Report from Dagstuhl Seminar 24041

Symmetric Cryptography

Christof Beierle*[1], Bart Mennink*[2], María Naya-Plasencia*[3], Yu Sasaki*[4], and Rachelle Heim Boissier†[5]

1 **Ruhr-Universität Bochum, DE.** `christof.beierle@rub.de`
2 **Radboud University Nijmegen, NL.** `b.mennink@cs.ru.nl`
3 **INRIA – Paris, FR.** `maria.naya_plasencia@inria.fr`
4 **NTT – Tokyo, JP.** `yu.sasaki.sk@hco.ntt.co.jp`
5 **UVSQ, Paris Saclay, FR.** `rachelle.heim@uvsq.fr`

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar "Symmetric Cryptography" (24041). The seminar was held on January 21–26, 2024 in Schloss Dagstuhl – Leibniz Center for Informatics. This was the ninth seminar in the series "Symmetric Cryptography". Previous editions were held in 2007, 2009, 2012, 2014, 2016, 2018, 2020 and 2022. Participants of the seminar presented their ongoing work and new results on topics of cryptanalysis and (post-quantum) provable security of symmetric cryptographic primitives. Participants also worked together within seven research group dedicated to various topics (Cryptanalysis of Poseidon, Cryptanalysis of TEA-3, Exploitation of the wrong key randomization hypothesis non-conformity in key recovery attacks, Cryptanalysis of SCARF, Differential cryptanalysis and more, Key control security and Security of sponge combiners). In this report, a brief summary of the seminar is given, followed by the abstracts of given talks and a summary of the progress of each research group.

Seminar January 21–26, 2024 – https://www.dagstuhl.de/24041
2012 ACM Subject Classification Security and privacy → Cryptanalysis and other attacks; Security and privacy → Symmetric cryptography and hash functions
Keywords and phrases Lightweight Cryptography, New Applications of Symmetric Cryptography, Permutation-Based Cryptography
Digital Object Identifier 10.4230/DagRep.14.1.72

1 Executive Summary

Christof Beierle (Ruhr-Universität Bochum, DE, christof.beierle@rub.de)
Bart Mennink (Radboud University Nijmegen, NL, b.mennink@cs.ru.nl)
María Naya-Plasencia (INRIA – Paris, FR, maria.naya_plasencia@inria.fr)
Yu Sasaki (NTT – Tokyo, JP, yu.sasaki.sk@hco.ntt.co.jp)

IT Security plays an increasingly crucial role in our everyday life and business. Virtually all modern security solutions are based on cryptographic primitives. Symmetric cryptography deals with the case where both the sender and the receiver of a message are using the same key. Due to their good performance, symmetric cryptosystems are the main workhorses of cryptography and are highly relevant not only for academia, but also for industrial activities.

* Editor / Organizer
† Editorial Assistant / Collector

Symmetric Cryptography, *Dagstuhl Reports*, Vol. 14, Issue 1, pp. 72–89
Editors: Christof Beierle, Bart Mennink, María Naya-Plasencia, and Yu Sasaki
DAGSTUHL REPORTS Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

For this Dagstuhl Seminar we focused on several topics, which we believe to be of great importance for the research community and, likewise, to have a positive impact on industry and the deployment of secure crypto in the future.

- **Follow Up on Main Results from Last Dagstuhl Seminar.** At the last Dagstuhl Seminar on symmetric cryptography in 2022, the participants were divided into six groups in order to discuss research topics proposed by each participant. The discussions were very productive and there were and will be publications from several groups. We believe that the discussions and results from these 2022 work groups reflect the main interests of the community and are useful topics to continue to discuss at the Dagstuhl Seminar in 2024. Participants at the 2024 Dagstuhl Seminar who also participated in the work groups in 2022 were thus invited to present their finished results.
- **Design and Analysis of Symmetric Crypto for New Applications.** Recently, the design of symmetric-key primitives has started to focus on different types of optimization. Those optimizations could be with respect to performance and with respect to special security requirements. Stated differently, one first considers a target application (such as multi-party computation or non-interactive zero-knowledge proofs), and only then designs symmetric-key primitives for this purpose. This causes a paradigm shift in design criteria. During this seminar, we explored the security of recently introduced ciphers that were designed specifically for such target applications, and develop novel ciphers with improved security arguments and guarantees.
- **Generic Analysis of Emerging Modes.** Permutation-based cryptography has gained astounding popularity in the last decade, and security proofs are performed in the ideal permutation model. A similar phenomenon is visible in various ideal cipher-based constructions that have appeared recently. In this seminar, we explored how results with different models (such as a standard model and an ideal model) compare from a theoretical perspective, and investigated what cryptanalytical results on certain primitives mean for the targeted construction.

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. The list of abstracts for talks given during the seminar can be found below. Also, participants met in smaller groups and spent a significant portion of the week, each group intensively discussing a specific research topic. There were seven research groups:

- Cryptanalysis of Poseidon;
- Cryptanalysis of TEA-3;
- Exploitation of the wrong key randomization hypothesis non-conformity in key recovery attacks;
- Cryptanalysis of SCARF;
- Differential cryptanalysis and more;
- Key control security;
- Security of sponge combiners.

On the last day of the week the leaders of each group gave brief summaries of achievements. An abstract corresponding to each research group can be found below. Some teams continued working on the topic after the seminar and started new research collaborations.

2 Table of Contents

Executive Summary

Overview of Talks

Working groups

3 Overview of Talks

3.1 Follow-up on Differential Meet-In-The-Middle Cryptanalysis

Zahra Ahmadian (Shahid Beheshti University – Tehran, IR)

Joint work of Zahra Ahmadian, Akram Khalesi, Dounia M'Foukh, Hossein Moghimi, María Naya-Plasencia

In this presentation, we generalize the differential meet-in-the-middle attack proposed at Crypto 2023 [1] to incorporate truncated differentials. Subsequently, we propose three enhancements to the differential-MITM attack: a stronger parallel partitioning technique covering more rounds, probabilistic key recovery requiring less key material, and benefiting from the state-test technique previously proposed in the context of impossible differential attacks.

Using a MILP-based tool to automate the search for optimized overall complexity, incorporating some of the proposed improvements, we develop the best-known attacks on the cipher CRAFT, reaching 23 rounds compared to the previous 21. We also improve the best attack on the 25-round SKINNY-128-384 and provide a new attack on the 23-round SKINNY-64-192.

References

1 Boura, C., David, N., Derbez, P., Leander, G., Naya-Plasencia, M.: Differential meet-in-the-middle cryptanalysis. In: Advances in Cryptology – CRYPTO 2023 – 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III. Lecture Notes in Computer Science, vol. 14083, pp. 240–272. Springer (2023)

3.2 A New Post-Quantum Proof Framework

Ritam Bhaumik (EPFL – Lausanne, CH)

Joint work of Ritam Bhaumik, Benoît Cogliati, Jordan Ethan, Ashwin Jha
Main reference Ritam Bhaumik, Benoît Cogliati, Jordan Ethan, Ashwin Jha: "On Quantum Secure Compressing Pseudorandom Functions", in Proc. of the Advances in Cryptology – ASIACRYPT 2023 – 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part III, Lecture Notes in Computer Science, Vol. 14440, pp. 34–66, Springer, 2023.
URL https://doi.org/10.1007/978-981-99-8727-6_2

While quantum attacks on symmetric cryptosystems have been less devastating than those on certain popular public-key cryptosystems, classical provable security results on symmetric modes are not trivial to extend to the Q2 setting where the adversary has superposition access to the mode. In this work we attempt to build a generic proof framework applicable to such games by building on several previous works on compressed oracles.

3.3 A generic algorithm for efficient key recovery in differential attacks – and its associated tool

Christina Boura (University of Versailles, FR), Nicolas David, Patrick Derbez (University of Rennes, FR), Rachelle Heim Boissier (University of Versailles, FR), and María Naya-Plasencia (INRIA – Paris, FR)

Main reference Christina Boura, Nicolas David, Patrick Derbez, Rachelle Heim Boissier, María Naya-Plasencia: "A generic algorithm for efficient key recovery in differential attacks – and its associated tool", 2024.
URL https://eprint.iacr.org/2024/288

Differential cryptanalysis is an old and powerful attack against block ciphers. While different techniques have been introduced throughout the years to improve the complexity of this attack, the key recovery phase remains a tedious and error-prone procedure. In this talk, we present a new algorithm and its associated tool that permits, given a distinguisher, to output an efficient key guessing strategy. Our tool can be applied to SPN ciphers whose linear layer consists of a bit-permutation and whose key schedule is linear or almost linear. It can be used not only to help cryptanalysts find the best differential attack on a given cipher but also to assist designers in their security analysis. We applied our tool to four targets: RECTANGLE, PRESENT-80, SPEEDY-7-192 and GIFT-64. We extend the previous best attack on RECTANGLE-128 by one round and the previous best differential attack against PRESENT-80 by 2 rounds. We improve a previous key recovery step in an attack against SPEEDY and present more efficient key recovery strategies for RECTANGLE-80 and GIFT. Our tool outputs the results in only a second for most targets.

3.4 Differential Meet-In-The-Middle Cryptanalysis

Christina Boura (University of Versailles, FR)

Joint work of Christina Boura, Nicolas David, Patrick Derbez, Gregor Leander, María Naya-Plasencia
Main reference Christina Boura, Nicolas David, Patrick Derbez, Gregor Leander, María Naya-Plasencia: "Differential Meet-In-The-Middle Cryptanalysis", in Proc. of the Advances in Cryptology – CRYPTO 2023 – 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III, Lecture Notes in Computer Science, Vol. 14083, pp. 240–272, Springer, 2023.
URL https://doi.org/10.1007/978-3-031-38548-3_9

In this talk we introduce the differential meet-in-the-middle framework, a new cryptanalysis technique for symmetric primitives. Our new cryptanalysis method combines techniques from both meet-in-the-middle and differential cryptanalysis. As such, the introduced technique can be seen as a way of extending meet-in-the-middle attacks and their variants but also as a new way to perform the key recovery part in differential attacks. We apply our approach to SKINNY-128-384 in the single-key model and to AES-256 in the related-key model. Our attack on SKINNY-128-384 permits to break 25 out of the 56 rounds of this variant and improves by two rounds the previous best known attacks. For AES-256 we attack 12 rounds by considering two related keys, thus outperforming the previous best related-key attack on AES-256 with only two related keys by 2 rounds.

3.5 Generalized Initialization of the Duplex Construction

Christoph Dobraunig (Intel – Villach, AT) and Bart Mennink (Radboud University Nijmegen, NL)

Main reference Christoph Dobraunig, Bart Mennink: "Generalized Initialization of the Duplex Construction", in Proc. of the Applied Cryptography and Network Security – 22nd International Conference, ACNS 2024, Abu Dhabi, United Arab Emirates, March 5-8, 2024, Proceedings, Part II, Lecture Notes in Computer Science, Vol. 14584, pp. 460–484, Springer, 2024.
URL https://doi.org/10.1007/978-3-031-54773-7_18

If we consider (authenticated) encryption schemes based on the sponge/duplex construction, it is typically assumed that the adversary has the capability to choose the nonce/IV on its will (except for repetitions). In this talk, we discuss how the security changes if restrictions on the choice of the nonce are imposed, varying from the global nonce case over the random nonce case to the nonce on key case.

3.6 Key Control Security of PRF-Based KDFs; Introduction and Preliminary Cryptanalysis Results

Tetsu Iwata (Nagoya University, JP)

Joint work of Tetsu Iwata, Keisuke Ozeki

NIST SP 800-108r1 specifies Key Derivation Functions (KDFs) based on PseudoRandom Functions (PRFs). In the document, the key control security is discussed, and it is pointed out KDFs based on CMAC have security issues. In this talk, we review the notion of the key control security and the security issues. We then point out similar security issues are in other block cipher based PRFs. We also present an attempt to formalize a cryptographic definition of the key control security, and discuss possible directions for future research.

3.7 Range-Restricted Vertex Labeling and Its Applications

Ashwin Jha (Ruhr-Universität Bochum, DE)

Joint work of Ashwin Jha, Mridul Nandi, Abishanka Saha

Most of the beyond-the-birthday-bound deterministic MAC (or PRF) constructions, like PMAC+ and LightMAC+, can be viewed as an instance of the Double-block Hash-then-Sum (DbHtS) paradigm (DDNP, IACR ToSC 2018). It is well-known (KLL, EUROCRYPT 2020; JN, JoC 2020; LNS, CRYPTO 2018) that DbHtS constructions are secure up to roughly $2^{3n/4}$ queries, where n denotes the block size. In contrast, the security guarantees for single-keyed variants of DbHtS, namely PMAC+ and LightMAC+, have only been proven up to $2^{2n/3}$ queries, with no known matching attack. In this work, we revisit the security of single-keyed DbHtS and map the problem to a graph vertex labeling problem where the labels are to be chosen outside some prohibited set (a strict subset of $\{0,1\}^n$). We derive a strong lower bound for the number of such valid vertex labelings, under certain randomness assumptions on the prohibited set. This directly implies security up to $2^{3n/4}$ queries for single-keyed DbHtS. Furthermore, we show that the hash functions in the single-keyed variants of PMAC+ and LightMAC+ satisfy the required conditions. Consequently, the single-keyed PMAC+ and LightMAC+ are shown to be equivalent (up to some constant factors) to their multi-keyed counterparts in terms of security. We conclude with a discussion on the potential applications of our techniques to similar problems in the random permutation model.

3.8 On Boomerang Attacks on Quadratic Feistel Ciphers

Virginie Lallemand (LORIA – Nancy, FR)

Joint work of Xavier Bonnetain, Virginie Lallemand
Main reference Xavier Bonnetain, Virginie Lallemand: "On Boomerang Attacks on Quadratic Feistel Ciphers New results on KATAN and Simon", IACR Trans. Symmetric Cryptol., Vol. 2023(3), pp. 101–145, 2023.
URL https://doi.org/10.46586/TOSC.V2023.I3.101-145

We study the application of the boomerang attack technique to ciphers following a Feistel construction and having a quadratic round function. We prove that many previously published papers give highly inaccurate probability approximations of the distinguishers they use. We next propose a new SMT model that takes into account our findings and we are able to propose a 19-round distinguisher of Simon-32/64 that we convert into the (to the best of our knowledge) first 25-round attack.

3.9 Algebraic Attack on FHE-Friendly Cipher HERA Using Multiple Collisions

Willi Meier (FH Nordwestschweiz – Windisch, CH)

Joint work of Willi Meier, Fukang Liu, Abul Kalam, Santanu Sarkar
Main reference Fukang Liu, Abul Kalam, Santanu Sarkar, Willi Meier: "Algebraic Attack on FHE-Friendly Cipher HERA Using Multiple Collisions", IACR Cryptol. ePrint Arch., p. 1800, 2023.
URL https://eprint.iacr.org/2023/1800

In this work, the first third-party cryptanalysis of the FHE-friendly stream cipher HERA is performed, by showing how to mount new algebraic attacks with multiple collisions in the round keys. Specifically, according to the special way to randomize the round keys in HERA, we peel off the last nonlinear layer by using collisions in the last-round key and a simple property of the power map. In this way, we construct an overdefined system of equations of a much lower degree in the key, and efficiently solve the system via the linearization technique. As a result, for HERA with 192 and 256 bits of security, respectively, we break some parameters under the same assumption made by designers that the algebra constant ω for Gaussian elimination is $\omega = 2$, *i.e.*, Gaussian elimination on an $n \times n$ matrix takes $\mathcal{O}(n^{\omega})$ field operations. If using more conservative choices like $\omega \in 2.8, 3$, our attacks can also successfully reduce the security margins of some variants of HERA to only 1 round.

3.10 Revisiting the Indifferentiability of the Sum of Permutations

Bart Mennink (Radboud University Nijmegen, NL)

Joint work of Aldo Gunsing, Ritam Bhaumik, Ashwin Jha, Bart Mennink, Yaobin Shen
Main reference Aldo Gunsing, Ritam Bhaumik, Ashwin Jha, Bart Mennink, Yaobin Shen: "Revisiting the Indifferentiability of the Sum of Permutations", in Proc. of the Advances in Cryptology – CRYPTO 2023 – 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III, Lecture Notes in Computer Science, Vol. 14083, pp. 628–660, Springer, 2023.
URL https://doi.org/10.1007/978-3-031-38548-3_21

The sum of two n-bit pseudorandom permutations is known to behave like a pseudorandom function with n bits of security. A recent line of research has investigated the security of two public n-bit permutations and its degree of indifferentiability. Mandal et al. (INDOCRYPT 2010) proved $2n/3$-bit security, Mennink and Preneel (ACNS 2015) pointed out a non-trivial flaw in their analysis and re-proved $(2n/3 - \log_2(n))$-bit security. Bhattacharya and Nandi (EUROCRYPT 2018) eventually improved the result to n-bit security. Recently, Gunsing at CRYPTO 2022 already observed that a proof technique used in this line of research only holds for sequential indifferentiability. We revisit the line of research in detail, and observe that the strongest bound of n-bit security has two other serious issues in the reasoning, the first one is actually the same non-trivial flaw that was present in the work of Mandal et al., while the second one discards biases in the randomness influenced by the distinguisher. More concretely, we introduce two attacks that show limited potential of different approaches. We (i) show that the latter issue that discards biases only holds up to $2^{3n/4}$ queries, and (ii) perform a differentiability attack against their simulator in $2^{5n/6}$ queries. On the upside, we revive the result of Mennink and Preneel and show $(2n/3 - \log_2(n))$-bit regular indifferentiability security of the sum of public permutations.

3.11 Revisiting Vector-input MACs

Kazuhiko Minematsu (NEC – Kawasaki, JP)

Joint work of Kazuhiko Minematsu, Isamu Furuya

Rogaway and Shrimpton (RS06) presented the idea of vector-input MAC that accepts a vector consisting of variable-length bit strings. A vector-input MAC could be built on a conventional (bit) string-input MAC, e.g, CMAC, with an injective encoding. RS06 pointed out an efficiency loss in this method and presented a general construction S2V that is more efficient than the encoding-based method. However, despite its potential, their work on vector-input MAC has been largely overlooked for more than 16 years. We revisit RS06's treatment of vector-input MAC and showed that the topic is more subtle than initially considered. We first formally define the problem of vector-input MAC and propose a natural efficiency goal for vector-input MACs as a counterpart of what has been considered for string-input MACs. Since S2V with any string-input MAC mode never achieves this efficiency goal, we propose a new MAC mode, VecMAC, that achieves this goal for any vector space. VecMAC is a variant of the popular PMAC. However, its use of tweaks is more involved and conceptually different from PMAC. We also provide preliminary implementation results.

3.12 On INT-RUP security analysis of GCM

Akiko Inoue (NEC – Kawasaki, JP), Tetsu Iwata (Nagoya University, JP), and Kazuhiko Minematsu (NEC – Kawasaki, JP)

Integrity under the release of unverified plaintext (INT-RUP) is the security notion for authenticated encryption with associated data (AEAD) schemes. When an AEAD scheme is INT-RUP secure, it guarantees authenticity even when the decryption function inevitably or erroneously outputs the decrypted message without verification. INT-RUP security against existing AEAD schemes has been extensively studied, such as ChaCha20-Poly1305, SAEF, and TinyJambu. Many schemes have been designed with a provable security claim on INT-RUP as one of the main security features, such as Minalpher, CPFB, LOTUS/LOCUS, and Oribatida. However, surprisingly, there is no INT-RUP analysis on GCM, which is one of the most widely deployed AEAD schemes. We prove that GCM has INT-RUP security with almost the same security level as that of the classical authenticity notion by showing that INT-RUP security of GCM is reduced to the variant of the unforgeability of GMAC inside GCM. Our future work is to analyze INT-RUP security on CCM.

3.13 Indifferentiability of 6-round Feistel

Mridul Nandi (Indian Statistical Institute - Kolkata, IN)

Joint work of Mridul Nandi, Ritam Bhaumik, Abishanka Saha, Paul Sayantan

The design and analysis of cryptographic systems often rely on proving the security of various primitives and constructions. One prominent framework for assessing the security of cryptographic constructions is indifferentiability introduced by Maurer et al. in [1], which provides a rigorous method to demonstrate the equivalence of constructed systems with idealized versions, even in the presence of adversaries with access to underlying primitives. This paper explores the indifferentiability of Feistel networks introduced by Horst Feistel as a design component of Lucifer [2], a widely used paradigm for constructing cryptographic primitives from simpler components known as round functions. Feistel networks offer a structured approach to building cryptographic systems, particularly permutations, by iteratively applying round functions to input data. Understanding the indifferentiability of Feistel networks is crucial for establishing the security of numerous cryptographic constructions.

A simulator to prove indifferentiability of six-round Feistel was proposed in [3] by Coron et. al., along with an attack on five-round Feistel that works against any simulator. This simulator was later shown to be incapable of demonstrating indifferentiability of six-round Feistel by Holenstein et. al. in [4]. An early version of [4] proposed a simulator for the 18-round construction that achieved indifferentiability, and in a later revision this was changed to a simulator for the 14-round version. Next, two concurrent works by Dai and Steinberger [5] and Dachman-Soled et al. [6] both proved indifferentiability of the 10-round Fesitel network, the former by repairing the flawed 10-round simulator from [7], and the latter by modifying the 14-round simulator from [4]. Finally, in what has so far been the latest work in this series, Dai and Steinberger [8] established the indifferentiability of the 8-round Fesitel construction by optimising their simulator from [5]. Thus, while later proofs have been found for the indifferentiability of Feistel networks with eight or more rounds, that of six-round Feistel still remains an open question. The highlight of this paper is the presentation of a novel proof demonstrating the indifferentiability of the six-round Feistel network. This proof is accompanied by the design of an advanced simulator that preemptively handles construction queries from adversaries, ensuring the security of the constructed system.

References

1 U. Maurer, R. Renner, and C. Holenstein Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology. Theory of Cryptography Conference – TCC 2004, Lecture Notes in Computer Science, Springer-Verlag, vol. 2951, pp. 21–39, Feb 2004.

2 H. Feistel Cryptography and Computer Privacy cientific American 228, no. 5 (1973): 15–23.

3 J. Coron, J. Patarin, Y. Seurin The Random Oracle Model and the Ideal Cipher Model Are Equivalent Advances in Cryptology – CRYPTO 2008. CRYPTO 2008. Lecture Notes in Computer Science, vol 5157. Springer, Berlin, Heidelberg.

4 T. Holenstein, R. Künzler, S. Tessaro Equivalence of the Random Oracle Model and the Ideal Cipher Model, Revisited. CoRR abs/1011.1264 (2010)

5 Y. Dai, J. Steinberger Indifferentiability of 10-Round Feistel Networks Eprint Paper 2015/874

6 D. Dachman-Soled, J. Katz, A. Thiruvengadam 10-Round Feistel is Indifferentiable from an Ideal Cipher EUROCRYPT (2) 2016: 649-678

7 Y. Seurin Primitives et protocoles cryptographiques à sécurité prouvée Université de Versailles Saint-Quentin-en-Yvelines

8 Y. Dai, J. Steinberger Indifferentiability of 8-Round Feistel Networks. CRYPTO (1) 2016: 95-120

3.14 The Algebraic Freelunch: Efficient Gröbner Basis Attacks Against Arithmetization-Oriented Primitives

Léo Perrin (INRIA – Paris, FR)

Joint work of Augustin Bariant, Aurélien Boeuf, Axel Lemoine, Irati Manterola Ayala, Morten Øygarden, Léo Perrin, Håvard Raddum
Main reference Augustin Bariant, Aurélien Boeuf, Axel Lemoine, Irati Manterola Ayala, Morten Øygarden, Léo Perrin, Håvard Raddum: "The Algebraic Freelunch Efficient Gröbner Basis Attacks Against Arithmetization-Oriented Primitives", IACR Cryptol. ePrint Arch., p. 347, 2024.
URL https://eprint.iacr.org/2024/347

In this talk, I presented a new type of algebraic attack that applies to many recent arithmetization-oriented families of permutations, such as those used in Griffin [1], Anemoi [2], and ArionHash [3], whose security relies on the hardness of the constrained-input constrained-output (CICO) problem. We introduce the FreeLunch approach: the monomial ordering is chosen so that the natural polynomial system encoding the CICO problem already is a Gröbner basis. In addition, we present a new dedicated resolution algorithm for FreeLunch systems of complexity lower than applicable state-of-the-art FGLM algorithms. We show that the FreeLunch approach challenges the security of fullround instances of Anemoi, Arion and Griffin. We confirm these theoretical results with experimental results on those three permutations. In particular, using the FreeLunch attack combined with a new technique to bypass 3 rounds of Griffin, we recover a CICO solution for 7 out of 10 rounds of Griffin in less than four hours on one core of AMD EPYC 7352 (2.3GHz).

References

1 Lorenzo Grassi, Yonglin Hao, Christian Rechberger, Markus Schofnegger, Roman Walch, Qingju Wang. *Horst meets fluid-SPN: Griffin for zero-knowledge applications.* Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2023.

2 Clémence Bouvier, Pierre Briaud, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov, Danny Willems. *New design techniques for efficient arithmetization-oriented hash functions: anemoi permutations and jive compression mode.* Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2023.

3 Arnab Roy, Matthias Johann Steiner, and Stefano Trevisani. *Arion: Arithmetization-oriented permutation and hashing from generalized triangular dynamical systems.* arXiv preprint arXiv:2303.04639 (2023).

3.15 The t-wise Independence of SPNs

Stefano Tessaro (University of Washington – Seattle, US)

Joint work of Tianren Liu, Angelos Pelecanos, Stefano Tessaro, Vinod Vaikuntanathan
Main reference Tianren Liu, Angelos Pelecanos, Stefano Tessaro, Vinod Vaikuntanathan: "Layout Graphs, Random Walks and the t-Wise Independence of SPN Block Ciphers", in Proc. of the Advances in Cryptology – CRYPTO 2023 – 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III, Lecture Notes in Computer Science, Vol. 14083, pp. 694–726, Springer, 2023.
URL https://doi.org/10.1007/978-3-031-38548-3_23

This talk overviews an ongoing research agenda aimed at proving security of block ciphers against limited classes of attacks. We focus on proving that Substitution Permutation Networks (SPNs), when instantiated with concrete S-boxes (such as the AES S-box), give us t-wise independent permutations. This is a weak property (compared to being a full-fledged pseudorandom permutation), but it implies in particular security against classical families of statistical attacks such as linear and differential cryptanalysis. Our approach is in contrast with prior works aiming at full proofs of security for idealized versions of block ciphers.

4 Working groups

4.1 First results on the multivariate cryptanalysis of Poseidon

Lorenzo Grassi (Ruhr-Universität Bochum, DE), Antoine Joux (CISPA – Saarbrücken, DE), Patrick Neumann (Ruhr-Universität Bochum, DE), Léo Perrin (INRIA – Paris, FR), Christian Rechberger (TU Graz, AT), Ferdinand Sibleyras (NTT – Tokyo, JP), Aleksei Udovenko (University of Luxembourg, LU), and Qingju Wang (University of Luxembourg, LU)

The aim of this working group was to identify ways to improve algebraic attacks targeting arithmetization-oriented primitives (AOP) using "classical" tricks, i.e. insights gained not from a study of the system of equations, but from a careful analysis of the round function using well known approaches.

To this end, we first agreed to focus our efforts on Poseidon [1], one of the oldest AOPs. It is indeed an interesting target: it has a simple description, there is some public analysis of it, and yet its security against multi-variate approaches is ill-understood. In fact, at the time of the seminar, such analyses were (for Poseidon) essentially absent. Such a setting is made all the more relevant by recent advances in the zero-knowledge realm: the field sizes considered tend to be smaller nowadays, and the univariate approaches that were arguably the main threat at the time of the design of Poseidon have somewhat lost their relevance.

Due to the structure of the inner rounds of Poseidon, it is possible to bypass some of them when building a system of equations. In fact, the more words there are in the internal state, the more rounds we can by pass. Furthermore, since the round function of Poseidon has a low degree, we do not need to introduce an equation in each round. Thus, we believe that a CICO attack could work as follows.

1. introduce variables at the end of the first full rounds (so, after round 4);
2. write the equations encoding that the first input blocks are set to 0, which involves inverting the first rounds (while the round function is of low degree, its inverse is of very high degree, which is why we cover much fewer rounds backwards);
3. write the equations encoding that the first output blocks are set to 0, using the fact that the middle variables can be chosen so as to correspond to a subspace that does not activate the unique S-box in the middle rounds for a few rounds.
4. solve the equations using off-the-shelf tools.

It remains to precisely quantify the number of rounds that can be attacked in this fashion. We expect it to be lower than for a univariate attack, but, again, such attacks are not really relevant when the field size is smaller.

We also plan to make a detailed comparison between the case of Poseidon and that of Neptune, a very similar AOP that crucially differs in the structure of its outer rounds: instead of relying on low degree monomials (and thus, on functions with a very degree inverse), it relies on low degree functions that have the same degree in both directions. This should allow us to attack more rounds in this case, an insight we would consider valuable in itself.

References

1 Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, Markus Schofnegger: *Poseidon: A new hash function for Zero-Knowledge proof systems.* 30th USENIX Security Symposium (USENIX Security 21). 2021.

4.2 Cryptanalysis of TEA3

Subhadeep Banik (University of Lugano, CH), Christof Beierle (Ruhr-Universität Bochum, DE), Anne Canteaut (INRIA – Paris, FR), Patrick Felke (Hochschule Emden/Leer, DE), Nils Gregor Leander (Ruhr-Universität Bochum, DE), Gaëtan Leurent (INRIA – Paris, FR), Yann Rotella (University of Versailles, FR), Sondre Rønjom (University of Bergen, NO), and Siwei Sun (University of Chinese Academy of Sciences, CN)

The proprietary TETRA Encryption standards, TEA1, TEA2, and TEA3, distributed by ETSI except for TEA2 (see [1]), were recently reverse-engineered in [2]. TEA1, TEA2, TEA3 are stream ciphers based on byte-oriented non-linear feedback shift registers (NFSRs). While TEA1 is an insecure cipher (the 80-bit key is compressed into a 4-byte register, effectively reducing its key length to 32 bits), the security level of the other algorithms TEA2 and TEA3 is less clear.

Although there is no obvious attack, the choices of components used in TEA3 (in contrast to TEA2) are questionable from a designer's point of view. In particular, the key register of TEA3 employs an 8-bit Sbox in its feedback, denoted S, that is *not* a permutation. Instead, its distance to a permutation is only one bit in the sense that flipping a single bit in its lookup table would cause S to be bijective. Furthermore, the 10-byte key register can be decomposed into the cascade connection of a 5-byte NFSR into a 5-byte LFSR with feedback polynomial $(X^5 + SB3X^2 + 1) \cdot (X^5 + 1)$. Our experiments (started as joint work with Jens Alich, Christof Beierle, Patrick Felke, Gregor Leander, and Lukas Stennes) reveal that there are initial states of the 10-byte key register that have a period of only 10 bytes and that the maximal period is only about $10 \cdot 2^{40}$ bytes. The TEA3 key stream generator is depicted in [2, Figure 8]. The goal of this research group was to study the following questions:

- Can we exploit these properties to conduct an attack on TEA3?
- How were the components used in TEA3 designed?

During the research meetings at the Dagstuhl Seminar, the working group made the following progress on those questions:

- Using the existing theory on NFSRs from [3] and the structure of the cascade connection of the key register, we were able to derive necessary conditions on the period lengths of the key register. We further developed ideas to fully understand the cycle structure.
- The 16-to-8 bit functions $F31$ and $F32$ used in the state register of TEA3 are balanced vectorial Boolean functions built from 8 parallel 4-bit Boolean functions with overlapping inputs. A priori, it is not clear why such a construction leads to a balanced function. We identified a possible underlying construction method of $F31$ and $F32$.
- We identified some generic time-memory tradeoff attacks on the key stream generator with a complexity slightly below 2^{80} (i.e., the complexity of a brute-force attack)

References

1 ETSI. Custodian, security algorithms. `https://www.etsi.org/security-algorithms-and-codes/security-algorithms`, 2023. [Online; accessed 31-January-2024].

2 C. Meijer, W. Bokslag, and J. Wetzels. All cops are broadcasting: TETRA under scrutiny. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 7463–7479, 2023.

3 J. Mykkeltveit, M.-K. Siu, and P. Tong. On the cycle structure of some nonlinear shift register sequences. *Information and control*, 43(2):202–215, 1979.

4.3 Exploitation of the Wrong Key Randomization Hypothesis Non-conformity in Key Recovery Attacks

Zhenzhen Bao (Tsinghua University – Beijing, CN) and Nils Gregor Leander (Ruhr-Universität Bochum, DE)

Main reference Aron Gohr: "Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning", in Proc. of the Advances in Cryptology – CRYPTO 2019 – 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II, Lecture Notes in Computer Science, Vol. 11693, pp. 150–179, Springer, 2019.
URL https://doi.org/10.1007/978-3-030-26951-7_6

At CRYPTO 2019, Gohr introduced a novel key recovery strategy for Speck32/64, termed the BayesianKeySearch algorithm. This approach challenges the conventional Wrong Key Randomization Hypothesis (WKRH), particularly in scenarios where the attack on Speck undergoes only a single round of trial decryption. The BayesianKeySearch algorithm iteratively refines key guesses by generating new round-key candidates based on previous guesses, thereby progressively enhancing the quality of the guessed key. Notably, this method requires a limited number of one-round trial decryptions, reducing time complexity.

Despite its practical implications, the algorithm lacks a comprehensive theoretical framework to quantify the impact of various parameters on attack complexity and success rate. This discussion group aimed to bridge this gap by establishing a theoretical model to evaluate its complexity better and broadening the application to conventional key recovery attacks.

The discussion centered on two primary aspects: examining how the wrong key-right key distance influences the statistics in traditional differential and linear attacks and developing methods to leverage these non-random influences. Initial outcomes of this discussion include a proposed formula hypothesizing the relationship between the Hamming weight of the wrong key-right key distance and the probability of returning to the same output difference, a drawn parallel between this probability's evaluation and the BCT's computation (difference-boomerang connective probability), and a proposed time-data tradeoff strategy in differential key-recovery attacks.

The group plans to persist in the investigation of this topic post-seminar.

4.4 Cryptanalysis of SCARF

Christina Boura (University of Versailles, FR), Zahra Ahmadian (Shahid Beheshti University – Tehran, IR), Yanis Belkheyar (Radboud University Nijmegen, NL), Christoph Dobraunig (Intel – Villach, AT), Henri Gilbert (ANSSI – Paris, FR), Shahram Rasoolzadeh (Radboud University Nijmegen, NL), Dhiman Saha (Indian Institute of Technology Bhilai – Durg, IN), Tyge Tiessen (Technical University of Denmark – Lyngby, DK), and Yosuke Todo (NTT – Tokyo, JP)

SCARF if a tweakable BC for cache randomization, proposed at Usenix Security 2023.

It's block length is 10 bits only, it absorbs a tweak of 48 bits and it offers 80-bit security (but a 240-bit key is used). The security claim is peculiar as an attacker cannot directly query the TBC. Instead, the attacker can query collision or composition oracles. The query complexity is up to $2^4 0$.

In this working group we analyzed the security of SCARF by investigating different cryptanalysis techniques. We thought of several approaches:

- Exploit the fact that 0 is a fixed point for some operations of the round function.
- Analyse the algebraic degree growth and exploit the algebraic normal form of the Sbox.
- Polytopic cryptanalysis.
- Multiple-tweak differential attack.

While all the approaches seem promising, the multiple-tweak differential attack seems to be particular interesting for this cipher and we hope to be able to break (7+7)/(8+8) rounds of this cipher with this approach.

References

1 Canale F., Güneysu T., Leander G., Thoma J. P., Todo Y., Ueno R. *A Low-Latency Block Cipher for Secure Cache-Randomization*. USENIX Security Symposium 2023: 1937-1954

4.5 Differential cryptanalysis and more

Patrick Derbez (University of Rennes, FR), Orr Dunkelman (University of Haifa, IL), Maria Eichlseder (TU Graz, AT), Ryoma Ito (NICT – Tokyo, JP), Virginie Lallemand (LORIA – Nancy, FR), and María Naya-Plasencia (INRIA – Paris, FR)

Our research group was composed of Maria Eichlseder, Orr Dunkelman, María Naya-Plasencia, Virginie Lallemand, Ryoma Ito and Patrick Derbez. The main topic of our group was to propose a new modelization of impossible differential attacks, more accurate than a classic "0/1/?" model but faster than exhausting all differential characteristics. Our idea is to track as well the equalities between internal state variables to propagate more information and extend the impossible cases. We also investigated several other topics including extension of differential-mitm attacks, impossible differential-linear attacks as well as an attack against a generic cipher relying on the nice algorithmic problem of finding the closest pair of vectors.

4.6 Key Control Security Group

Tetsu Iwata (Nagoya University, JP), Ritam Bhaumik (EPFL – Lausanne, CH), Avijit Dutta (TCG CREST – Kolkata, IN), Akiko Inoue (NEC – Kawasaki, JP), Ashwin Jha (Ruhr-Universität Bochum, DE), Kazuhiko Minematsu (NEC – Kawasaki, JP), Mridul Nandi (Indian Statistical Institute – Kolkata, IN), Yu Sasaki (NTT – Tokyo, JP), Meltem Sonmez Turan (NIST – Gaithersburg, US), Stefano Tessaro (University of Washington – Seattle, US), and Aishwarya Thiruvengadam (Indian Institute of Techology Madras, IN)

NIST SP 800-108r1 [1] specifies Key Derivation Functions (KDFs) based on PseudoRandom Functions (PRFs). It specifies a KDF based on KMAC, and it also specifies KDFs in counter mode, feedback mode, and double-pipeline mode, which are combined with HMAC or CMAC as the PRF.

The document was revised in August 2022, and a discussion on the key control security was added, showing a security issue in KDFs with CMAC. The goal of this research group is to formalize a cryptographic definition of the key control security, and analyze the security of KDFs in the NIST document from the provable security and cryptanalytic perspectives.

The group identified a formal security definition, and drafted a security proof of a KDF based on KMAC. We also analyzed KDFs based on CMAC from a cryptanalytic view point. In particular, we focused on the strengthened version, which is a variant of the KDFs based on CMAC to mitigate the issue in their key control security.

References

1 Lily Chen. Recommendation for Key Derivation Using Pseudorandom Functions. NIST Special Publication, NIST SP 800-108r1, August 2022, https://doi.org/10.6028/NIST.SP.800-108r1

4.7 Security of sponge combiners

Charlotte Lefevre (Radboud University Nijmegen, NL), Rachelle Heim Boissier (University of Versailles, FR), Bart Mennink (Radboud University Nijmegen, NL), and Bart Preneel (KU Leuven, BE)

The aim of this research group was to investigate the security of sponge-based combiners and variants from both cryptanalytical and provable security perspectives. The motivation behind this investigation stemmed from the observation that while finding inner collisions in a sponge generically requires $2^{c/2}$ permutation evaluations, the associated attack does not straightforwardly generalize with combiners due to the repeated absorption of the same message block. On the cryptanalytical aspect, we examined various sponge-based combiners and derivatives, namely the concatenation combiner, XOR combiner, and two hash-twice-like constructions. We focused on collision, second preimage, and preimage attacks, with Joux's attack [1] serving as the main tool. Notably, except for collision of the hash-twice construction with identical permutations (which costs $2^{c/2}$ evaluations), a term in $2^{b/2}$ emerged consistently in our analysis. On the provable security aspect, the discussions provided valuable insights that could be helpful to improve the security of these constructions, ideally up to min(c, b/2) bits. We plan to continue working on these two aspects after the seminar.

References

1 A. Joux. Multicollisions in Iterated Hash Functions. *Advances in Cryptology – Crypto 2004,*, Volume 3152 of Lecture Notes in Computer Science. Springer-Verlag, 2004.

Participants

- Zahra Ahmadian
Shahid Beheshti University – Tehran, IR
- Subhadeep Banik
University of Lugano, CH
- Zhenzhen Bao
Tsinghua University – Beijing, CN
- Christof Beierle
Ruhr-Universität Bochum, DE
- Yanis Belkheyar
Radboud University Nijmegen, NL
- Ritam Bhaumik
EPFL – Lausanne, CH
- Christina Boura
University of Versailles, FR
- Anne Canteaut
INRIA – Paris, FR
- Patrick Derbez
University of Rennes, FR
- Christoph Dobraunig
Intel – Villach, AT
- Orr Dunkelman
University of Haifa, IL
- Avijit Dutta
TCG CREST – Kolkata, IN
- Maria Eichlseder
TU Graz, AT
- Patrick Felke
Hochschule Emden/Leer, DE
- Henri Gilbert
ANSSI – Paris, FR
- Lorenzo Grassi
Ruhr-Universität Bochum, DE
- Rachelle Heim Boissier
University of Versailles, FR
- Akiko Inoue
NEC – Kawasaki, JP
- Ryoma Ito
NICT – Tokyo, JP
- Tetsu Iwata
Nagoya University, JP
- Ashwin Jha
Ruhr-Universität Bochum, DE
- Antoine Joux
CISPA – Saarbrücken, DE
- Virginie Lallemand
LORIA – Nancy, FR
- Nils Gregor Leander
Ruhr-Universität Bochum, DE
- Charlotte Lefevre
Radboud University Nijmegen, NL
- Gaëtan Leurent
INRIA – Paris, FR
- Willi Meier
FH Nordwestschweiz – Windisch, CH
- Bart Mennink
Radboud University Nijmegen, NL
- Kazuhiko Minematsu
NEC – Kawasaki, JP
- Mridul Nandi
Indian Statistical Institute – Kolkata, IN
- Maria Naya-Plasencia
INRIA – Paris, FR
- Patrick Neumann
Ruhr-Universität Bochum, DE
- Léo Perrin
INRIA – Paris, FR
- Bart Preneel
KU Leuven, BE
- Shahram Rasoolzadeh
Radboud University Nijmegen, NL
- Christian Rechberger
TU Graz, AT
- Yann Rotella
University of Versailles, FR
- Sondre Rønjom
University of Bergen, NO
- Dhiman Saha
Indian Institute of Technology Bhilai – Durg, IN
- Yu Sasaki
NTT – Tokyo, JP
- Ferdinand Sibleyras
NTT – Tokyo, JP
- Meltem Sonmez Turan
NIST – Gaithersburg, US
- Siwei Sun
University of Chinese Academy of Sciences, CN
- Stefano Tessaro
University of Washington – Seattle, US
- Aishwarya Thiruvengadam
Indian Institute of Techology Madras, IN
- Tyge Tiessen
Technical University of Denmark – Lyngby, DK
- Yosuke Todo
NTT – Tokyo, JP
- Aleksei Udovenko
University of Luxembourg, LU
- Qingju Wang
University of Luxembourg, LU