digital systems can never be fully trusted and hence the security awareness of citizens has increased substantially. Whenever digital data is communicated or stored, it is subject to various attacks. One of the few working countermeasures are the use of cryptography. As Edward Snowden puts it: “*Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.*”¹

Consequently it holds that although modern cryptography addresses a variety of security challenges, efficiently protecting the enormous amount of daily electronic communication represents a major challenge. Here, symmetric cryptography is especially highly relevant not only for academia, but also for industrial research and applications.

¹ See <http://techcrunch.com/2013/06/17/encrypting-your-email-works-says-nsa-whistleblower-edward-snowden/>.



Although symmetric cryptography has made enormous progress in the last couple of decades, for several reasons regularly new insights and challenges are evolving. In the past, the AES competition was led by US NIST to standardize a next generation block cipher to replace DES. Similar competitions, such as the eSTREAM and the SHA-3 competition, resulted in new standard algorithms that meet public demands. The outcome of the projects are practically used in our daily lives, and the fundamental understanding of the cryptographic research community of these primitives has been increased significantly.

While this seminar concentrates in general on the design and analysis of symmetric cryptographic primitives, special focus has been put on the following two topics that we explain in more detail below:

1. Authenticated encryption
2. Even-Mansour designs

Authenticated Encryption. Today the central research question is the construction of schemes for *authenticated* encryption. This symmetric primitive efficiently integrates the protection of secrecy and integrity in a single construction. The first wave of solutions resulted in several widely used standards, including CCM and GCM standardized by NIST, and the EAX-prime standardized by ANSI. However, it turns out that these constructions are far from optimum in terms of performance, security, usability, and functionality. For instance a stream of data cannot be protected with CCM, as the length of the entire input has to be known in advance. The security of GCM heavily relies on the existence of data called a nonce, which is supposed to never be repeated. Indeed, the security of GCM is completely lost once the nonce is repeated. While it is easy to state such a mathematical assumption, experience shows that there are many practical cases where realizing this condition is very hard. For instance the nonce may repeat if a crypto device is reset with malice aforethought, or as a consequence of physical attacks on the device. Furthermore, weak keys were identified in GCM, and the security of EAX-prime is questionable.

Thus there is a strong demand for secure and efficient authenticating encryption scheme. As a consequence, the CAESAR project (Competition for Authenticated Encryption: Security, Applicability, and Robustness) has been initiated.² The goal of the project is to identify a portfolio of authenticated encryption schemes that (1) offer advantages over GCM/CCM and (2) are suitable for widespread adoption. The deadline of the submission was March 15, 2014, and the project attracted a total of 56 algorithms from 136 designers from all over the world. There are plenty of innovative designs with attractive features, and the final portfolio is planned to be announced at the end of 2017.

This seminar took place in the middle of the CAESAR competition; it is two years from the submission deadline and we have about two years until the announcement of the final portfolio. Therefore, it was a perfect point in time to sum up the research done so far, to exchange ideas and to discuss future directions.

Even-Mansour Designs. Another strong trend in the current symmetric key cryptography is related to the so-called *Even-Mansour designs*. This design paradigm was proposed in 1991 and can be seen as the abstraction of the framework adopted in the design of AES. This general design framework iterates r times the xor of a key and a public permutation. The design framework is highly relevant in practice, and it has been adopted in a variety of recent hash functions, block ciphers, and even in the underlying primitive of several CAESAR submissions. Despite its long history of practical use, the community has so far failed to

² See <http://competitions.cr.yp.to/caesar.html> for details.

develop a complete understanding of its security. From a theoretical viewpoint, the original proposal was accompanied with a proof of security, dealing with the case of $r = 1$ iteration.

Only 20 years after the initial proposal, in 2012, a bound was proven for the security of $r = 2$ iterations. In 2014, the question was solved to cover the general case of r iterations. However, these results only deal with the simple case of distinguishing attack on a single, unknown key setting. Its security in more advanced, yet practically relevant security models, such as the related-key setting or the chosen/known-key setting, is largely unexplored.

Another problem here is that the theoretical analysis assumes that the permutation used therein is ideal and the keys are ideally random, which is not the case for practical constructions. This implies that the theoretical results do not directly translate into the practical constructions, and the security analysis has to be repeated for each constructions.

Summing up, Evan-Mansour designs represent a fruitful and challenging area of research, that hopefully will lead to a fundamental understanding of iterated constructions and ultimately to more efficient and more secure ciphers.

Seminar Program. The seminar program consists of the presentations about the above topics, and relevant areas of symmetric cryptography, including new cryptanalytic techniques and new designs. Furthermore, there were three discussion sessions. In “discussion on attacks,” we discussed what constitutes a valid cryptographic attack in light of weak key classes, “discussion on secret agency crypto standards” was about cryptography developed by secret agencies, and there was a discussion session about the ongoing CAESAR project.

2 Table of Contents

Executive Summary

Frederik Armknecht, Tetsu Iwata, Kaisa Nyberg, and Bart Preneel 34

Overview of Talks

On Ciphers that Continuously Access the Non-Volatile Key <i>Frederik Armknecht</i>	39
Another view of the division property <i>Anne Canteaut</i>	39
How to Tweak Even-Mansour Ciphers <i>Benoît Cogliati</i>	40
On modes and primitives in the CAESAR competition <i>Joan Daemen</i>	40
New Attacks on Hash function Combiners <i>Itai Dinur</i>	41
Second Preimage Attacks against Dithered Hash Functions with Practical Online Memory Complexity <i>Orr Dunkelman</i>	41
Some Results on the GOST block ciphers <i>Orr Dunkelman, Ashur Tomer, Bar-On Achiya, and Keller Nathan</i>	42
Provable Security Evaluation of Structures against Impossible Differential and Zero Correlation Linear Cryptanalysis <i>Jian Guo</i>	42
On GCM-SIV <i>Tetsu Iwata</i>	43
Key Alternating PRFs and provable security of stream ciphers against time-memory-data tradeoff attacks <i>Matthias Krause</i>	43
Even-Mansour Type Block Ciphers Based on Involutions <i>Jooyoung Lee</i>	43
Dynamic Cube Attacks Revisited, with Applications to Grain-128a <i>Willi Meier</i>	44
Improved Masking for Tweakable Blockciphers with Applications to Authenticated Encryption <i>Bart Mennink</i>	44
Parallel MAC with Low Overhead <i>Kazuhiko Minematsu</i>	45
Simpira: A Family of Efficient Permutations Using the AES Round Function <i>Nicky Mouha</i>	46
Revisiting Structure Graph and Its Applications to CBC-MAC and EMAC <i>Mridul Nandi</i>	46

Even-Mansour cipher analysis reduced to the generalized birthday problem <i>Ivica Nikolic</i>	47
The Problem of Estimating the Variance of the Linear Cryptanalysis Test Statistic <i>Kaisa Nyberg</i>	47
Mirror Theory and Cryptography <i>Jacques Patarin</i>	49
S-Box Reverse-Engineering: Recovering Design Criteria, Hidden Structures and New Boolean Function Results <i>Léo Paul Perrin and Alex Biryukov</i>	50
Invariant Subspace Attack Against Full Midori64 <i>Yu Sasaki</i>	50
Transitivity aspects of the (iterated) Even-Mansour cipher <i>Ernst Schulte-Geers</i>	51
Polytopic cryptanalysis <i>Tyge Tiessen</i>	52
Universal Multidimensional and Multiple Zero-Correlation Cryptanalysis <i>Meiqin Wang</i>	52
Bit Cryptanalysis on Symmetric Ciphers <i>Xianyun Wang</i>	53
Panel discussions	
Discussion on Secret Agency Crypto Standards <i>Orr Dunkelman</i>	53
Participants	54

3 Overview of Talks

3.1 On Ciphers that Continuously Access the Non-Volatile Key

Frederik Armknecht (Universität Mannheim, DE)

License © Creative Commons BY 3.0 Unported license
© Frederik Armknecht

Joint work of Frederik Armknecht, Christian Müller, Vasily Mikhalev

Due to the increased use of devices with restricted resources, the community has developed various techniques for designing lightweight ciphers. One approach that is increasingly discussed is to use the key that is stored on the device in non-volatile memory not only for initialization but during the encryption/decryption process as well. This may on the one hand help to save area size, but also may allow for a stronger key involvement and hence higher security.

However, only little is known so far if and to what extent this approach is indeed practical. In this work, we investigate this question. After a discussion on reasonable approaches for storing a key in non-volatile memory, motivated by several commercial products we focus on the case that the key is stored in EEPROM. Here, we highlight existing constraints and derive that some designs are better suited for reducing the area size than others. Based on these findings, we improve an existing design for proposing a new lightweight stream cipher that (i) has a significantly smaller area size than almost all other stream ciphers and (ii) can be efficiently realized using common non-volatile memory techniques. Hence, we see our work as an important step towards putting such designs on a more solid ground and to initiate further discussions on realistic designs.

3.2 Another view of the division property

Anne Canteaut (INRIA – Paris, FR)


License © Creative Commons BY 3.0 Unported license
© Anne Canteaut

Joint work of Anne Canteaut, Christina Boura

A new distinguishing property against block ciphers, called the division property, was introduced by Todo at Eurocrypt 2015. Our work gives a new approach to it by the introduction of the notion of parity sets. First of all, this new notion permits us to formulate and characterize in a simple way the division property of any order. At a second step, we are interested in the way of building distinguishers on a block cipher by considering some further properties of parity sets, generalising the division property. We detail in particular this approach for substitution-permutation networks. To illustrate our method, we provide low-data distinguishers against reduced-round Present. These distinguishers reach a much higher number of rounds than generic distinguishers based on the division property and demonstrate, amongst others, how the distinguishers can be improved when the properties of the linear and the Sbox layer are taken into account.

3.3 How to Tweak Even-Mansour Ciphers

Benoît Cogliati (University of Versailles, FR)

License  Creative Commons BY 3.0 Unported license
© Benoît Cogliati

Joint work of Benoît Cogliati, Rodolphe Lampe, Yannick Seurin

Tweakable block ciphers are a generalization of traditional block ciphers which take an extra input for variability called a tweak. This primitive has proved to be useful to construct various higher level cryptographic schemes such as length-preserving encryption modes, online ciphers, message authentication codes and authenticated encryption modes.

In this talk, we focus on the state of the art about the construction of efficient tweakable block ciphers in the Random Permutation model, where all parties have access to public random permutation oracles, using generalizations of the standard Even-Mansour construction. We present the most recent constructions (Mennink’s XPX construction [1], the TEM construction introduced by Cogliati et al [2]. and the MEM construction introduced by Granger et al [3]) and their best known security results. We also explain the proof techniques behind those results, which are all based on Patarin’s H coefficient technique, and discuss some related open problems.

References

- 1 Mennink, B. *XPX: Generalized Tweakable Even-Mansour with Improved Security Guarantees*. IACR Cryptology ePrint Archive 2015:476 (2015).
- 2 Cogliati, B., Lampe, R., Seurin, Y. *Tweaking Even-Mansour Ciphers*. Advances in Cryptology – CRYPTO 2015 – Proceedings, Part I, volume 9215 of LNCS, pages 189–208. Springer Berlin Heidelberg (2015).
- 3 Granger, R., Jovanovic, P., Mennink, B., Neves, S. *Improved Masking for Tweakable Block-ciphers with Applications to Authenticated Encryption*. Advances in Cryptology – EURO-CRYPT 2016, to appear. Springer Berlin Heidelberg (2016).

3.4 On modes and primitives in the CAESAR competition

Joan Daemen (STMicroelectronics – Diegem, BE)

License  Creative Commons BY 3.0 Unported license
© Joan Daemen

I have made a proposal for the evaluation of 2nd round candidates in the CAESAR competition for authenticated encryption schemes. This proposal mainly consists in separately evaluating primitives (block ciphers, tweakable block ciphers, permutations, . . .) from modes (sponge, OCB, . . .). In many candidates there is a clear distinction between the two and across candidates very similar modes or primitives are used. In many candidates the novelty is concentrated in either the mode or the primitive. These typically take as primitive a standard block cipher like AES or as mode a (close variant) of a published mode such as OCB. There are a few 2nd round candidates for which this split does not apply and that will have to be evaluated as a whole. I illustrated the proposal with a preliminary classification of the modes and primitives in the 2nd round CAESAR candidates.

The presentation gave rise to some discussion and finally a meeting of the CAESAR committee was held at Dagstuhl. The evaluation of the 2nd round candidates will use some of the presented ideas.

3.5 New Attacks on Hash function Combiners

Itai Dinur (Ben Gurion University – Beer Sheva, IL)

License © Creative Commons BY 3.0 Unported license
© Itai Dinur

Main reference I. Dinur, “New Attacks on the Concatenation and XOR Hash Combiners”, IACR Cryptology ePrint Archive, Report 2016/131, 2016.

URL <http://eprint.iacr.org/2016/131>

We study the security of the concatenation combiner $H_1(M)\|H_2(M)$ for two independent iterated hash functions with n -bit outputs that are built using the Merkle-Damgård construction. In 2004 Joux showed that the concatenation combiner of hash functions with an n -bit internal state does not offer better collision and preimage resistance compared to a single strong n -bit hash function. On the other hand, the problem of devising second preimage attacks faster than 2^n against this combiner has remained open since 2005 when Kelsey and Schneier showed that a single Merkle-Damgård hash function does not offer optimal second preimage resistance for long messages.

In this paper, we develop new algorithms for cryptanalysis of hash combiners and use them to devise the first second preimage attack on the concatenation combiner. The attack finds second preimages faster than 2^n for messages longer than $2^{2n/7}$ and has optimal complexity of $2^{3n/4}$. This shows that the concatenation of two Merkle-Damgård hash functions is not as strong as a single ideal hash function.

Our methods are also applicable to other well-studied combiners, and we use them to devise a new preimage attack with complexity of $2^{2n/3}$ on the XOR combiner $H_1(M)\oplus H_2(M)$ of two Merkle-Damgård hash functions. This improves upon the attack by Leurent and Wang (presented at Eurocrypt 2015) whose complexity is $2^{5n/6}$ (but unlike our attack is also applicable to HAIFA hash functions).

Our algorithms exploit properties of random mappings generated by fixing the message block input to the compression functions of H_1 and H_2 . Such random mappings have been widely used in cryptanalysis, but we exploit them in new ways to attack hash function combiners.

3.6 Second Preimage Attacks against Dithered Hash Functions with Practical Online Memory Complexity

Orr Dunkelman (University of Haifa, IL)

License © Creative Commons BY 3.0 Unported license
© Orr Dunkelman

Joint work of Orr Dunkelman, Barham Muhammad

In this work we show how to reduce the online memory complexity of second preimage attacks against dithered hash functions to less than 1 GB.

3.7 Some Results on the GOST block ciphers

Orr Dunkelman (University of Haifa, IL)

License © Creative Commons BY 3.0 Unported license

© Orr Dunkelman, Ashur Tomer, Bar-On Achiya, and Keller Nathan

Joint work of Orr Dunkelman, Ashur Tomer, Bar-On Achiya, Keller Nathan

The talk covered several new attacks reported against the GOST family of block ciphers:

1. Attacking GOST2 using a reflection property (for a weak key class of 2^{224} keys),
2. New improved cycle finding attack on GOST's original key schedule – attacking the weak key class of $K1K2K3K4K4K3K2K1$ in 2^{36} data and 2^{40} time.

3.8 Provable Security Evaluation of Structures against Impossible Differential and Zero Correlation Linear Cryptanalysis

Jian Guo (Nanyang TU – Singapore, SG)

License © Creative Commons BY 3.0 Unported license

© Jian Guo

Joint work of Bing Sun, Meicheng Liu, Jian Guo, Vincent Rijmen, Ruilin Li

Main reference B. Sun, Z. Liu, V. Rijmen, R. Li, L. Cheng, Q. Wang, H. AlKhzaimi, C. Li, “Links Among Impossible Differential, Integral and Zero Correlation Linear Cryptanalysis,” in Proc. of the 35th Annual Cryptology Conference – Advances in Cryptology (CRYPTO'15), LNCS, Vol. 9215, pp. 95–115, Springer, 2015.

URL http://dx.doi.org/10.1007/978-3-662-47989-6_5

Impossible differential and zero correlation linear cryptanalysis are two of the most important cryptanalytic vectors. To characterize the impossible differentials and zero correlation linear hulls which are independent of the choices of the non-linear components, Sun *et al.* proposed the structure deduced by a block cipher at CRYPTO 2015. Based on that, we concentrate in this paper on the security of the SPN structure and Feistel structure with SP-type round functions. Firstly, we prove that for an SPN structure, if $\alpha_1 \rightarrow \beta_1$ and $\alpha_2 \rightarrow \beta_2$ are possible differentials, $\alpha_1|\alpha_2 \rightarrow \beta_1|\beta_2$ is also a possible differential, i.e., the OR “|” operation preserves differentials. Secondly, we show that for an SPN structure, there exists an r -round impossible differential if and only if there exists an r -round impossible differential $\alpha \not\rightarrow \beta$ where the Hamming weights of both α and β are 1. Thus for an SPN structure operating on m bytes, the computation complexity for deciding whether there exists an impossible differential can be reduced from $\mathcal{O}(2^{2m})$ to $\mathcal{O}(m^2)$. Thirdly, we associate a primitive index with the linear layers of SPN structures. Based on the matrices theory over integer rings, we prove that the length of impossible differentials of an SPN structure is upper bounded by the primitive index of the linear layers. As a result we show that, unless the details of the S-boxes are considered, there do not exist 5-round impossible differentials for the AES and ARIA. Lastly, based on the links between impossible differential and zero correlation linear hull, we projected these results on impossible differentials to zero correlation linear hulls. It is interesting to note some of our results also apply to the Feistel structures with SP-type round functions.

3.9 On GCM-SIV

Tetsu Iwata (Nagoya University, JP)

License © Creative Commons BY 3.0 Unported license
© Tetsu Iwata

Joint work of Tetsu Iwata, Kazuhiko Minematsu

At CCS 2015, Gueron and Lindell proposed GCM-SIV, a provably secure authenticated encryption scheme that remains secure even if the nonce is repeated. We first point out that GCM-SIV allows a trivial distinguishing attack with about $2^{(n-32)/2}$ attack complexity, where n is the block length of the underlying blockcipher and $n = 128$ for GCM-SIV. This shows the tightness of the security claim and does not contradict the provable security result. We present a minor variant of GCM-SIV, which we call GCM-SIV1, that is secure up to the standard birthday-bound-security, in the total number of input blocks, of about $2^{n/2}$ attack complexity. We then explore constructions of a scheme with a stronger security guarantee. We present GCM-SIV2 that is obtained by running two instances of GCM-SIV1 in parallel and mixing them in a simple way. We show that it is secure up to about $2^{2n/3}$ attack complexity. Finally, we generalize this to show GCM-SIV r by running r instances of GCM-SIV1 in parallel, where $r \geq 3$, and show that the scheme is secure up to about $2^{nr/(r+1)}$ attack complexity.

3.10 Key Alternating PRFs and provable security of stream ciphers against time-memory-data tradeoff attacks

Matthias Krause (Universität Mannheim, DE)

License © Creative Commons BY 3.0 Unported license
© Matthias Krause

We consider keystream generator based stream ciphers which generate the keystream packet-wise, like the Bluetooth cipher E_0 . We show a method how to design such ciphers in such a way that beyond-the-birthday-bound security against generic time-memory-tradeoff attacks can be proved. This allows, in principle, for designing practical stream ciphers with a significantly smaller inner state length. One further consequence is that only a small change in the state initialization algorithm of the E_0 -cipher suffices for raising the security level from $n/2$ to $(2/3)n$. We obtain our results by modelling the state initialization – and keystream generation process by Even-Mansour like constructions, and analyzing them in a generalized random oracle model.

3.11 Even-Mansour Type Block Ciphers Based on Involutions

Jooyoung Lee (Sejong University – Seoul, KR)

License © Creative Commons BY 3.0 Unported license
© Jooyoung Lee

In this work, we study the security of Even-Mansour type ciphers whose encryption and decryption are (almost) the same. Such ciphers, called involutorial, possibly allow efficient hardware implementation with a same circuit shared for encryption and decryption, expected

to be suitable for lightweight environment where low power consumption and implementation costs are desirable.

With this motivation, we consider a single-round Even-Mansour cipher using an involution as its basing primitive. Then the decryption of such a cipher is the same as encryption with the order of the round keys reversed. It is known that such a cipher permits an attack using only construction queries below the birthday bound, while it has been open how it provides provable security within the range below the birthday bound. We prove that the Even-Mansour cipher based on a random involution is as secure as the permutation-based one when the number of construction queries is limited by the birthday bound.

In order to achieve security beyond the birthday bound, we propose a two-round Even-Mansour-like construction that makes a single call to each of the basing permutation P and its inverse using a fixed permutation in the middle layer. The security of this construction is proved beyond the birthday bound. As an open problem, we ask for the block cipher construction that uses only a single involution and provides security beyond the birthday bound at the same time.

3.12 Dynamic Cube Attacks Revisited, with Applications to Grain-128a

Willi Meier (FH Nordwestschweiz – Windisch, CH)

License  Creative Commons BY 3.0 Unported license
© Willi Meier

Joint work of Willi Meier, Yonglin Hao

Dynamic cube attacks are revisited, and a probabilistic model of their success is given. This model identifies the main factors influencing the success probability of dynamic cube attacks. Based on this model, a new strategy for constructing the necessary cube testers is provided so that a higher success probability can be acquired. The correctness of our deductions are verified experimentally on the round-reduced stream cipher Grain-128a. Similar methods enable dynamic cube key recovery attacks on up to 177 of the 256 initialization rounds of this cipher. These are the first practical results on key recovery of (round-reduced) Grain-128a in the single key model.

3.13 Improved Masking for Tweakable Blockciphers with Applications to Authenticated Encryption

Bart Mennink (KU Leuven, BE)

License  Creative Commons BY 3.0 Unported license
© Bart Mennink

Joint work of Robert Granger, Philipp Jovanovic, Bart Mennink, Samuel Neves

Main reference R. Granger, P. Jovanovic, B. Mennink, S. Neves, “Improved Masking for Tweakable Blockciphers with Applications to Authenticated Encryption,” IACR Cryptology ePrint Archive, Report 2015/999, 2015.

URL <https://eprint.iacr.org/2015/999>

A popular approach to tweakable blockcipher design is via masking, where a certain primitive (a blockcipher or a permutation) is preceded and followed by an easy-to-compute tweak-dependent mask. In this work, we revisit the principle of masking. We do so alongside the introduction of the tweakable Even-Mansour construction MEM. Its masking function combines the advantages of word-oriented LFSR- and powering-up-based methods. We show

in particular how recent advancements in computing discrete logarithms over finite fields of characteristic 2 can be exploited in a constructive way to realize highly efficient, constant-time masking functions. If the masking satisfies a set of simple conditions, then MEM is a secure tweakable blockcipher up to the birthday bound. The strengths of MEM are exhibited by the design of fully parallelizable authenticated encryption schemes OPP (nonce-respecting) and MRO (misuse-resistant). If instantiated with a reduced-round BLAKE2b permutation, OPP and MRO achieve speeds up to 0.55 and 1.06 cycles per byte on the Intel Haswell microarchitecture, and are able to significantly outperform their closest competitors.

3.14 Parallel MAC with Low Overhead

Kazuhiko Minematsu (NEC – Kawasaki, JP)

License © Creative Commons BY 3.0 Unported license
© Kazuhiko Minematsu

Joint work of Tetsu Iwata, Kazuhiko Minematsu

In this talk we propose a new message authentication code (MAC) mode of operation based on blockcipher. We first survey popular MAC modes, such as CMAC and PMAC. Our survey reveals that there is no known scheme to achieve all the following four properties.

1. Optimal efficiency with pre-computation: m blockcipher calls to process m -block message, for any $m \geq 1$, with one precomputed encrypted block (typically $L = E_K(0^n)$).
2. Quasi-optimal efficiency w/o pre-computation: m BC calls for $m > 1$ and 2 calls for $m = 1$. It does not need a precomputation of L .
3. One-key (key is a BC key)
4. Well parallelizable

Here, CMAC (a.k.a. OMAC [1]) achieves Properties 1 and 3, and PMAC[4] achieves Properties 1 and 3 and 4. A variant of CMAC called GCBC [3] achieves Properties 2 and 3. In other words, what is lacked here is a parallelizable MAC without precomputation of L . It means computation overhead is low, which is important when memory is precious or low-latency operation is required. Based on the work on a MAC proposal by Minematsu[2], we provide a scheme which enables all four properties, in particular, parallelizable up to around n blocks in case n -bit blockcipher is used. The security proof is work in progress but we expect standard birthday-type bound for the forgery probability.

References

- 1 Iwata, T., Kurosawa, K.: OMAC: one-key CBC MAC. In: FSE. Lecture Notes in Computer Science, vol. 2887, pp. 129–153. Springer (2003)
- 2 Minematsu, K.: A short universal hash function from bit rotation, and applications to blockcipher modes. In: ProvSec. Lecture Notes in Computer Science, vol. 8209, pp. 221–238. Springer (2013)
- 3 Nandi, M.: Fast and Secure CBC-Type MAC Algorithms. In: FSE. Lecture Notes in Computer Science, vol. 5665, pp. 375–393. Springer (2009)
- 4 Rogaway, P.: Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In: Lee, P.J. (ed.) ASIACRYPT. Lecture Notes in Computer Science, vol. 3329, pp. 16–31. Springer (2004)

3.15 Simpira: A Family of Efficient Permutations Using the AES Round Function

Nicky Mouha (KU Leuven, BE)

License © Creative Commons BY 3.0 Unported license
© Nicky Mouha

Joint work of Shay Gueron, Nicky Mouha

Main reference S. Gueron, N. Mouha, “Simpira v2: A Family of Efficient Permutations Using the AES Round Function,” IACR Cryptology ePrint Archive, Report 2016/122, 2016.

URL <https://eprint.iacr.org/2016/122>

This talk introduces Simpira, a family of cryptographic permutations that supports inputs of $128 * b$ bits, where b is a positive integer. Its design goal is to achieve high throughput on virtually all modern 64-bit processor architectures, that nowadays already have native instructions to support AES computations. To achieve this goal, Simpira uses only one building block: the AES round function. For $b = 1$, Simpira corresponds to 12-round AES with fixed round keys, whereas for $b \geq 2$, Simpira is a Generalized Feistel Structure (GFS) with an F-function that consists of two rounds of AES. From the security viewpoint, we claim that there are no structural distinguishers for Simpira with a complexity below 2^{128} , and analyze its security against a variety of attacks in this setting. From the efficiency viewpoint, we show that the throughput of Simpira is close to the theoretical optimum, namely, the number of AES rounds in the construction. For example, on the latest Intel Skylake processor, Simpira has throughput below 1 cycle per byte for $b \leq 4$ and $b = 6$. For larger permutations, where moving data in memory has a more pronounced effect, Simpira with $b = 32$ (512 byte inputs) evaluates 732 AES rounds, and performs at 802 cycles (1.56 cycles per byte), i.e., less than 10% off the theoretical optimum. The Simpira family offers an efficient solution for multiple usages where operating on wide blocks, larger than 128 bits, is desired.

3.16 Revisiting Structure Graph and Its Applications to CBC-MAC and EMAC

Mridul Nandi (Indian Statistical Institute – Kolkata, IN)

License © Creative Commons BY 3.0 Unported license
© Mridul Nandi

Joint work of Mridul Nandi, Ashwin Jha

Main reference A. Jha, M. Nandi, “Revisiting Structure Graph and Its Applications to CBC-MAC and EMAC,” IACR Cryptology ePrint Archive, Report 2016/161, 2016.

URL <http://eprint.iacr.org/2016/161>

In CRYPTO’05, Bellare et al. proved $O(\ell q^2/2^n)$ bound for the PRF (pseudorandom function) security of the CBC-MAC based on an n -bit random permutation Π , provided $\ell < 2^{n/3}$. Here an adversary can make at most q prefix-free queries each having at most ℓ “blocks” (elements of $\{0, 1\}^n$). In the same paper $O(\ell^{o(1)} q^2/2^n)$ bound for EMAC (or encrypted CBC-MAC) was proved, provided $\ell < 2^{n/4}$. Both proofs are based on **structure graphs** representing all collisions among “intermediate inputs” to Π during the computation of CBC. The problem of bounding PRF-advantage is shown to be reduced to bounding the number of structure graphs satisfying certain collision patterns. Unfortunately, we have shown here that *the Lemma 10 in the Crypto’05 paper, stating an important result on structure graphs, is incorrect*. This is due to the fact that the authors **overlooked certain structure graphs**. This invalidates the proofs of the PRF bounds. In ICALP’06, Pietrzak improved the bound for EMAC by

showing a *tight bound* $O(q^2/2^n)$ under the restriction that $\ell < 2^{n/8}$. As he used the same flawed lemma, this proof also becomes invalid. In this paper, we have revised and sometimes simplified these proofs. We revisit structure graphs in a slightly different mathematical language and provide a complete characterization of certain types of structure graphs. Using this characterization, we show that PRF security of CBC-MAC is about $\sigma q/2^n$ provided $\ell < 2^{n/3}$ where σ is the total number of blocks in all queries. We also recovered the tight bound of EMAC with a much relaxed constraint $\ell < 2^{n/4}$ than the original.

3.17 Even-Mansour cipher analysis reduced to the generalized birthday problem

Ivica Nikolic (Nanyang TU – Singapore, SG)

License  Creative Commons BY 3.0 Unported license
© Ivica Nikolic

We show that full subkey recovery of iterated Even-Mansour ciphers can be reduced to the generalized birthday problem.

3.18 The Problem of Estimating the Variance of the Linear Cryptanalysis Test Statistic

Kaisa Nyberg (Aalto University, FI)

License  Creative Commons BY 3.0 Unported license
© Kaisa Nyberg

Joint work of Celine Blondeau, Kaisa Nyberg

Main reference C. Blondeau, K. Nyberg, “Joint Data and Key Distribution of the Linear Cryptanalysis Test Statistic and Its Impact to Data Complexity Estimates of Multiple/Multidimensional Linear and Truncated Differential Attacks,” IACR Cryptology ePrint Archive, Report 2015/935, 2015.

URL <http://eprint.iacr.org/2015/935>

Until recently, most statistical models of linear key-recovery attacks determine and analyze the attack statistic with fixed keys and taking only the data as a random variable. When using such models in practice, it is assumed that for all cipher keys, all wrong key candidates draw the value of the test statistic from the same (uniform) distribution, and similarly, all correct key candidates draw the value of the test statistic from the same (non-uniform) distribution. Previously, in [4, 5] experiments were provided to demonstrate that the probability distributions of the test statistic vary significantly over the key. In [3], the simple linear attack using one linear approximation with a single dominant trail was considered and the wrong-key randomization hypothesis revised accordingly. As the result, the estimate of the data complexity was improved as demonstrated in experiments. In [6], the variation in the probability distribution of capacity over the right key was studied in the context of multiple and multidimensional linear attacks. In particular, the authors determined weak-key quantiles, that is, lower bounds of capacity that are satisfied by a given proportion, say one half, or 30% of the keys. Such approach was previously taken also in [7] in the case of single linear hull.

In [1] we presented the first complete treatment on the probability distributions of linear attack test statistics, that is, the empirical correlations and capacities, by considering both the data sample and the key as random variables. We analyzed and combined the different

previously presented models and went beyond by studying the joint probability distribution of the test statistic, where in addition to the data, also both the wrong and right keys are taken as random variables. From this model one can derive formulas for success probability and data complexity in multiple and multidimensional linear key-recovery attacks.

We also mention in [1] how to apply the same approach to the simplest case of linear key-recovery attack, that is, Matsui's Algorithm 2, which uses one linear approximation with a single dominant trail. In this case, the probability distribution of the empirical correlation observed from data with the correct key can be approximated by a union of two normal distributions. For details, we refer to [9]. One of the main benefits of integrating the key as a random variable in the model is that the data complexity of the attack can be expressed as a function of the *ELP* of the linear approximation. Until now, the data complexity was determined from a fixed-key statistical model and assuming that the expected capacity of the probability distribution of the test statistic is equal for all keys. The new integrated statistical model gives the data complexity estimate for a random key. As a consequence, the issue raised in [8] is resolved. In particular, the fact that multiple strong characteristics cancel each other for many keys is not a problem for linear cryptanalysis in general. Indeed, it is very likely that the average correlation is equal to zero. The situation is as stated in [5]: "The average correlation of a hull gives no indication about the complexity of a linear attack. Therefore, we only talk about the *ELP* of a hull." While it has been known by most authors that *ELP* is the right quantity to consider in the context of linear attacks, no satisfactory presentation of exactly how it determines the data complexity of the attack for a random encryption key has not been given in the literature until now.

Two major problems remained in the treatment given in [1]. First, it was observed that the formula of variance of capacity gives serious underestimates in the experiments on SmallPRESENT. This formula originated from the work of [6] and was obtained under the assumption of independently and identically distributed correlations of the involved linear approximations.

Secondly, using the results of our analysis we ended up with somewhat pessimistic results about the success of previous attacks on PRESENT. In particular, we had estimated the capacity based on the enumerated characteristics of the strongest linear approximations, and concluded that if this capacity estimate is less than the capacity of random noise, then distinguishing of the wrong-key and right-key distributions becomes impossible. Fortunately, this problem turned out to be easy to solve. In this Dagstuhl seminar, it was pointed out to us by Bogdanov [2] that also many weaker linear approximations contribute to the total capacity at least as much as random noise. Indeed, if their impact is taken into account (similarly as we had done in our analysis of Matsui's Algorithm 2) and even if not more than random noise, the capacity estimate will never be less than the capacity of random noise. It follows that distinguishing may be possible depending now crucially on the variances of the distributions of the test statistics. Then it is even more important to get the variances correct.

In this talk, we focused on the non-trivial problem of obtaining an accurate estimate of the variance of the capacity of the value distribution of the test statistic in the multidimensional linear key-recovery attack. In this context, the set of linear approximations involved in the online attack is typically not the same as the one used in the offline analysis of the capacity. In the offline analysis the cryptanalyst usually identifies only the strongest linear approximations, which form a small subset of all linear approximations involved in the multidimensional linear attack. Moreover, it is often possible to get accurate estimates of their *ELPs*, which in turn allow a more realistic estimate of the variance of the test statistic.

References

- 1 Céline Blondeau and Kaisa Nyberg. Joint data and key distribution of the linear cryptanalysis test statistic and its impact to data complexity estimates of multiple/multidimensional linear and truncated differential attacks. *IACR Cryptology ePrint Archive*, 2015:935, 2015.
- 2 Andrey Bogdanov. Private communication. Dagstuhl seminar 16021“Symmetric Cryptography”, 2016.
- 3 Andrey Bogdanov and Elmar Tischhauser. On the wrong key randomisation and key equivalence hypotheses in Matsui’s Algorithm 2. In Shiho Moriai, editor, *Fast Software Encryption – 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*, pages 19–38. Springer, 2013.
- 4 Joan Daemen and Vincent Rijmen. Probability distributions of correlation and differentials in block ciphers. *IACR Cryptology ePrint Archive*, 2005:212, 2006.
- 5 Joan Daemen and Vincent Rijmen. Probability distributions of correlation and differentials in block ciphers. *J. Mathematical Cryptology*, 1(3):221–242, 2007.
- 6 Jialin Huang, Serge Vaudenay, Xuejia Lai, and Kaisa Nyberg. Capacity and data complexity in multidimensional linear attack. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology – CRYPTO 2015 – 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, volume 9215 of *Lecture Notes in Computer Science*, pages 141–160. Springer, 2015.
- 7 Gregor Leander. On Linear Hulls, Statistical Saturation Attacks, PRESENT and a Cryptanalysis of PUFFIN. In K. G. Paterson, editor, *EUROCRYPT*, volume 6632 of *LNCS*, pages 303–322. Springer, 2011.
- 8 Sean Murphy. The effectiveness of the linear hull effect. Technical report, Royal Holloway College London, 2009.
- 9 Kaisa Nyberg. Linear cryptanalysis. *SAC Summer School, Sackville, New Brunswick*, 2015.

3.19 Mirror Theory and Cryptography


Jacques Patarin (University of Versailles, FR)

License  Creative Commons BY 3.0 Unported license
© Jacques Patarin

“Mirror Theory” is the theory that evaluates the number of solutions of affine systems of equalities ($=$) and non equalities (\neq) in finite groups. It is deeply related to the security and attacks of many generic cryptographic secret key schemes, for example random Feistel schemes (balanced or unbalanced), Misty schemes, Xor of two pseudo-random bijections to generate a pseudo-random function etc. We will present here general definitions, some theorems, and many examples and computer simulations.

3.20 S-Box Reverse-Engineering: Recovering Design Criteria, Hidden Structures and New Boolean Function Results

Léo Paul Perrin (University of Luxembourg, LU) and Alex Biryukov (University of Luxembourg, LU)

License  Creative Commons BY 3.0 Unported license

© Léo Paul Perrin and Alex Biryukov

Joint work of Léo Paul Perrin, Alex Biryukov, Aleksei Udovenko

Main reference A. Biryukov, L. Perrin, A. Udovenko, “Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1,” *Advances in Cryptology – EUROCRYPT 2016*, to appear 2016.

S-Boxes are key components of many symmetric primitives. Their properties can be used to provide convincing security arguments. However, they may be specified using only a look-up table without providing any rationale. Skipjack, designed by the American NSA, and Kuznyechik, designed by the Russian FSB, are two block ciphers with S-Boxes designed in an unknown fashion.

In this talk, we described how to analyse S-Boxes with secret design criteria or structure. First, a statistical test based on the differential and linear properties of the S-Box can be used to rule out randomness [1]. Second, visual patterns in the Linear Approximation Table can provide useful informations. In fact, we described how these were used in the first step of our reverse-engineering of the S-Box of the last Russian standards [2].


We also presented new results on the 6-bit APN permutation published by Dillon et. al. Using the same methods, we found a decomposition of this function which leads to a more efficient implementation. The structure found can also be generalized to larger dimensions and, while not APN, remains differentially 4-uniform.

References

- 1 Biryukov, A., Perrin, L. *On Reverse-Engineering S-Boxes with Hidden Design Criteria or Structure*. *Advances in Cryptology – CRYPTO 2015. Lecture Notes in Computer Science*, pp. 116–140. Springer Berlin Heidelberg (2015).
- 2 Biryukov, A., Perrin, L., Udovenko, A. *Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1*. *Advances in Cryptology – EUROCRYPT 2016*, to appear.

3.21 Invariant Subspace Attack Against Full Midori64

Yu Sasaki (NTT Labs – Tokyo, JP)

License  Creative Commons BY 3.0 Unported license

© Yu Sasaki

Joint work of Jian Guo, Jérémy Jean, Ivica Nikolić, Kexin Qiao, Yu Sasaki, Siang Meng Sim

We show that the block cipher Midori64 allows a class of invariant subspace. With 2^{32} fractions of the key, the cipher can be distinguished from random permutation with 1 chosen plaintext query. In addition, the key can be recovered with 2 chosen plaintext queries and 2^{18} computations. We the investigate further research directions. The first approach is extending the class of invariant subspaces, which reveals weaker keys. The second approach is designing S-boxes that resist the invariant subspace no matter how the other components of the cipher is chosen. The last approach is a probabilistic transition, which can be applied to reduced-round versions of Midori128.

3.22 Transitivity aspects of the (iterated) Even-Mansour cipher

Ernst Schulte-Geers (BSI – Bonn, DE)

License  Creative Commons BY 3.0 Unported license
© Ernst Schulte-Geers

As a consequence of the CSFG the highly transitive permutation groups have also been classified in the past century.

In particular, the following is true:

► **Theorem.** *Let G be a permutation group on a set X with $|X| \geq 25$. If G is neither the alternating group $A(X)$ nor the symmetric group $S(X)$, then G is at most 3-transitive.*

We interpret the implications for iterated Even-Mansour constructions with non-ideal public permutations P_i (e.g. round functions), and with $X = \{0, 1\}^n$ ($n \geq 5$) as the set plain-/ciphertext blocks.

For non-ideal P_i it may be desirable to strengthen the encryption by iterating several rounds (with independent keys). Under the assumption that the permutation group G generated by the keyed encryption functions is (at least) the alternating group $A(X)$, this generating process should be as fast as possible, i.e. the key additions should interact with the public permutations in such a way such that the r -round encryptions are “totally unrelated, diverse” permutations. From the permutation group viewpoint this is interpreted here as the requirement that no large fraction of the keyed round functions should lie (in large part) in the same “small” permutation group (otherwise the r -round encryptions would “leave” this group only slowly).

Interpreting “small” as “small transitivity”, in our view the theorem above then suggests the following aim: the keyed encryption functions should “look” 4-transitive after as few iterations as possible (since by the theorem above (and recalling that $A(X)$ resp. $S(X)$ are $(|X| - 2)$ - resp. $|X|$ -transitive) a 4-transitive permutation group on X is either $A(X)$ or $S(X)$).

This aim seems only loosely related to conventional cryptographic quality criteria (consider the case where each P_i is the inversion in $\text{GF}(2^n)$).

Ideally only 4 independent keys (i.e. 3 rounds E-M) could suffice to reach the aim.

The orbit counting lemma gives the possibility to estimate statistically the “transitivity look” of r -round encryption functions: the first four factorial moments of the empirical fixed point distribution should all be (approximately) 1, in this respect the empirical fixed point distribution should resemble the *Poiss*(1) distribution. (Recall $\text{Prob}(\text{Poiss}(1) = k) = e^{-1}/k!$.) This gives also a theoretical means to determine a round number: take (say) the smallest no. of rounds (with independent keys) for which the first four factorial moments are close enough to 1 (of course, such a decision would have to be further backed up by cryptanalysis).

However, for block sizes of practical interest this method is impractical.

A better understanding of the mechanisms which lead to maximal diversity, and a practical diversity measure would be desirable.

3.23 Polytopic cryptanalysis

Tyge Tiessen (Technical University of Denmark – Lyngby, DK)

License © Creative Commons BY 3.0 Unported license
© Tyge Tiessen

Main reference T. Tiessen, “Polytopic Cryptanalysis,” IACR Cryptology ePrint Archive, Report 2016/160, 2016.

URL <https://eprint.iacr.org/2016/160.pdf>

Standard differential cryptanalysis uses statistical dependencies between the difference of two plaintexts and the difference of the respective two ciphertexts to attack a cipher. Here we introduce polytopic cryptanalysis which considers interdependencies between larger sets of texts as they traverse through the cipher. We prove that the methodology of standard differential cryptanalysis can unambiguously be extended and transferred to the polytopic case including impossible differentials. We show that impossible polytopic transitions have generic advantages over impossible differentials. To demonstrate the practical relevance of the generalization, we present new low-data attacks on round-reduced DES and AES using impossible polytopic transitions that are able to compete with existing attacks, partially outperforming these.

3.24 Universal Multidimensional and Multiple Zero-Correlation Cryptanalysis

Meiqin Wang (Shandong University – Jinan, CN)

License © Creative Commons BY 3.0 Unported license
© Meiqin Wang

Joint work of Ling Sun, Huaifeng Chen, Meiqin Wang

Multidimensional zero-correlation linear attack and multiple zero-correlation linear attack have been two of the most powerful cryptanalytic techniques for block ciphers. Nevertheless, questions remain regarding how these attacks can be universal without any limitations and can be used to accurately estimate data complexity and success probability. More concretely, the current models for multidimensional and multiple zero-correlation cryptanalysis are not valid in the setting with limited number of zero-correlation linear approximations and the accuracy of the estimation for data complexity can not be guaranteed under that setting. However, in a lot of cases, using too many zero-correlation linear approximations may cause an unacceptable time complexity which leads the attack unfeasible. In order to construct the generalization of the original models built by Bogdanov *et al.* using normal approximation of χ^2 -distribution, we provide new models to estimate data complexity and success probability for multidimensional and multiple zero-correlation attacks without such approximation. As a result, our new models are valid in every setting of multidimensional and multiple linear attacks, which release the limitation on the number of zero-correlation linear approximations, so we name them as universal multidimensional and multiple zero-correlation linear distinguishers.

As an illustration, we apply the universal multiple zero-correlation linear attack on TEA and XTEA. These new attacks can cover more rounds of TEA and XTEA than the previous multiple zero-correlation attacks. Moreover, we reevaluate almost all existing multidimensional and multiple zero-correlation cryptanalysis for various block ciphers, such as CLEFIA, Camellia, LBlock, TWINE, E2, and so on.

3.25 Bit Cryptanalysis on Symmetric Ciphers

Xianyun Wang (Tsinghua University – Beijing, CN)

License  Creative Commons BY 3.0 Unported license
© Xianyun Wang

This talk recalls the existing three main differential attacks: XOR differential attack, modular differential attack and conditional differential attack, and the bit cryptanalysis means the modular differential attack or the XOR differential attack by considering the bit conditions to ensure the differential path hold.

This talk introduces the details of the bit cryptanalysis in differential attack, linear attack and cube attack respectively. As a result, we get the best differential attacks and the linear hull attacks on the full 10 round-reduced SIMON versions, and the cube attack combining with bit cryptanalysis can results in the new key recovery attack on the reduced Keccak-MAC.

4 Panel discussions

4.1 Discussion on Secret Agency Crypto Standards

Orr Dunkelman (University of Haifa, IL)

License  Creative Commons BY 3.0 Unported license
© Orr Dunkelman

The discussion was about what should be the assurance level we need to require as community from cryptography developed by secret agencies.

Participants

- Elena Andreeva
KU Leuven, BE
- Frederik Armknecht
Universität Mannheim, DE
- Daniel J. Bernstein
Univ. of Illinois – Chicago, US
- Eli Biham
Technion – Haifa, IL
- Alex Biryukov
University of Luxembourg, LU
- Andrey Bogdanov
Technical University of Denmark
– Lyngby, DK
- Anne Canteaut
INRIA – Paris, FR
- Benoît Cogliati
University of Versailles, FR
- Joan Daemen
STMicroelectronics –
Diegem, BE
- Itai Dinur
Ben Gurion University – Beer
Sheva, IL
- Orr Dunkelman
University of Haifa, IL
- Henri Gilbert
ANSSI – Paris, FR
- Jian Guo
Nanyang TU – Singapore, SG
- Matthias Hamann
Universität Mannheim, DE
- Tetsu Iwata
Nagoya University, JP
- Jérémy Jean
ANSSI – Paris, FR
- Antoine Joux
UPMC – Paris, FR
- Dmitry Khovratovich
University of Luxembourg, LU
- Matthias Krause
Universität Mannheim, DE
- Nils Gregor Leander
Ruhr-Universität Bochum, DE
- Jooyoung Lee
Sejong University – Seoul, KR
- Gaëtan Leurent
INRIA – Paris, FR
- Stefan Lucks
Bauhaus-Universität Weimar, DE
- Willi Meier
FH Nordwestschweiz –
Windisch, CH
- Bart Mennink
KU Leuven, BE
- Kazuhiko Minematsu
NEC – Kawasaki, JP
- Nicky Mouha
KU Leuven, BE
- Chanathip Namprempre
Thammasat University –
Patumtani, TH
- Mridul Nandi
Indian Statistical Institute –
Kolkata, IN
- Ivica Nikolic
Nanyang TU – Singapore, SG
- Kaisa Nyberg
Aalto University, FI
- Jacques Patarin
University of Versailles, FR
- Léo Paul Perrin
University of Luxembourg, LU
- Bart Preneel
KU Leuven, BE
- Christian Rechberger
Technical University of Denmark
– Lyngby, DK
- Yu Sasaki
NTT Labs – Tokyo, JP
- Ernst Schulte-Geers
BSI – Bonn, DE
- Adi Shamir
Weizmann Inst. – Rehovot, IL
- John Steinberger
Tsinghua Univ. – Beijing, CN
- Marc Stevens
CWI – Amsterdam, NL
- Tyge Tiessen
Technical University of Denmark
– Lyngby, DK
- Meiqin Wang
Shandong Univ. – Jinan, CN
- Xianyun Wang
Tsinghua Univ. – Beijing, CN
- Kan Yasuda
NTT Labs – Tokyo, JP

