Report from Dagstuhl Seminar 20041

Symmetric Cryptography

Edited by

Nils Gregor Leander[1], Bart Mennink[2], Kaisa Nyberg[3], and Kan Yasuda[4]

1 **Ruhr-Universität Bochum, DE,** gregor.leander@rub.de
2 **Radboud University Nijmegen, NL,** b.mennink@cs.ru.nl
3 **Aalto University, FI,** kaisa.nyberg@aalto.fi
4 **NTT – Tokyo, JP,** kan.yasuda.hy@hco.ntt.co.jp

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 20041 "Symmetric Cryptography". The seminar was held on January 19-24, 2020 in Schloss Dagstuhl – Leibniz Center for Informatics. This was the seventh seminar in the series "Symmetric Cryptography". Previous editions were held in 2007, 2009, 2012, 2014, 2016, and 2018.

Participants of the seminar presented their ongoing work and new results on topics of (quantum) cryptanalysis and provable security of symmetric cryptographic primitives. In this report, a brief summary of the seminar is given followed by the abstracts of given talks.

Seminar January 19–24, 2020 – http://www.dagstuhl.de/20041
2012 ACM Subject Classification Security and privacy → Cryptanalysis and other attacks, Security and privacy → Symmetric cryptography and hash functions
Keywords and phrases (quantum) cryptanalysis, constrained platforms, symmetric cryptography
Digital Object Identifier 10.4230/DagRep.10.1.130
Edited in cooperation with Aleksei Udovenko

1 Executive Summary

Nils Gregor Leander (Ruhr-Universität Bochum, DE)
Bart Mennink (Radboud University Nijmegen, NL)
Kaisa Nyberg (Aalto University, FI)
Kan Yasuda (NTT – Tokyo, JP)

IT Security plays a crucial role in everyday life and business. Virtually all modern security solutions are based on cryptographic primitives. *Symmetric* cryptography deals with the case that both the sender and the receiver of a message are using the same key and is highly relevant not only for academia, but also for industrial research and applications.

We identified the following areas as among the most important topics for future research.

Cryptography in the presence of strong constraints. This area deals with the development of symmetric cryptographic primitives and modes that must operate under strong constraints. The area, often indicated by the misleading term lightweight cryptography, has become a very active research field in recent years.

Proving relevant bounds for permutations and (tweakable) block ciphers. Security arguments for symmetric cryptographic primitives often rely on simplifying assumptions and unproven heuristics. Moreover, not only are they often limited by those simplifications, but more fundamentally by the resulting statements.

Development of modes for dedicated functionality or robustness. A cryptographic primitive, e.g., a cryptographic permutation or a (tweakable) block cipher, is of little use without being embedded in a suitable mode of operation. Traditional modes turn such a primitive into an (authenticated) encryption scheme, a message authentication code or a hash function. However, modes of operations could provide more advanced functionalities on the one hand and advanced security features on the other hand.

Quantum cryptanalysis. The threat that one would be able to build a sufficiently large quantum computer has a major impact on the security of many cryptographic schemes we are using today. In particular, the seminal work of Shor showed that such computers would allow to factor large integers and compute discrete logs over large groups in practical time. In the case of symmetric cryptography, the situation seems less critical – but is also significantly less studied. For almost 20 years, it was believed that the only advantage an attacker would have by using a quantum computer when attacking symmetric cryptography is due to Grover's algorithm for speeding up brute force search. Only recently researchers have started to investigate in more detail how the security of symmetric primitives would be affected by attackers equipped with quantum computers.

Seminar Program

The seminar program consisted of short presentations and group meetings. Presentations were about the above topics and other relevant areas of symmetric cryptography, including state-of-the-art cryptanalytic techniques and new designs. Below one can find the list of abstracts for talks given during the seminar. Also, participants met in smaller groups and spent a significant portion of the week, each group intensively discussing a specific research topic. There were eight research groups: 1) Design and analyze ciphers over prime fields, 2) Bounds on the degree of Feistel ciphers with round functions with low univariate degree, 3) Forkcipher, 4) Time-space tradeoffs, 5) Quantum cryptanalysis of hash functions, 6) NIST LWC, 7) Cryptanalysis of the Russian standards, and 8) Security of ProMACs. On the last day of the week the leaders of each group gave brief summaries of achievements. Some teams continued working on the topic after the seminar and started new research collaborations.

2 Table of Contents

3 Overview of Talks

3.1 A MAC Construction for Continuous Message Streams

Frederik Armknecht (Universität Mannheim, DE)

Joint work of Frederik Armknech, Paul Walther, Thorsten Strufe, Gene Tsudik, Martin Beck

Efficiently ensuring integrity of received data requires message authentication code (MAC) tags. The dominating factor determining their security is their length, measured in bits: Short tags are easy to guess, and improving security corresponds to expanding tags. High security constraints hence require sufficiently long tags, which in turn can entail prohibitive cost. This becomes particularly apparent in the context of increasingly common scenarios with typically small payload sizes but strict delay requirements, like robot- or drone control. It is of similar importance in scenarios that suffer from resource scarcity, like LoRaWAN networks with limited battery capacities, or memory protection in Intel SGX with a limitation on the number of costly, additional cells that can be used for integrity protection.

Prior techniques suggested truncation of tags, thus achieving linear performance gain at exponential loss of security. To guarantee security identical to full MAC schemes at the performance of truncated MACs, we suggest a new construction. It introduces internal state to facilitate gradually increasing security upon reception of subsequent messages. We define such schemes as Progressive MACs, provide a formal security framework, prove their security, and evaluate their applicability in several realistic scenarios.

3.2 Security of the STARK-friendly hash functions

Anne Canteaut (INRIA – Paris, FR)

Joint work of Tim Beyne, Anne Canteaut, Itai Dinur, Maria Eichlseder, Gregor Leander, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, Yu Sasaki, Yosuke Todo, Friedrich Wiemer
Main reference Tim Beyne, Anne Canteaut, Itai Dinur, Maria Eichlseder, Gregor Leander, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, Yu Sasaki, Yosuke Todo, Friedrich Wiemer: "Out of Oddity – New Cryptanalytic Techniques against Symmetric Primitives Optimized for Integrity Proof Systems", IACR Cryptol. ePrint Arch., Vol. 2020, p. 188, 2020.
URL https://eprint.iacr.org/2020/188

The security and performance of many integrity proof systems like SNARKs, STARKs and Bulletproofs highly depend on the underlying hash function. For this reason several new proposals have recently been developed. These primitives obviously require an in-depth security evaluation, especially since their implementation constraints have led to less standard design approaches. This work compares the security levels offered by three recent families of such primitives, namely GMiMC, Hades-MiMC and Vision/Rescue. We exhibit low-complexity distinguishers against the GMiMC and Hades-MiMC permutations for most parameters proposed in recently launched public challenges for STARK-friendly hash functions. To achieve those results, we adapt and generalize several cryptographic techniques to fields of odd characteristic.

3.3 Tight Time-Space Lower Bounds for Finding Multiple Collision Pairs (and Applications)

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

Main reference Itai Dinur: "Tight Time-Space Lower Bounds for Finding Multiple Collision Pairs and Their Applications", in Proc. of the Advances in Cryptology – EUROCRYPT 2020 – 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part I, Lecture Notes in Computer Science, Vol. 12105, pp. 405–434, Springer, 2020.
URL https://doi.org/10.1007/978-3-030-45721-1_15

We consider a *collision search problem* (CSP), where given a parameter C, the goal is to find C collision pairs in a random function $f : [N] \to [N]$ (where $[N] = \{0, 1, \ldots, N-1\}$) using S bits of memory. Algorithms for CSP have numerous cryptanalytic applications such as space-efficient attacks on double and triple encryption. The best known algorithm for CSP is *parallel collision search* (PCS) published by van Oorschot and Wiener, which achieves the time-space tradeoff $T^2 \cdot S = \tilde{O}(C^2 \cdot N)$.

In this talk, I will prove that any algorithm for CSP satisfies $T^2 \cdot S = \tilde{\Omega}(C^2 \cdot N)$, hence the best known time-space tradeoff is optimal. On the other hand, I give strong evidence that proving similar unconditional time-space tradeoff lower bounds on CSP applications (such as breaking double and triple encryption) may be very difficult, and would imply a breakthrough in complexity theory. Hence, I propose a new restricted model of computation and prove that under this model, the best known time-space tradeoff attack on double encryption is optimal.

3.4 Analyzing the Linear Keystream Biases in AEGIS

Maria Eichlseder (TU Graz, AT)

Joint work of Maria Eichlseder, Marcel Nageler, Robert Primas
Main reference Maria Eichlseder, Marcel Nageler, Robert Primas: "Analyzing the Linear Keystream Biases in AEGIS", IACR Cryptol. ePrint Arch., Vol. 2019, p. 1372, 2019.
URL https://eprint.iacr.org/2019/1372

AEGIS is one of the authenticated encryption designs selected for the final portfolio of the CAESAR competition [2, 3]. It combines the AES round function and simple Boolean operations to update its large state and extract a keystream to achieve an excellent software performance. In 2014, Minaud discovered slight biases in the keystream based on linear characteristics [1]. For family member AEGIS-256, these could be exploited to undermine the confidentiality faster than generic attacks, but this still requires very large amounts of data. For final portfolio member AEGIS-128, these attacks are currently less efficient than generic attacks.

We search for better linear characteristics, as well as upper bounds on the best possible correlation. We observe that straightforward truncated models of linear characteristics of AEGIS only produce very weak bounds since they fail to capture connections and constraints that follow from dependencies in the AEGIS state update function. We briefly discuss several examples of such linear incompatibilities from the related literature, where they have primarily been identified in the context of linear key or tweakey schedules. To obtain tighter bounds and consistent solutions, we identify additional constraints on the differences and

higher-order differences of the linear masks and propose an improved truncated model. This model yields much better results, including consistent solutions for AEGIS-128, but still shows a significant gap between the bounds and the best found characteristics, mainly due to the Boolean output function. We propose a partially bitwise model to close this gap. As a result, for all AEGIS family members, we derive upper bounds below 2^{-128} for the squared correlation contribution of any single suitable linear characteristic. This supports AEGIS' security with realistic amounts of data. Finally, we apply Constraint Programming (CP) to find consistent characteristics and obtain improved attacks for all members.

References

1 Brice Minaud. Linear biases in AEGIS keystream. In Antoine Joux and Amr M. Youssef, editors, *Selected Areas in Cryptography – SAC 2014*, volume 8781 of *LNCS*, pages 290–305. Springer, 2014.

2 Hongjun Wu and Bart Preneel. AEGIS: A fast authenticated encryption algorithm. In Tanja Lange, Kristin E. Lauter, and Petr Lisonek, editors, *Selected Areas in Cryptography – SAC 2013*, volume 8282 of *LNCS*, pages 185–201. Springer, 2013.

3 Hongjun Wu and Bart Preneel. AEGIS: A fast authenticated encryption algorithm (v1.1). Submission to CAESAR: Competition for Authenticated Encryption. Security, Applicability, and Robustness (Round 3 and Final Portfolio), September 2016. http://competitions.cr.yp.to/round3/aegisv11.pdf.

3.5 Higher-Order Differential Attacks on Ciphers with Low-Degree Polynomial S-Boxes in $GF(2^n)$: Open Problems

Lorenzo Grassi (TU Graz, AT)

Joint work of Lorenzo Grassi, Carlos Cid, Maria Eichlseder, Reinhard Lüftenegger, Christian Rechberger, Markus Schofnegger, Qingju Wang

Higher-order differential attacks are among the most powerful attacks against low-degree ciphers and hash functions. Predicting the evolution of the degree of the cipher (as a function of the number of rounds) is the main issue in such attacks. Given an SPN cipher over a field $\mathbb{F}$, where each round has algebraic degree δ, it is a common belief that the degree grows essentially exponentially in δ. Several analyses made in the literature confirm this belief, with the only exception of the case in which the algebraic degree of the function is close to its maximum. As a result, the number of rounds necessary for security against higher-order differential attacks grows logarithmic in the size of F.

In this presentation, we show that surprisingly, if the round function/S-Box can be described as an invertible (low-degree) polynomial function in $\mathbb{F}_{2^n}$, then the algebraic degree grows linearly with the number of rounds, and not exponentially. In particular, we present several examples of this, including iterated Even-Mansour and SPN ciphers with (low-degree) polynomial round functions/S-Boxes.

3.6 Analysis on Adiantum

Tetsu Iwata (Nagoya University, JP)

Joint work of Habu Makoto, Tetsu Iwata

Adiantum is a disk sector encryption scheme designed by Google [1]. It can be seen as a tweakable, variable-input-length strong pseudorandom permutation, and has an indistinguishability security proof. In this talk, we first present a distinguishing attack with the birthday complexity. We then present plaintext recovery and forgery attacks, with almost the same complexity as the distinguishing attack. These results do not violate the security proof.

References

1 Paul Crowley and Eric Biggers. Adiantum: length-preserving encryption for entry-level processors. *IACR Transactions on Symmetric Cryptology*, 2018, Issue 4:39–61, 2018.

3.7 Some Thoughts on Boomerang Switches

Virginie Lallemand (LORIA – Nancy, FR)

Joint work of Hamid Boukerrou, Paul Huynh, Virginie Lallemand, Bimal Mandal, Marine Minier

Boomerang distinguishers were introduced at FSE 1999 by David Wagner. It is a variant of differential cryptanalysis that works on quartets of messages and studies if a difference "comes back". Namely, it looks at the probability that:

$$E^{-1}(E(M_1) + b) + E^{-1}(E(M_1 + a) + b) = a.$$

In practice, this type of distinguisher is built by splitting the cipher in three parts:

$$E = E_1 \circ E_m \circ E_0,$$

where E_m is a middle part that contains the boomerang switch. With such a framework, the probability of the distinguisher is evaluated to be: p^2q^2r where p is the probability of the differential used over E_0, q the one used over E_1 and r is the probability of the boomerang switch.

At Eurocrypt 2018, Cid et al. introduced the Boomerang Connectivity Table (BCT), a tool to easily compute the value of r for the case where the cipher E is a substitution-permutation network and where E_m covers one round.

In this talk, we introduce the FBCT, the counterpart of the BCT for the case where the cipher follows a Feistel construction. We show that the value of an FBCT coefficient is related to the second order derivative of the Sbox at play and study its properties.

3.8 The First Chosen-Prefix Collision on SHA-1

Gaëtan Leurent (INRIA – Paris, FR) and Thomas Peyrin

Main reference Gaëtan Leurent, Thomas Peyrin: "SHA-1 is a Shambles – First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust", IACR Cryptol. ePrint Arch., Vol. 2020, p. 14, 2020.
URL https://eprint.iacr.org/2020/014

The SHA-1 hash function was designed in 1995 and has been widely used during two decades. A theoretical collision attack was first proposed in 2004 [3], but due to its high complexity it was only implemented in practice in 2017, using a large GPU cluster [2]. More recently, an almost practical *chosen-prefix* collision attack against SHA-1 has been proposed [1]. This more powerful attack allows to build colliding messages with two arbitrary prefixes, which is much more threatening for real protocols.

In this talk, we reported the first practical implementation of this attack, and its impact on real-world security with a PGP/GnuPG impersonation attack. We managed to significantly reduce the complexity of collisions attack against SHA-1: on an Nvidia GTX 970, identical-prefix collisions can now be computed with a complexity of $2^{61.2}$ rather than $2^{64.7}$, and chosen-prefix collisions with a complexity of $2^{63.4}$ rather than $2^{67.1}$. When renting cheap GPUs, this translates to a cost of 11k US$ for a collision, and 45k US$ for a chosen-prefix collision, within the means of academic researchers. Our actual attack required two months of computations using 900 Nvidia GTX 1060 GPUs (we paid 75k US$ because GPU prices were higher, and we wasted some time preparing the attack).

Therefore, the same attacks that have been practical on MD-5 since 2009 are now practical on SHA-1. In particular, chosen-prefix collisions can break signature schemes and handshake security in secure channel protocols (TLS, SSH). We strongly advise to remove SHA-1 from those type of applications as soon as possible.

We exemplify our cryptanalysis by creating a pair of PGP/GnuPG keys with different identities, but colliding SHA-1 certificates. A SHA-1 certification of the first key can therefore be transferred to the second key, leading to an impersonation attack. This proves that SHA-1 signatures now offers virtually no security in practice. The legacy branch of GnuPG still uses SHA-1 by default for identity certifications, but after notifying the authors, the modern branch now rejects SHA-1 signatures (the issue is tracked as CVE-2019-14855).

References

1 Gaëtan Leurent and Thomas Peyrin. From collisions to chosen-prefix collisions application to full SHA-1. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part III*, volume 11478 of *LNCS*, pages 527–555. Springer, Heidelberg, May 2019.

2 Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, and Yarik Markov. The first collision for full SHA-1. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 570–596. Springer, Heidelberg, August 2017.

3 Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Victor Shoup, editor, *CRYPTO 2005*, volume 3621 of *LNCS*, pages 17–36. Springer, Heidelberg, August 2005.

3.9 Conditional Cube Attack on Keccak Keyed Modes

Willi Meier (FH Nordwestschweiz – Windisch, CH)

Joint work of Zheng Li, Xiaoyang Dong, Wenquan Bi, Keting Jia, Xiaoyun Wang, Willi Meier
Main reference Zheng Li, Xiaoyang Dong, Wenquan Bi, Keting Jia, Xiaoyun Wang, Willi Meier: "New Conditional Cube Attack on Keccak Keyed Modes", IACR Trans. Symmetric Cryptol., Vol. 2019(2), pp. 94–124, 2019.
URL https://doi.org/10.13154/tosc.v2019.i2.94-124

The conditional cube attack on round-reduced Keccak keyed modes was proposed by Huang et al. at Eurocrypt 2017. A new conditional cube attack on Keccak is proposed by removing some limitations of previous attacks. As a result, the time complexity of key recovery attacks on 7-round Keccak-MAC-512 can be reduced from 2^{111} to 2^{72}, and similarly, the time complexity of key recovery on KMAC256 can be reduced from 2^{147} to 2^{139}.

3.10 Accelerating MRAE

Kazuhiko Minematsu (NEC – Kawasaki, JP)

Since nonce-based AE (NAE) schemes are generally fragile to a misuse of nonce, MRAE has received significant attention from the initial proposal by Rogaway and Shrimpton at Eurocrypt 2006. They showed a generic MRAE construction called SIV. SIV has become a de-facto scheme for MRAE, however, one notable drawback is its two-pass operation for both encryption and decryption. This implies that MRAE built on SIV is slower than the integrated nonce-based AE schemes, such as OCB.

In this talk, we propose a new method to improve this situation. Particularly, our MRAE proposal (decryption-integrated SIV or DI-SIV) allows to decrypt as fast as a plain decryption, hence theoretically doubles its speed from the original SIV, while keeping the encryption speed equivalent to SIV.

We show three generic compositions for DI-SIV, called DI-SIV1, DI-SIV2 and DI-SIV3, and prove their security bounds that are comparable to the original SIV. We also provide several concrete instantiations to show their effectiveness compare to the existing MRAE schemes, namely the same encryption speed but decryption is ideally fast.

3.11 Bits and Pieces

Orr Dunkelman (University of Haifa, IL)

Joint work of Orr Dunkelman, Nathan Keller, Abhishek Kumar, Eran Lambooij, Somitra Sandhya, Ariel Weizman

This talk presented a few ideas in the context of block cipher's cryptanalysis.

1. The partition of plaintext pairs according whether they satisfied the differential characteristic in the first round or not. This allows improving the probability of boomerang attacks

and the bias in differential-linear attacks, as in each partition the probability/biased is increased significantly. (joint work with Nathan Keller and Ariel Weizman)
2. We showed how to use multiple differential-linear approximations to recover the decorrelation module keys (joint work with Nathan Keller and Ariel Weizman)
3. We showed that counting the number of active S-boxes is not always a good measure for security estimation. We showed a 4-round Feistel cipher with a round function composed of many S-box/MDS layers, but with very high probability one could build a decent differential characteristic for the scheme. (joint work with Eran Lambooij, Abhishek Kumar, Somitra Sandhya).
4. Finally, we used ideas related to the above idea to attack the Korean FPE standard FEA-1.

3.12 Update on the ISO Standardization of Kuznyechik

Léo Perrin (INRIA – Paris, FR)

Joint work of Xavier Bonnetain, Léo Perrin, Shizhu Tian
Main reference Xavier Bonnetain, Léo Perrin, Shizhu Tian: "Anomalies and Vector Space Search: Tools for S-Box Analysis", in Proc. of the Advances in Cryptology – ASIACRYPT 2019 – 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I, Lecture Notes in Computer Science, Vol. 11921, pp. 196–223, Springer, 2019.
URL https://doi.org/10.1007/978-3-030-34578-5_8

In this talk, I presented the latest results on a specific S-box, how they disprove verifiable claims by its designers, and what their consequences were at ISO.

A year ago, we established that the S-box of Kuznyechik [2] (the block cipher recently standardized in Russia) is more structured than previously thought [3]: it can be written as a so-called TKlog. Yet, at ISO/IEC meetings, the Russian delegation was still pushing for the standardization of this block cipher, insisting that the S-box was generated by picking permutations uniformly at random until some properties were met.

To figure out if this claim could be true, we investigated the properties of random permutations (both in terms of cryptographic properties and in terms of structure) [1]. We found that a C implementation of this S-box exists that fits in 1155 bits. As there are $256! \approx 2^{1684}$ distinct 8-bit permutations, the probability that a C-implementation at least this short exists is at most $2^{1155+1-1684} = 2^{-528}$. This bound would be tight if all 2^{1155+1} bit strings of length at most 1155 were valid ASCII encoded C programs implementing 8-bit permutations; we thus expect it to be an extremely loose upper bound. As a consequence, we have to conclude that the designers of Kuznyechik are lying about the design process of a key component of their cipher: the probability of obtaining such a structured S-box using the process they disclosed is negligible.

At an ISO meeting held in Paris in October, the Russian delegation thus tried to convince the audience that all permutations are in fact structured (in spite of the facts highlighted above), the aim being to argue that their claims of randomness are true. Unsurprisingly, they failed to convince other countries representatives. As a consequence, the standardization of Kuznyechik has been stopped.

References

1 Bonnetain X., Perrin L., Tian S. *Anomalies and Vector Space Search: Tools for S-Box Analysis*. In: Galbraith S., Moriai S. (eds) Advances in Cryptology – ASIACRYPT 2019. Lecture Notes in Computer Science, vol 11921, pp 196–223. Springer, Cham.

2 Federal Agency on Technical Regulation and Metrology. *Information technology – data security: Block ciphers*. 2015. English version available at http://wwwold.tc26.ru/en/standard/gost/GOST_R_34_12_2015_ENG.pdf

3 Perrin, L. (2019). *Partitions in the S-Box of Streebog and Kuznyechik*. IACR Transactions on Symmetric Cryptology, 2019(1), 302-329.

3.13 On generating collisions in blinded keyed hashing

Yann Rotella (University of Versailles, FR)

Joint work of Yann Rotella, Joan Daemen, Jonathan Fuchs

In this talk, we analyze keyed-hashing modes with respect to collision resistance in a blinded keyed hashing model for the attacker in both serial and parallel constructions to do compression functions in cryptography.

The serial construction is used in CBC-MAC for blockcipher-based or DonkeySponge for Permutation-based, while the parallel one is used in P-MAC (blockcipher-based) or Farfalle (Permutation-based).

We try to obtain collisions in this setting by using differential trails existing in the inner permutation (or underlying blockcipher). Eventually, we mount two different attack strategies for both constructions, by using a single trail core. Our attack takes use of a huge set of trails, all sharing the same trail core.

More precisely, the expected number of inputs that we need to take into account for finding a collision is 2^W where W is defined as the sum of the weights of the round differentials starting from the 2nd round and where the weight of the last round is divided by 2. Also, in the case of the parallel construction, W is twice as large as in the case of the serial construction.

So in the case of a collision attack based on a single trail core, under reasonable assumptions the parallel construction offers twice the security level than the serial construction.

3.14 Improved Differential-Linear Attacks with Applications to ARX Ciphers

Yosuke Todo (NTT – Tokyo, JP)

Joint work of Christof Beierle, Gregor Leander, Yosuke Todo

Differential cryptanalysis and linear cryptanalysis are ones of the most common cryptanalysis techniques. The differential-linear attack is an extension of their techniques, and it used both in the same time: the differential characteristic for the first part and the linear trail for the second part. Usually, when the differential probability is p and the linear correlation

is q, the required data complexity is $p^{-2}q^{-4}$. We proposed several new techniques for the differential-linear attack, in particular, the main focus of the application is ARX design.

On the differential part, we propose a new technique, where many "right pairs" are generated for free once we find only one "right pair". This technique allows us to distinguish the ciphers with data complexity of $p^{-1}q^{-4}$.

On the linear part, we propose a new partition technique using multiple linear trails. ARX ciphers have many multiple linear trails with particular structure, and these linear trails can be evaluated by guessing the same key bits. Moreover, we propose a new key-recovery algorithm, where the involved key bits are decomposed into two parts and only guessing the first part is enough to recover the whole of keys.

3.15 Attacks on the Legendre PRF

Aleksei Udovenko (CryptoExperts – Paris, FR)

Joint work of Aleksei Udovenko, Ward Beullens, Tim Beyne, Giuseppe Vitto
Main reference Ward Beullens, Tim Beyne, Aleksei Udovenko, Giuseppe Vitto: "Cryptanalysis of the Legendre PRF and generalizations", IACR Cryptol. ePrint Arch., Vol. 2019, p. 1357, 2019.
URL https://eprint.iacr.org/2019/1357

The Legendre PRF relies on the conjectured pseudorandomness properties of the Legendre symbol with a hidden shift. Originally proposed as a PRG by Damgård at CRYPTO 1988 [1], it was recently suggested as an efficient PRF for multiparty computation purposes by Grassi et al. at CCS 2016. Moreover, the Legendre PRF is being considered for usage in the Ethereum 2.0 blockchain.

In the talk, I describe a birthday-bound attack on the Legendre PRF with reduced query complexity compared to previous attacks due to Khovratovich [2]. Furthermore, I study a higher-degree generalization of the PRF and point out a large class of weak keys for this construction.

References

1 Ivan Damgard. *On the randomness of Legendre and Jacobi sequences*. In Shafi Goldwasser, editor, CRYPTO'88, volume 403 of LNCS, pages 163–172. Springer, Heidelberg, August 1990
2 Dmitry Khovratovich. Key recovery attacks on the Legendre PRFs within the birthday bound. Cryptology ePrint Archive, Report 2019/862, 2019

3.16 Forkciphers and Provable Security

Damian Vizár (CSEM – Neuchatel, CH)

Joint work of Elena Andreeva, Virginie Lallemand, Antoon Purnal, Reza Reyhanitabar, Arnab Roy, Damian Vizár

We report updates on the security of NIST Lightweight Cryptography candidate algorithm SAEF [1]. SAEF is a mode of operation of a forkcipher for authenticated encryption. SAEF was proposed with security up to $\approx 2^{n/2}$ processed bytes in the nonce-based AE security

model in the original submission. The new result says that SAEF has online-AE (OAE) security up to $2^{n/2}$ processed bytes. This means that SAEF can be safely used when plaintext or ciphertext arrives in blocks, and does not crumble if nonces accidentally repeat, while being more efficient than many existing constructions.

We then propose several directions of interest. Firstly we point out the similarity of DECK function and multi-forkcipher security notions, and propose to study their relation. We remark that a recent DECK construction Farfalle can never achieve quantitatively optimal DECK security, and suggest that a notion between MFC and DECK would model it more closely.

References

1 Andreeva, E., Lallemand, V., Purnal, A., Reyhanitabar, R., Roy, A., Vizár, D.: ForkAE v1. Submission to NIST Lightweight Cryptography Project (2019)

Participants

- Elena Andreeva
Technical University of Denmark – Lyngby, DK
- Frederik Armknecht
Universität Mannheim, DE
- Christof Beierle
Ruhr-Universität Bochum, DE
- Daniel J. Bernstein
University of Illinois – Chicago, US
- Eli Biham
Technion – Haifa, IL
- Christina Boura
University of Versailles, FR
- Anne Canteaut
INRIA – Paris, FR
- Joo Yeon Cho
ADVA Optical Networking – Martinsried, DE
- Itai Dinur
Ben Gurion University – Beer Sheva, IL
- Christoph Dobraunig
Radboud University Nijmegen, NL
- Orr Dunkelman
University of Haifa, IL
- Maria Eichlseder
TU Graz, AT
- Patrick Felke
FH Emden, DE
- Henri Gilbert
ANSSI – Paris, FR
- Lorenzo Grassi
TU Graz, AT
- Tetsu Iwata
Nagoya University, JP
- Pierre Karpman
Université Grenoble Alpes – Saint Martin d'Hères, FR
- Dmitry Khovratovich
Ethereum – Luxembourg, LU
- Virginie Lallemand
LORIA – Nancy, FR
- Tanja Lange
TU Eindhoven, NL
- Nils Gregor Leander
Ruhr-Universität Bochum, DE
- Gaëtan Leurent
INRIA – Paris, FR
- Stefan Lucks
Bauhaus-Universität Weimar, DE
- Atul Luykx
Swirlds – San Francisco, US
- Willi Meier
FH Nordwestschweiz – Windisch, CH
- Florian Mendel
Infineon Technologies AG – Neubiberg, DE
- Bart Mennink
Radboud University Nijmegen, NL
- Kazuhiko Minematsu
NEC – Kawasaki, JP
- Maria Naya-Plasencia
INRIA – Paris, FR
- Kaisa Nyberg
Aalto University, FI
- Léo Perrin
INRIA – Paris, FR
- Bart Preneel
KU Leuven, BE
- Yann Rotella
University of Versailles, FR
- Arnab Roy
University of Bristol, GB
- Yu Sasaki
NTT – Tokyo, JP
- Ling Song
Chinese Academy of Sciences – Beijing, CN
- Meltem Sonmez Turan
NIST – Gaithersburg, US
- Marc Stevens
CWI – Amsterdam, NL
- Stefano Tessaro
University of Washington – Seattle, US
- Emmanuel Thomé
INRIA Nancy – Grand Est, FR
- Yosuke Todo
NTT – Tokyo, JP
- Aleksei Udovenko
CryptoExperts – Paris, FR
- Damian Vizár
CSEM – Neuchatel, CH
- Kan Yasuda
NTT – Tokyo, JP