

# Symmetric Cryptography

Edited by

Joan Daemen<sup>1</sup>, Tetsu Iwata<sup>2</sup>, Nils Gregor Leander<sup>3</sup>, and  
Kaisa Nyberg<sup>4</sup>

- 1 Radboud University Nijmegen, NL, and STMicroelectronics – Diegem, BE,  
joan@cs.ru.nl
- 2 Nagoya University, JP, iwata@cse.nagoya-u.ac.jp
- 3 Ruhr-Universität Bochum, DE, gregor.leander@rub.de
- 4 Aalto University, FI, kaisa.nyberg@aalto.fi

---

## Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 18021 “Symmetric Cryptography”, which was held on January 7–12, 2018 in Schloss Dagstuhl – Leibniz Center for Informatics. The seminar was the sixth in a series of Dagstuhl seminars on “Symmetric Cryptography”, previously held in 2007, 2009, 2012, 2014, and 2016.

During the seminar, many of the participants presented their current research in the design, analysis, and application of symmetric cryptographic algorithms, including ongoing work and open problems. This report documents the abstracts or extended abstracts of the talks presented during the seminar, as well as summaries of the discussion sessions.

**Seminar** January 7–12, 2018 – <https://www.dagstuhl.de/18021>

**2012 ACM Subject Classification** Security and privacy → Cryptography → Cryptanalysis and other attacks, Security and privacy → Cryptography → Symmetric cryptography and hash functions

**Keywords and phrases** symmetric cryptography, cryptanalysis, authenticated encryption, cryptography for IoT, mass surveillance

**Digital Object Identifier** 10.4230/DagRep.8.1.1

**Edited in cooperation with** Maria Eichlseder

## 1 Executive Summary

*Nils Gregor Leander (Ruhr-Universität Bochum, DE)*

*Joan Daemen (Radboud University Nijmegen, NL, and STMicroelectronics – Diegem, BE)*

*Tetsu Iwata (Nagoya University, JP)*

*Kaisa Nyberg (Aalto University, FI)*

**License** © Creative Commons BY 3.0 Unported license  
© Nils Gregor Leander, Joan Daemen, Tetsu Iwata, and Kaisa Nyberg

IT Security plays an increasingly vital role in everyday life and business. When talking on a mobile phone, when withdrawing money from an ATM or when buying goods over the internet, security plays a crucial role in both protecting the user and in maintaining public confidence in the system. Especially after the disclosure of the NSA’s world-spanning spying activities and in the context of the Internet of Things, IT Security and privacy protection is a vital topic of the 21st century. In the Internet of Things (IoT) era, everything will be connected. Intel estimates that 200 billion objects will be connected by 2020. The objects



Except where otherwise noted, content of this report is licensed under a Creative Commons BY 3.0 Unported license

Symmetric Cryptography, *Dagstuhl Reports*, Vol. 8, Issue 01, pp. 1–32

Editors: Joan Daemen, Tetsu Iwata, Nils Gregor Leander, and Kaisa Nyberg



Dagstuhl Reports

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

include for instance smart devices for healthcare, industrial control systems, automotive, and smart homes. Virtually all modern security solutions rely on cryptography.

Symmetric cryptography deals with the case that both the sender and the receiver of a message are using the same key. This differentiates symmetric cryptography from its asymmetric counterpart, where senders or verifiers use a “public key” and receivers or signers use a corresponding but different “private key”. As asymmetric primitives are typically orders of magnitude less efficient than symmetric cryptographic schemes, symmetric cryptosystems remain the main workhorses of cryptography and highly relevant not only for academia, but also for industrial research and applications. While great progress has been made in designing and analyzing ciphers, fundamental aspects of these ciphers are still not fully understood. Moreover, as we have learned from the Snowden revelations, cryptography in general and symmetric cryptography in particular faces new fascinating challenges.

### Current Topics and Challenges

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

**Cryptography for the IoT.** Motivated by the upcoming IoT, one of the strong research trends in symmetric cryptography is about lightweight cryptography. Here, lightweight cryptography refers to strong cryptography, that can be executed on heavily resource constrained devices. Those efforts resulted in a wide variety of block cipher designs suitable for IoT applications. For instance, PRESENT designed in 2007 is one of the early designs with strong implementation advantages on hardware, and there have been other innovative follow-up block cipher designs. Some of them are standardized as the international standard, and used in thousands of devices in our daily lives. However, a block cipher is not the solution to all cryptographic purposes. For instance, to encrypt a certain amount of data, the block cipher has to be integrated into a suitable mode of operation. In most practical use cases, confidentiality is not the only concern, as many scenarios require data authenticity as well. Here a message authentication code (MAC) can be used to ensure authenticity. Authenticated encryption (AE) is used for protecting both confidentiality and authenticity.

The first MAC, called Chaskey, that specifically targets applications for lightweight cryptography was proposed only recently in 2014. The CAESAR project, an international competition for AE initiated at Dagstuhl, attracted several submissions that were designed for the purposes for lightweight cryptography. There is also a recent attempt to design a lightweight tweakable block cipher, an advanced primitive of a block cipher that allows more flexible usage, which can be efficiently integrated into highly secure encryption and/or authentication mechanisms. However, this research just started and many primitives and modes of operations suitable for lightweight crypto remain to be explored.

**Statistical Attacks.** Statistical attacks have been deployed widely and providing strong resistance against them has resulted in several important design criteria for contemporary symmetric primitives. The first type of statistical attacks that is applicable to a large set of block ciphers is differential cryptanalysis, introduced by Biham and Shamir. Since its invention in the early nineties several variants, tweaks and generalizations have been proposed and applied to many block ciphers. The second generally applicable attack on block ciphers is Matsui’s linear cryptanalysis. Similarly to differential attacks, since its introduction, many extensions and improvements have been made. One main issue that has become apparent only recently is the accuracy of the underlying statistical models that researchers are using. Typically, those models are presented under some simplifying assumptions, whose validity remains an open question. It is an important challenge to settle these unsatisfactory

simplifications. This becomes even more important when the attacks are hard or impossible to verify experimentally due to the large computational costs involved. Moreover, to allow comparison between different attacks the researchers must agree on common attack models and parameters that measure the performance of the attack.

**Symmetric Cryptography and Real-World Needs.** The symmetric cryptography community has many very talented people and the state of the area has moved from it infancy in the seventies to a mature field today. However, we should ensure that the world's population does benefit of this progress. In particular, the Snowden leaks have painfully illustrated that citizen privacy and anonymity is next to non-existent nowadays. Secret services and IT corporations massively spy on people's communication and data storage for motives such as profit and surveillance. They don't seem to be hindered significantly in this at all by the pervasive deployment of cryptography (TLS, GSM, WPA, etc.). Cynically, monopolistic corporations like Google use encryption to protect the data of their users from prying eyes of other players such as network providers. It appears that much of the cryptography deployed today is there to protect the powers that be rather than protect human rights. With the roll-out of smart grid and internet-of-things surveillance will become quasi universal with all imaginable devices reporting on our behavior to big corporations. This situation has been addressed in several invited talks by Bart Preneel and Adi Shamir and they rightfully say that we as a cryptographic community should attempt to improve this. Along the same lines, Phil Rogaway gave a highly acclaimed invited talk at Asiacrypt 2015 on the moral aspects on cryptographic research. He invites us to do some introspection and ask the question: are we doing the right thing?

We believe these questions are important also for the symmetric crypto community. While the problem is certainly not restricted to symmetric cryptography and probably cannot be solved by symmetric cryptography alone, we should consider it our moral duty to improve the situation.

### Seminar Program

The seminar program consists of presentations about the above topics, and relevant areas of symmetric cryptography, including new cryptanalytic techniques and new designs. Furthermore, there were discussion sessions. In "Discussion on CAESAR with focus on robustness", we discussed about the meaning and relevance of the term robustness in general and for the CAESAR competition in particular. In "Discussion on Mass Surveillance", a number of questions related to the real-world relevance of the symmetric crypto community and its research were discussed. For both discussions we provide summery of the questions and results.

## 2 Table of Contents

### Executive Summary

<i>Nils Gregor Leander, Joan Daemen, Tetsu Iwata, and Kaisa Nyberg . . . . .</i>	1
----------------------------------------------------------------------------------	---

### Overview of Talks


TMD tradeoffs on small-state stream ciphers <i>Willi Meier . . . . .</i>	6
Towards Low Energy Stream Ciphers <i>Vasily Mikhalev . . . . .</i>	6
An LFSR-based Proof of Work <i>Frederik Armknecht . . . . .</i>	7
Rasta: Designing a cipher with low ANDdepth and few ANDs per bit <i>Christoph Dobraunig . . . . .</i>	7
Leakage-Resilient Authenticated Encryption <i>Stefan Lucks . . . . .</i>	8
Key Prediction Security of Keyed Sponges <i>Bart Mennink . . . . .</i>	8
Tree-searching for trail bounds <i>Gilles Van Assche . . . . .</i>	8
Merkle Tree is not Optimal <i>Dmitry Khovratovich . . . . .</i>	9
Fast Correlation Attack Revisited <i>Yosuke Todo . . . . .</i>	9
Towards Quantitative Analysis of Cyber Security <i>Adi Shamir . . . . .</i>	9
Security of Caesar Candidates against (beyond) Birthday and/or Nonce-Reusing Attacks <i>Damian Vizár . . . . .</i>	10
Key-Recovery Attacks on Full Kravatte <i>Henri Gilbert . . . . .</i>	10
Clustering Related-Tweak Characteristics <i>Maria Eichlseder . . . . .</i>	11
Conditional Linear Cryptanalysis <i>Stav Perle and Eli Biham . . . . .</i>	11
Linear Cryptanalysis Using Low-Bias Approximations <i>Tomer Ashur . . . . .</i>	12
Multidimensional, Affine and Conditional Linear Cryptanalysis <i>Kaisa Nyberg . . . . .</i>	12
The Chi-Squared Method <i>Stefano Tessaro . . . . .</i>	17
Some applications of the chi square method <i>Mridul Nandi . . . . .</i>	17

Beyond-Birthday-Bound Secure MACs <i>Yannick Seurin</i> . . . . .	18
Recent Advancements in Sponge-Based MACs <i>Kan Yasuda</i> . . . . .	18
The collision-resistance of keyed hashing <i>Joan Daemen</i> . . . . .	18
Challenges and Opportunities for the Standardization of Threshold Cryptography <i>Nicky Mouha</i> . . . . .	20
Tools on Cryptanalysis <i>Stefan Kölbl</i> . . . . .	20
A survey of recent results on AES permutations <i>Christian Rechberger</i> . . . . .	20
Cryptanalysis of Reduced Round AES, Revisited <i>Orr Dunkelman</i> . . . . .	21
Integral Attacks on AES <i>Meiqin Wang</i> . . . . .	21
On Sboxes sharing the same DDT <i>Anne Canteaut</i> . . . . .	22
Boomerang Connectivity Table (BCT) for Boomerang Attacks <i>Yu Sasaki</i> . . . . .	22
QCCA on Feistel <i>Tetsu Iwata</i> . . . . .	23
Some Feistel structures with low degree round functions <i>Arnab Roy</i> . . . . .	23
Generalized Feistel Networks with Optimal Diffusion <i>Léo Paul Perrin</i> . . . . .	24
An Improved Affine Equivalence Algorithm . . . . .	24
Invariant Attacks and (Non-)linear Approximations . . . . .	25
Recent results on reduced versions of Ketje . . . . .	25
On the security of LINE messaging application . . . . .	26
Multiplication Operated Encryption with Trojan Resilience . . . . .	27
Instantiating the Whitened Swap-Or-Not Construction . . . . .	27
Better proofs for rekeying . . . . .	28
<b>Panel discussions</b>	
Discussion on Mass Surveillance and the Real-World Impact of the Symmetric- Crypto Research Community . . . . .	28
Discussion on Robustness of CAESAR Candidates . . . . .	29
<b>Participants</b> . . . . .	32

### 3 Overview of Talks

#### 3.1 TMD tradeoffs on small-state stream ciphers

*Willi Meier (FH Nordwestschweiz – Windisch, CH)*

**License**  Creative Commons BY 3.0 Unported license  
© Willi Meier

Design and analysis of stream ciphers whose state is smaller than double the key size (small-state stream ciphers) is not fully exploited yet. For small-state stream ciphers that continuously use the non-volatile key in the state update, a TMD-TO distinguisher is described. A new mode for stream ciphers that continuously involve the IV (instead of the key) is proposed. Arguments are provided that this mode can resist generic TMD-TOs.

#### 3.2 Towards Low Energy Stream Ciphers

*Vasily Mikhalev (Universität Mannheim, DE)*

**License**  Creative Commons BY 3.0 Unported license  
© Vasily Mikhalev

**Joint work of** Subhadeep Banik, Frederik Armknecht, Takanori Isobe, Willi Meier, Andrey Bogdanov, Yuhei Watanabe, Francesco Regazzoni

Energy optimization is an important design aspect of lightweight cryptography. Since low energy ciphers drain less battery, they are invaluable components of devices that operate on a tight energy budget such as handheld devices or RFID tags. At Asiacrypt 2015, Banik et. al. presented the block cipher family Midori which was designed to optimize the energy consumed per encryption and which reduces the energy consumption by more than 30 % compared to previous block ciphers. However, if one has to encrypt/decrypt longer streams of data, i.e. for bulk data encryption/decryption, it is expected that a stream cipher should perform even better than block ciphers in terms of energy required to encrypt.

In this work, we address the question of designing low energy ciphers. To this end, we first analyze for common stream cipher design components their impact on the energy consumption. Based on this, we give arguments why indeed stream ciphers allow for encrypting long data streams with less energy than block ciphers and validate our findings by implementations. Afterwards, we use the analysis results to identify energy minimizing design principles for stream ciphers.

### 3.3 An LFSR-based Proof of Work

*Frederik Armknecht (Universität Mannheim, DE)*

**License** © Creative Commons BY 3.0 Unported license  
© Frederik Armknecht

**Joint work of** Frederik Armknecht, Ludovic Barman, Jens-Matthias Bohli, Ghassan O. Karame

**Main reference** Frederik Armknecht, Ludovic Barman, Jens-Matthias Bohli, Ghassan O. Karame: “Mirror: Enabling Proofs of Data Replication and Retrieval in the Cloud”, in Proc. of the 25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016., pp. 1051–1068, USENIX Association, 2016.

**URL** <https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/armknecht>

In this talk, we present a novel cryptographic mechanism that is based on LFSRs (linear feedback shift register). It may be seen as a kind of proof of work in the following sense. The task is to compute certain elements from a finite group that are determined by an LFSR. The novel aspect here is that to this end, a short LFSR with small coefficients (over some finite field larger than  $\text{GF}(2)$ ) are used but these specifications are kept secret. Instead, one publishes a related LFSR that is longer and has large coefficients. The aim of this scheme is that a prover who knows only the public specifications has to invest a minimum amount of effort to generate the elements while a verifier can use the knowledge of the secret specifications for a much faster verification.

The scheme has been initially introduced by us at USENIX Security 2016 to realize a scheme that allows for remote verification whether data has been stored with a sufficient level of redundancy. We think however that the presented mechanism can be of independent interest and poses some novel challenges, e.g., how to prove a minimum effort of the prover. In this talk, we explain the mechanism into more detail and also tell security arguments why a prover seem to have a higher computational effort than the verifier.

### 3.4 Rasta: Designing a cipher with low ANDdepth and few ANDs per bit

*Christoph Dobraunig (TU Graz, AT)*

**License** © Creative Commons BY 3.0 Unported license  
© Christoph Dobraunig


**Joint work of** Christoph Dobraunig, Maria Eichlseder, Lorenzo Grassi, Virginie Lallemand, Gregor Leander, Florian Mendel, Christian Rechberger

Various lines of work have recently progressed with the investigation of the design and analysis of symmetric cryptographic schemes that minimize multiplications in one way or another. This has already led to unusual designs and interesting cryptanalytic insights. Even when only considering the class of schemes whose circuit has a natural and simple description in  $\text{GF}(2)$ , there are various metrics that are interesting and useful: The total number of AND gates, the number of AND gates per encrypted bit, or the depth of the AND gate part of the circuit (ANDdepth), among others.

In this talk, we present with Rasta a design strategy for symmetric encryption that has ANDdepth  $d$  and at the same time only needs  $d$  ANDs per encrypted bit. The main result is that even for very low values of  $d$  between 2 and 6 we can give strong evidence that attacks may not exist. This contributes to a better understanding of the limits of what concrete symmetric-key constructions can theoretically achieve with respect to AND-related metrics.

### 3.5 Leakage-Resilient Authenticated Encryption

*Stefan Lucks (Bauhaus-Universität Weimar, DE)*

**License**  Creative Commons BY 3.0 Unported license  
© Stefan Lucks

Practical cryptography often suffers from vulnerabilities to side-channel attacks. Two major approaches to deal with this problem are physical and algorithmic countermeasures. Physical countermeasures, such as “masking”, try to prevent the side-channel, or to narrow it down. Algorithmic countermeasures are about meaningful security against adversaries with access to a (limited) side-channel.

This talk is about algorithmic countermeasures, which have been initiated with high hopes (Micali, Reyzin, 2004; Dziembowski, Pietrzak, 2008), but so far failed to take off in practice, specifically in Symmetric Cryptography. This talk is about algorithmic countermeasures and schemes which are supposed to be practically useful, while still maintaining a sound theoretical security proof. The formal approach is the introduction of leaking queries for (otherwise) ideal block ciphers.

### 3.6 Key Prediction Security of Keyed Sponges

*Bart Mennink (Radboud University Nijmegen, NL)*

**License**  Creative Commons BY 3.0 Unported license  
© Bart Mennink

The keyed sponge is a well-accepted method for message authentication. It processes data at a certain rate by sequential evaluation of an underlying permutation. If the key size  $k$  is smaller than the rate, currently known bounds are tight, but if it exceeds the rate, state of the art only dictates security up to  $2^{k/2}$ . We take closer inspection at the key prediction security of the sponge and close the remaining gap in the existing security analysis: we confirm key security up to close to  $2^k$ , regardless of the rate. The result impacts all applications of the keyed sponge and duplex that process at a rate smaller than the key size, including the STROBE protocol framework, as well as the related constructions such as HMAC-SHA-3 and the sandwich sponge.

### 3.7 Tree-searching for trail bounds

*Gilles Van Assche (STMicroelectronics – Diegem, BE)*

**License**  Creative Commons BY 3.0 Unported license  
© Gilles Van Assche

**Joint work of** Silvia Mella, Joan Daemen, Gilles Van Assche

**Main reference** Silvia Mella, Joan Daemen, Gilles Van Assche: “New techniques for trail bounds and application to differential trails in Keccak”, IACR Trans. Symmetric Cryptol., Vol. 2017(1), pp. 329–357, 2017.

**URL** <http://dx.doi.org/10.13154/tosc.v2017.i1.329-357>

In this presentation, we present the advantages of using a unit-based tree search for bounding the weight of differential and linear trails in cryptographic primitives. After recalling the definitions as set out in [1], we motivate the technique for the generation and the extension of differential and linear trails in the KECCAK- $f$  permutation. We then explain how the technique can easily avoid generating states that are equivalent under symmetry properties,



and how to use it to express trail extension when the states form an affine space. As an additional application, we show the bounds obtained on the new Xoodoo permutation and how the definition of units differed from those in Keccak- $f$ . Finally, we conclude with questions that guide the application of the technique to a given cryptographic primitive.

## References

- 1 S. Mella, J. Daemen and G. Van Assche. New techniques for trail bounds and application to differential trails in Keccak. IACR Trans. Symmetric Cryptol. 2017(1): 329-357 (2017)

## 3.8 Merkle Tree is not Optimal

*Dmitry Khovratovich (University of Luxembourg, LU)*

**License** © Creative Commons BY 3.0 Unported license  
© Dmitry Khovratovich

No abstract given.

## 3.9 Fast Correlation Attack Revisited

*Yosuke Todo (NTT – Tokyo, JP)*

**License** © Creative Commons BY 3.0 Unported license  
© Yosuke Todo

**Joint work of** Takanori Isobe, Willi Meier, Kazumaro Aoki, Bin Zhang

A fast correlation attack (FCA) is a well-known cryptanalysis technique for LFSR-based stream ciphers. The correlation between the initial state of an LFSR and corresponding key stream is exploited, and the goal is to recover the initial state of the LFSR. In this talk we revisit the FCA from a new point of view based on a finite field, and it brings a new property for the FCA when there are multiple linear approximations. Moreover we propose a novel algorithm by using the new property, which enables us to reduce both time and data complexities. We finally apply this technique to the Grain family, which is a well-analyzed class of stream ciphers. There are three stream ciphers, Grain-128a, Grain-128, and Grain-v1 in the Grain family, and Grain-v1 is in the eSTREAM portfolio and Grain-128a is standardized by ISO/IEC. As a result we break them all, and especially for Grain-128a, the cryptanalysis on its full version is reported for the first time.

## 3.10 Towards Quantitative Analysis of Cyber Security

*Adi Shamir (Weizmann Institute – Rehovot, IL)*

**License** © Creative Commons BY 3.0 Unported license  
© Adi Shamir

**Joint work of** Achiya Bar-On, Itai Dinur, Orr Dunkelman, Rani Hod, Nathan Keller, Eyal Ronen, Adi Shamir

Cyber security is a hot research area, but almost all the discussion about it is qualitative rather than quantitative. In this talk we consider the specific subtopic of backup schemes designed to protect computer systems against ransomware and cyber attacks. We develop a precise model with a concrete cost function, which describes the problem as an online/offline

optimization problem whose solution can be described by a pebbling game. We provide optimal backup schemes for all the cases with up to 10 backup devices, and find matching upper and lower bounds on the asymptotic efficiency of optimal backup schemes with an arbitrarily large number of backup devices.

### 3.11 Security of Caesar Candidates against (beyond) Birthday and/or Nonce-Reusing Attacks

*Damian Vizár (EPFL – Lausanne, CH)*

**License** © Creative Commons BY 3.0 Unported license

© Damian Vizár

**Joint work of** Serge Vaudenay, Damian Vizár

**Main reference** Serge Vaudenay, Damian Vizár: “Under Pressure: Security of Caesar Candidates beyond their Guarantees”, IACR Cryptology ePrint Archive, Vol. 2017, p. 1147, 2017.

**URL** <http://eprint.iacr.org/2017/1147>

The Competition for Authenticated Encryption: Security, Applicability and Robustness (CAESAR) has as its official goal to “identify a portfolio of authenticated ciphers that offer advantages over [the Galois-Counter Mode with AES]” and are suitable for widespread adoption.” Each of the 15 candidate schemes competing in the currently ongoing 3<sup>rd</sup> round of CAESAR must clearly declare its security claims, i.a. whether or not it can tolerate nonce misuse, and what is the maximal data complexity for which security is guaranteed. These claims appear to be valid for all 15 candidates.

Interpreting “Robustness” in CAESAR as the ability to mitigate damage when security guarantees are void, we describe attacks with 64-bit complexity or beyond, and/or with nonce reuse for each of the 15 candidates. We then classify the candidates depending on how powerful does an attacker need to be to mount (semi-)universal forgeries, decryption attacks, or key recoveries. Rather than invalidating the security claims of any of the candidates, our results provide an additional criterion for evaluating the security that candidates deliver, which can be useful for e.g. breaking ties in the final CAESAR discussions.

### 3.12 Key-Recovery Attacks on Full Kravatte

*Henri Gilbert (ANSSI – Paris, FR)*

**License** © Creative Commons BY 3.0 Unported license

© Henri Gilbert

**Joint work of** Colin Chaigneau, Thomas Fuhr, Henri Gilbert, Jian Guo, Jérémy Jean, Jean-René Reinhard, Ling Song

**Main reference** Colin Chaigneau, Thomas Fuhr, Henri Gilbert, Jian Guo, Jérémy Jean, Jean-René Reinhard, Ling Song: “Key-Recovery Attacks on Full Kravatte”, IACR Trans. Symmetric Cryptol., Vol. 2018(1), pp. 5–28, 2018.

**URL** <http://dx.doi.org/10.13154/tosc.v2018.i1.5-28>

We present a cryptanalysis of the July 2017 version of the full Kravatte and of a strengthened version presented in November at ECC 2017. Kravatte is an instantiation of the Farfalle construction of a pseudorandom function (PRF) with variable input and output length. This construction, proposed by Bertoni et al., represents an efficiently parallelizable and extremely versatile building block for the design of symmetric mechanisms, e.g. message authentication codes or stream ciphers. It relies on a set of non-linear permutations and on so-called rolling functions and can be split into a compression layer followed by a two-step expansion layer.

Kravatte instantiates Farfalle using linear rolling functions and non-linear permutations obtained by iterating the Keccak round function.

We develop several key recovery attacks against this PRF, based on three different attack strategies that bypass part of the construction and target a reduced number of permutation rounds. A higher order differential attack exploits the possibility to build an affine space of values in the cipher state after the compression layer. An algebraic meet-in-the-middle attack can be mounted on the second step of the expansion layer. Finally, a linear recurrence distinguisher can be found on intermediate states of the second step of the expansion layer and leveraged to mount a third attack. All the attacks rely on the ability to invert a small number of the final rounds of the construction. In particular, the last two rounds of the construction together with the final masking by the key can be algebraically inverted, which allows to recover the key. The complexities of the attacks are far below the claimed security level. Following the communication of the above cryptanalyses to the designers, a tweaked version of Kravatte was released in December 2017, in which one of the linear rolling functions is replaced by a non-linear rolling function.

### 3.13 Clustering Related-Tweak Characteristics

*Maria Eichlseder (TU Graz, AT)*

**License** © Creative Commons BY 3.0 Unported license  
© Maria Eichlseder

**Joint work of** Maria Eichlseder, Daniel Kales

The TWEAKEY/STK construction is an increasingly popular approach for designing tweakable block ciphers that notably uses a linear tweakkey schedule. Several recent attacks have analyzed the implications of this approach for differential cryptanalysis and other attacks that can take advantage of related tweakkeys. We generalize the clustering approach of a recent differential attack on the tweakable block cipher MANTIS-5 and describe a tool for efficiently finding and evaluating such clusters. More specifically, we consider the set of all differential characteristics compatible with a given truncated characteristic, tweak difference, and optional constraints for the differential. We refer to this set as a semi-truncated characteristic and estimate its probability by analyzing the distribution of compatible differences at each step.

We apply this approach to find a semi-truncated differential characteristic for MANTIS-6 with probability about  $2^{-68}$  and derive a key-recovery attack with a complexity of about  $2^{55}$  chosen-plaintext queries and computations. The data-time product is about  $2^{110} \ll 2^{126}$ .

### 3.14 Conditional Linear Cryptanalysis

*Stav Perle (Technion – Haifa, IL) and Eli Biham (Technion – Haifa, IL)*

**License** © Creative Commons BY 3.0 Unported license  
© Stav Perle and Eli Biham

In this talk we introduce an extension of linear cryptanalysis that may reduce the complexity of attacks by conditioning linear approximations on other linear approximations. We show that the bias of some linear approximations may increase under such conditions, so that after discarding the known plaintexts that do not satisfy the conditions, the bias of the remaining

known plaintexts increases. We show that this extension can lead to improvements of attacks, which may require fewer known plaintexts in total. By a careful application of our extension to Matsui’s attack on the full 16-round DES we succeed to reduce the complexity of the best attack on DES to less than  $2^{42}$ .

### 3.15 Linear Cryptanalysis Using Low-Bias Approximations

*Tomer Ashur (KU Leuven, BE)*

**License** © Creative Commons BY 3.0 Unported license  
© Tomer Ashur

**Joint work of** Tomer Ashur, Daniël Bodden, Orr Dunkelman

**Main reference** Tomer Ashur, Daniël Bodden, Orr Dunkelman: “Linear Cryptanalysis Using Low-bias Linear Approximations”, IACR Cryptology ePrint Archive, Vol. 2017, p. 204, 2017.

**URL** <http://eprint.iacr.org/2017/204>

This work deals with linear approximations having absolute bias smaller than  $2^{-n/2}$  which were previously believed to be unusable for a linear attack. We show how a series of observations which are individually not statistically significant can be used to create a  $\chi^2$  distinguisher. This is different from previous works which combined a series of significant observations to reduce the data complexity of a linear attack.

### 3.16 Multidimensional, Affine and Conditional Linear Cryptanalysis

*Kaisa Nyberg (Aalto University, FI)*

**License** © Creative Commons BY 3.0 Unported license  
© Kaisa Nyberg

Recently, new variants of linear cryptanalysis have been proposed. In this talk we focus on the affine multidimensional cryptanalysis and the conditional linear cryptanalysis. The affine method is based on multidimensional linear cryptanalysis and offers the option of discarding a whole half-space of linear approximations that do not contribute to statistical nonrandomness to keep only the information extracted from an affine subspace of linear approximations. The conditional linear cryptanalysis was invented by Biham and Perle. In this talk we compare these methods and explain their relationships in the light of a small practical example originating from the DES cipher.

#### Introduction

Linear cryptanalysis is a statistical method used for distinguishing a block cipher from a random family of permutations and can be extended to key recovery attacks in practical ciphers. It makes use of nonrandom behavior of linear approximations, which are single-bit values obtained by exclusive-or summation of certain input bits and output bits of the block cipher, or some rounds of it, over a large number of plaintexts.

Correlations of linear approximations over a block cipher with a fixed key are typically not statistically independent when taken as random variables over the data space. Methods that explicitly measure such dependencies, and use them in statistical analysis, have been presented previously by Murphy in [5] and very recently by Biham and Perle [1]. On the other hand, the main motivation of multidimensional linear cryptanalysis is that the

dependencies of linear approximations need not be measured explicitly as they are captured by the multidimensional linear test statistic. In this paper, we will present a concrete example to illustrate how this works in practice.

Next we briefly recall the multidimensional linear method, the affine space method, and the conditional linear cryptanalysis, and illustrate them for an example presented by Biham and Perle.

### Multidimensional Linear Cryptanalysis

In the context of linear cryptanalysis, a linear approximation of a transformation  $F$  from  $\mathbb{F}_2^n$  to  $\mathbb{F}_2^m$  is a Boolean function in  $\mathbb{F}_2^n$  defined by two vectors  $a, \in \mathbb{F}_2^n$  and  $b \in \mathbb{F}_2^m$  as follows

$$x \mapsto a \cdot x + b \cdot F(x).$$

In the statistical setting, a linear approximation is considered as a binary random variable  $X$  over the given space of transformations with a probability density function defined by

$$\Pr(X = 0) = 2^{-n} \#\{x \in \mathbb{F}_2^n \mid a \cdot x + b \cdot F(x) = 0\}.$$

So we can write  $X = a \cdot x + b \cdot F(x)$ . In the linear-algebraic setting, a linear approximation  $a \cdot x + b \cdot F(x)$  is identified with the vector  $(a, b)$ , called a mask pair, in the linear space  $\mathbb{F}_2^n \times \mathbb{F}_2^m$  over  $\mathbb{F}_2$ .

Each linear approximation of  $F(x)$  is a Boolean function and induces a probability distribution on  $\{0, 1\}$ . Its bias  $\varepsilon_{(a,b)}$  is given by

$$\varepsilon_{(a,b)} = \Pr(a \cdot x + b \cdot F(x) = 0) - 1/2$$

and its correlation  $c_{(a,b)}$  by

$$c_{(a,b)} = 2\varepsilon_{(a,b)} = \Pr(a \cdot x + b \cdot F(x) = 0) - \Pr(a \cdot x + b \cdot F(x) = 1).$$

Multidimensional linear cryptanalysis considers a number of linear approximations that form a linear subspace  $V$  in  $\mathbb{F}_2^n \times \mathbb{F}_2^m$ . Let  $t$  be the dimension of this subspace. Then a multidimensional linear approximation is a vector-valued Boolean function from  $\mathbb{F}_2^n$  to  $\mathbb{F}_2^t$ . The components of this vector-valued function are in one-to-one correspondence with the mask pairs  $(a, b) \in V$ .

The strength of a multidimensional linear approximation is measured by its capacity  $C_V$  given as follows

$$C_V = \sum_{(a,b) \in V, (a,b) \neq 0} c_{(a,b)}^2.$$

The multidimensional distinguisher is defined by the following test statistic

$$\begin{aligned} T(D) &= N \sum_{(a,b) \in V, (a,b) \neq 0} \hat{c}_{(a,b)}(D)^2, \text{ where} \\ D &= \text{is a sample of } N \text{ plaintexts } x, \\ \hat{c}_{(a,b)}(D) &= N^{-1} (\#\{x \in D \mid a \cdot x + b \cdot F(x) = 0\} - \#\{x \in D \mid a \cdot x + b \cdot F(x) = 1\}). \end{aligned}$$

Under the assumption that the data for the observed correlations are computed from  $N$  independently and randomly drawn  $x$ , the test statistic  $T(D)$  is a Pearson's chi square test statistic with  $2^t - 1$  degrees of freedom. For large  $N$  and for uniformly distributed data,  $T(D)$  follows a central chi square distribution. In the case, where the sample is drawn from a

nonuniform distribution, it was argued in [4] based on [3] that  $T(D)$  follows a noncentral chi square distribution with noncentrality parameter  $NC_V$ , where  $C_V$  is the nonzero capacity of the multidimensional linear approximation applied to cipher.

Let us now present an example of a typical situation where the subspace  $V$  contains many useless linear approximations. Suppose that a multidimensional linear approximation of a cipher is built around a set of mask pairs  $(a, b)$ , where  $a$  is a fixed nonzero mask on the plaintext and the ciphertext masks  $b$  vary within a linear subspace  $B$ . The least linear subspace to contain all such masks is  $\{0, a\} \times B$ . Then the correlations of the linear masks of the form  $(0, b)$ ,  $b \in B$  have correlation zero, and do not add to the capacity of the multidimensional linear approximation, but just make the linear approximation space larger. Clearly,

$$\{a, 0\} \times B = (\{a\} \times B) \cup (\{0\} \times B).$$

The affine subspace method to be presented next allows to discard the useless linear approximations in  $\{0\} \times B$  and exploit the useful ones in the affine subspace  $\{a\} \times B$ .

### Affine Multidimensional Linear Cryptanalysis

Given a multidimensional linear approximation as described in the previous section, we split  $V$  into two halves, a subspace  $U$  of dimension  $s = t - 1$  and the affine subspace  $V \setminus U$ . Given  $(a_1, b_1) \in V \setminus U$ , all the mask pairs in  $V$  can be written in the form  $(a_2, b_2)$  or  $(a_1 + a_2, b_1 + b_2)$ , where  $(a_2, b_2) \in U$ .

First, Let us apply the multidimensional linear model to the sapce  $V$ . Then the test statistic  $T_V(D)$  is computed as follows

$$T_V(D) = N \sum_{(a,b) \in V} \hat{c}_{(a,b)}(D)^2.$$

Secondly, let us apply the multidimensional model to the linear approximations in the subspace  $U$  to obtain whence the test statistic is computed as

$$T_U(D) = N \sum_{(a_2,b_2) \in U} \hat{c}_{(a_2,b_2)}(D)^2.$$

We now define the affine test statistic  $T_{\text{aff}}(D)$  as follows

$$T_{\text{aff}}(D) = T_V(D) - T_U(D) = N \sum_{(a_2,b_2) \in U} \hat{c}_{(a_1+a_2,b_1+b_2)}(D)^2.$$

Under the assumption that the data for the observed correlations are computed from  $N$  independently and randomly drawn  $x$ , we obtain using Pearson's chi square test that  $T_{\text{aff}}(D)$  is chi square distributed with  $2^s$  degrees of freedom, for large  $N$ . In the random case, we then have a central chi square distribution with mean  $2^s$  and variance  $2^{s+1}$ . Otherwise, the mean can be computed from the expression  $T_{\text{aff}}(D) = T_V(D) - T_U(D)$  to get

$$\text{Exp } T_{\text{aff}}(D) = 2^s + N(C_V - C_U).$$

Thus the noncentrality parameter of the chi square distribution of  $T_{\text{aff}}(D)$  in the cipher case is equal to  $C_V - C_U$ , and we obtain

$$\text{Var } T_{\text{aff}}(D) = 2(2^s + 2N(C_V - C_U)).$$

Similarly as for multidimensional linear cryptanalysis, the derived affine statistical model can be used in cryptanalytic distinguishing and key-recovery attacks. Next we present a second example which shows that the affine space method can improve upon the multidimensional linear cryptanalysis.

### Example of Biham and Perle

Recently, Eli Biham and Stav Perle proposed a new cryptanalysis method called as conditional linear cryptanalysis [1]. It applies to the case where two linear approximations are mutually dependent. For example, they found two dependent linear approximations in DES. We denote the random variables related to them by  $X$  and  $Y$ . They have the following probability density functions

$$\begin{aligned}\Pr(X = 0) &= \frac{1}{2} + \varepsilon & \Pr(X = 1) &= \frac{1}{2} - \varepsilon \\ \Pr(Y = 0) &= \frac{1}{2} & \Pr(Y = 1) &= \frac{1}{2}.\end{aligned}$$

Their dependency is given in terms of conditional probabilities

$$\begin{aligned}\Pr(X = 0|Y = 0) &= \frac{1}{2} + 2\varepsilon, & \Pr(X = 0|Y = 1) &= \frac{1}{2}, \\ \Pr(X = 1|Y = 0) &= \frac{1}{2} - 2\varepsilon, & \Pr(X = 1|Y = 1) &= \frac{1}{2}.\end{aligned}$$

We use this example to illustrate the behavior of the three variants of linear cryptanalysis.

**The multidimensional linear model.** The capacity of the 2-dimensional multidimensional linear approximation in  $V$  spanned by the linear approximations  $X$  and  $Y$  is equal to

$$C_V = c_X^2 + c_Y^2 + c_{X+Y}^2.$$

Note that we use the variable symbol instead of the mask pairs to identify the non-zero linear approximations. It is easy to check that the linear approximation  $X + Y$  has the same bias as  $X$ , and the bias of  $Y$  is equal to zero. We get  $C_V = 8\varepsilon^2$ . Then the multidimensional test statistic

$$T_V = N (\hat{c}_X(D)^2 + \hat{c}_Y(D)^2 + \hat{c}_{X+Y}(D)^2)$$

has a noncentral chi square distribution with 3 degrees of freedom and noncentrality parameter equal to  $8N\varepsilon^2$ .

**The affine linear model.** Since  $c_Y = 0$ , it does not contribute to the capacity of the multidimensional distribution. To discard it, we apply the affine linear model with the 1-dimensional subspace  $U = \{0, Y\}$ . Then the affine test statistic

$$T_{\text{aff}} = N (\hat{c}_X(D)^2 + \hat{c}_{X+Y}(D)^2)$$

has chi square distribution with 2 degrees of freedom and noncentrality parameter

$$N(C_V - C_U) = N(c_X^2 + c_{X+Y}^2) = 8N\varepsilon^2.$$

It means that the affine linear test has the same noncentrality parameter but less degrees of freedom than the multidimensional linear test and hence is more efficient.

**The conditional linear model.** Recently, Biham and Perle proposed conditional linear cryptanalysis to exploit high conditional correlations [1]. The idea is to use the analogical statistical model as for classical linear cryptanalysis in the context of conditional probabilities and biases by discarding the data that does not satisfy the condition. According to this model the observed number of data  $\hat{N}'$  that satisfy  $X = 0$  within a sample of  $N'$  plaintext-ciphertext pairs that satisfy  $Y = 0$  is binomially distributed with probability  $\Pr(X = 0|Y = 0) =$

$1/2 + 2\varepsilon$  and sample size  $N'$ . The bias of this conditional distribution is  $2\varepsilon$  and the correlation is  $4\varepsilon$ . Hence the distribution of the observed correlation

$$2\hat{N}'/N' - 1$$

can be approximated by a normal distribution with mean  $c_{X|Y=0} = 4\varepsilon$  and variance  $1/N'$ , where we denoted by

$$c_{X|Y=0} = \Pr(X = 0 | Y = 0) - \Pr(X = 1 | Y = 0)$$

the conditional correlation.

The data complexity estimate obtained from the normal distribution is the same that can be obtain using the chi square distribution obtained from the squared observed correlation [2]. More precisely, the conditional test statistic  $T_{\text{cond}}$  defined as

$$T_{\text{cond}} = N'(2\hat{N}'/N' - 1)^2 \sim \chi_1^2(\delta)$$

where

$$\delta = N'c_{X|Y=0}^2 = 16N'\varepsilon^2$$

gives the same data complexity estimate as the binomial (normal) test statistic  $\hat{N}'/N'$  traditionally used in linear cryptanalysis. Since  $Y$  is unbiased, it is estimated that for the total size  $N$  of the sample is equal to  $2N'$ .

We can see that the non-centrality parameter  $\delta$  is the same also in the case of conditional linear cryptanalysis. To explain this coincidence, we need to express the capacity of the affine linear approximation in terms of the probabilities  $p_{00}$ ,  $p_{01}$ ,  $p_{10}$ , and  $p_{11}$ , where

$$p_{uv} = \Pr(X = u, Y = v), \quad u = 0, 1 \text{ and } v = 0, 1$$

are the probabilities of the 2-dimensional variable  $(X, Y)$ . Then it can be shown that

$$C_V - C_U = c_X^2 + c_{X+Y}^2 = 2((p_{00} - p_{10})^2 + (p_{01} - p_{11})^2)$$

Now we observe that  $p_{01} - p_{11} = 0$ . It means that all the nonbalancedness of the distribution of this pair  $(X, Y)$  of linear approximations can be measured by the first term

$$p_{00} - p_{10} = \Pr(Y = 0)(\Pr(X = 0 | Y = 0) - \Pr(X = 1 | Y = 0)) = \Pr(Y = 0)c_{X|Y=0},$$

that is, by the product of  $\Pr(Y = 0)$  and the conditional correlation  $c_{X|Y=0}$ .

Finally, we observe that the conditional approach allows to reduce the degree of freedom to one while keeping the noncentrality parameter the same as in the usual multidimensional cryptanalysis and in the affine multidimensional cryptanalysis. We conclude that from the three statistical models considered for the given example, the conditional linear cryptanalysis of Biham and Perle gives the most efficient statistical distinguisher.

**Acknowledgements.** I wish to thank Eli Biham for discussions related to conditional linear cryptanalysis and Céline Blondeau for suggestions how to improve the presentation.

## References

- 1 Eli Biham and Stav Perle. Conditional linear cryptanalysis. Presentation at Romanian Cryptology Days, Bucharest, Romania, Sept 18–20, 2017, and at Dagstuhl Seminar 18021 “Symmetric Cryptography”, Jan 7–12, 2018.



- 2 Céline Blondeau and Kaisa Nyberg. Improved parameter estimates for correlation and capacity deviates in linear cryptanalysis. *IACR Transactions on Symmetric Cryptology*, 2016(2):162–191, 2017.
- 3 F.C. Drost, W.C.M. Kallenberg, D.S. Moore, and J. Oosterhoff. Power Approximations to Multinomial Tests of Fit. *Journal of the American Statistical Association*, 84(405):130–141, Mar 1989.
- 4 Miia Hermelin, Joo Yeon Cho, and Kaisa Nyberg. Multidimensional Extension of Matsui’s Algorithm 2. In Orr Dunkelman, editor, *FSE 2009*, vol. 5665 of LNCS, pages 209–227. Springer, 2009.
- 5 Sean Murphy. The independence of linear approximations in symmetric cryptanalysis. *IEEE Transactions on Information Theory*, 52(12):5510–5518, 2006.

### 3.17 The Chi-Squared Method

*Stefano Tessaro (University of California – Santa Barbara, US)*

**License** © Creative Commons BY 3.0 Unported license  
© Stefano Tessaro

**Joint work of** Wei Dai, Viet Tung Hoang

Proving tight bounds on information-theoretic indistinguishability is a central problem in symmetric cryptography. In this talk, I introduce a new method for information-theoretic indistinguishability proofs, called “the chi-squared method”. At its core, the method requires upper-bounds on the so-called chi-squared divergence between the output distributions of two systems being queried

I will showcase the chi-squared method by giving a simple proof of optimal security for the XOR of two random permutations, which improves upon bounds previously shown with much more involved machinery (e.g., mirror theory).

### 3.18 Some applications of the chi square method


*Mridul Nandi (Indian Statistical Institute – Kolkata, IN)*

**License** © Creative Commons BY 3.0 Unported license  
© Mridul Nandi

In this talk, I would like to discuss some possible applications of chi-squared method. So far, it has been applied to the sum of random permutations, EDM and truncation of random permutation. Very recently, it is also applied to prove the PRF security of sum of permutation where the inputs are reused in a certain way. This is related the well known powerful tool – mirror theory. As the proof of the Mirror theory is highly complex and contains several non-trivial gap, it would be nice to explore other way out for the application of the mirror theory. Chi-squared method could be such an alternative. I also describe how to prove a weaker form of mirror theory using the chi-squared method result applied to the reused sum of permutation. Using this, I would be able to prove the weak-PRF full  $n$  bit security of EDM. This can be possibly extended to standard PRF security, but requires more closer analysis.

### 3.19 Beyond-Birthday-Bound Secure MACs

Yannick Seurin (ANSSI – Paris, FR)

License  Creative Commons BY 3.0 Unported license  
© Yannick Seurin

Joint work of Benoît Cogliati, Tetsu Iwata, Jooyoung Lee, Kazuhiko Minematsu, Thomas Peyrin

A Message Authentication Code (MAC) is a fundamental symmetric primitive allowing two entities sharing a secret key to verify that a received message originates from one of the two parties and was not modified by an attacker. Most existing MACs are built from a block cipher, e.g., CBC-MAC or OMAC, or from a cryptographic hash function, e.g., HMAC. In general, MACs which are constructed from a block cipher are secure only up to the so-called birthday bound with respect to the block size  $n$  of the block cipher: they become insecure when  $\sim 2^{n/2}$  (blocks of) messages have been treated. This might be problematic, especially when relying on lightweight block ciphers with small block size or when updating the secret key is impractical. In this talk, we survey recent results on MAC constructions based on a block cipher or a tweakable block cipher which are secure beyond the birthday bound such as EWCDM [1], ZMAC [2] and HaT/NaT/HaK/NaK [3] and we highlight some open problems along the way.

#### References

- 1 Benoît Cogliati and Yannick Seurin. EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC. In Matthew Robshaw and Jonathan Katz, editors, CRYPTO 2016 (1), vol. 9814 of LNCS, pp. 121–149. Springer, 2016.
- 2 Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin. ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication. In Jonathan Katz and Hovav Shacham, editors, CRYPTO 2017 (3), vol. 10403 of LNCS, pp. 34–65. Springer, 2017.
- 3 Benoît Cogliati, Jooyoung Lee, and Yannick Seurin. New Constructions of MACs from (Tweakable) Block Ciphers. IACR Trans. Symmetric Cryptol., 2017(2):27–58, 2017.

### 3.20 Recent Advancements in Sponge-Based MACs

Kan Yasuda (NTT - Tokyo, JP)

License  Creative Commons BY 3.0 Unported license  
© Kan Yasuda

No abstract given.

### 3.21 The collision-resistance of keyed hashing

Joan Daemen (Radboud University Nijmegen, NL, and STMicroelectronics – Diegem, BE)

License  Creative Commons BY 3.0 Unported license  
© Joan Daemen

MAC functions and pseudorandom functions with arbitrary input length often consist of two stages: a keyed hash function that compresses the input to a fixed-length *accumulator* followed by a function that maps the accumulator to the output, that may also have variable

length. The security requirement for the keyed hash is that it should be difficult for an adversary that does not know the key to find inputs that collide in the accumulator. More precisely, the adversary gets adaptive query access to the keyed hash function where she gets the image of the accumulator through a random oracle. In other words, she can only see whether inputs collide or not in the accumulator.

Keyed hash functions are implemented in a wide variety of ways: serial constructions such as CBC-MAC, polynomial evaluations in a finite field and Pelican-MAC or parallel constructions such as PMAC or Farfalle. These constructions make use of block ciphers, tweakable block ciphers or permutations. Each of these have their own advantages and disadvantages, but all are vulnerable to a generic collision attack that has success probability  $M^2 2^{-(b+1)}$  with  $b$  the size of the accumulator and  $M$  the number of queries to the keyed hash function (data complexity).

One usually characterizes the level of security that a cryptographic scheme offers by the so-called *security strength* that is expressed in bits. For a certain attack, it is the binary logarithm of its data complexity  $M$  minus that of its success probability  $p$ , so  $s = \log_2 M - \log_2 p$ . For the generic attacks, at one end of the spectrum is an attack with just a couple of queries that has  $s \approx b$ . At the other end the success probability approaches 1 when  $M \approx 2^{b/2}$  and hence it has  $s \approx b/2$ . So the maximum achievable security strength decreases from  $b$  to  $b/2$  bits as the attack complexity grows from 2 to  $2^{b/2}$ . This curve is called the *birthday bound*.

When designing a keyed hash function, different strategies may be followed. First, one may aim either for a capacity claim or for a security strength claim.

In the former, one makes a claim for the function that there are no attacks with success probability below  $M^2 2^{-(c+1)}$  with  $c$  some specified constant usually called the *capacity*. In the so-called *hermetic* design strategy, one chooses  $b = c$ , implying that there are no attacks better than the generic attack and hence that the used primitive has no exploitable weaknesses. This usually requires using a primitive with a significant computational cost. This cost can be reduced drastically by taking  $b > c$ , so by over-dimensioning the primitive. An example of this strategy is Pelican-MAC, that has  $c = 120$  and uses 4 unkeyed AES rounds as permutation, so  $b = 128$ .

In a security strength claim one states that there are no attacks with success probability below  $M 2^{-s}$ , possibly putting an upper bound on  $M$ . If this upper bound is  $2^a$  with  $a < s$ , this requires taking  $b$  at least  $s + a$  and  $2s$  otherwise. An example is Kravatte with  $b = 1600$  and  $s = 137$ .

Determining the best attack strategy for collision attacks for the different constructions in combination with different primitives is an interesting research problem and allows gaining insight in how to build the most efficient keyed hash function for some given set of target platforms and for some target security, either expressed by a capacity  $c$  or a strength  $s$ .

### 3.22 Challenges and Opportunities for the Standardization of Threshold Cryptography

*Nicky Mouha (NIST – Gaithersburg, US)*

**License** © Creative Commons BY 3.0 Unported license  
© Nicky Mouha

**Joint work of** Apostol Vassilev, Nicky Mouha, Luís Brandão

**Main reference** Apostol Vassilev, Nicky Mouha, Luis Brandao: “Psst, Can You Keep a Secret?”, IEEE Computer, Vol. 51(1), pp. 94–97, 2018.

**URL** <http://dx.doi.org/10.1109/MC.2018.1151029>

Cryptography lies at the heart of the protection of data at rest and in transit over the Internet. The security of data afforded by the employed cryptographic primitives depends not only on their theoretical properties but also on the robustness of their implementations in software and hardware. Threshold cryptography introduces a computational paradigm that enables a higher level of assurance for the implementations of cryptographic primitives.

We discuss challenges and opportunities related to the standardization of threshold cryptography [1], and give some insights into their application to symmetric-key cryptography.

#### References

- 1 Apostol Vassilev, Nicky Mouha, Luís Brandão. Psst, Can you Keep a Secret? IEEE Computer 51(1): 94–97, 2018, <https://dx.doi.org/10.1109/MC.2018.1151029>

### 3.23 Tools on Cryptanalysis

*Stefan Kölbl (Technical University of Denmark – Lyngby, DK)*

**License** © Creative Commons BY 3.0 Unported license  
© Stefan Kölbl

**Joint work of** Zahra Eskandari, Andreas Brasen Kidmose, Stefan Kölbl, Tyge Tiessen

The division property method is a powerful technique to determine integral distinguishers on block ciphers. While the complexity of finding these distinguishers is higher, it has recently been shown that MILP and SAT solvers can efficiently find such distinguishers.

In this work, we provide a framework to fully automate finding those distinguishers which solely relies on a simple description of the cryptographic primitive. We demonstrate the ease of use by finding integral distinguishers for more than 30 primitives based on different design strategies and present several new or improved distinguishers for ChaCha, ChasKey, DES, GIFT, LBlock, Mantis, Qarma, RoadRunner, Salsa and SM4.

### 3.24 A survey of recent results on AES permutations

*Christian Rechberger (TU Graz, AT)*

**License** © Creative Commons BY 3.0 Unported license  
© Christian Rechberger

We survey recent results on new properties of AES, and subspace trail cryptanalysis as a way to describe it. This includes various properties of 5-round AES that hold for any secret key, and a 10-round property that holds for a set of  $2^{32}$  chosen keys.

### 3.25 Cryptanalysis of Reduced Round AES, Revisited

*Orr Dunkelman (University of Haifa, IL)*

**License** © Creative Commons BY 3.0 Unported license  
© Orr Dunkelman

**Joint work of** Achiya Bar-On, Nathan Keller, Eyal Ronen, Adi Shamir

Determining the security of AES is a central problem in cryptanalysis, but progress in this area had been slow and only a handful of cryptanalytic techniques led to significant advancements. At Eurocrypt 2017 Grassi et al. presented a novel type of distinguisher for AES-like structures, but so far all the published attacks which were based on this distinguisher were either inferior or comparable to previously known attacks in their complexity. In this paper we combine the technique of Grassi et al. with several other techniques to obtain the best known key recovery attack on 5-round AES in the single-key model, reducing its data, memory and time complexities from about  $2^{32}$  to about  $2^{22.5}$ . Extending our techniques to 7-round AES, we obtain the best known attacks which use practical amounts of data and memory, breaking the record for such attacks which was obtained 18 years ago by the classical Square attack.

### 3.26 Integral Attacks on AES

*Meiqin Wang (Shandong University – Jinan, CN)*

**License** © Creative Commons BY 3.0 Unported license  
© Meiqin Wang


Reduced-round version of AES has been a popular underlying primitives to design new cryptographic schemes. The security including the distinguishing property of AES deserves to study more. Recently, the key-dependent integral and impossible differential distinguishers for 5-round AES have been put forward. Later, the structural distinguisher and Yoyo distinguisher for 5-round or 6-round AES have been introduced. Although the complexities of the key-dependent integral and impossible differential distinguishers are much higher than those of the structural or Yoyo distinguisher for 5-round AES, more detailed property for MixColumn can be identified by them. Traditional impossible differential and integral distinguishers for 4-round AES have approximately equal data complexity. However, for the recent proposed key-dependent distinguishers, there is a big gap between the complexities of the integral and impossible differential distinguishers. Even with the same property of MixColumn, the integral distinguisher requires the whole codebook while the impossible distinguisher just needs  $2^{98.2}$  chosen plaintexts. Moreover, the complexities of traditional impossible differential or integral distinguishers are identical for the chosen-plaintext and chosen-ciphertext settings, but they are very different for the key-dependent distinguishers. Till now, the 5-round integral and impossible differential distinguishers can only work for chosen-ciphertext and chosen plaintext settings, respectively.

In this talk, by appending the condition for the output values for 5-round zero-correlation linear hull, we can transform such zero-correlation linear hull to a new key-dependent integral distinguisher for 5-round AES with  $2^{96}$  chosen plaintexts which is much better than the previous integral distinguisher at CRYPTO 2015 with the whole codebook. Secondly, we focus on transforming the key-dependent impossible differential distinguishers from the chosen-plaintext to chosen-ciphertext situation by setting the condition on the output values.

We found that the key-dependent integral distinguishers have very different complexities but the key-dependent impossible differential distinguishers have no significant difference for the complexity under different attacking modes. Finally, we utilize our proposed 5-round integral distinguisher to recover the key for 6-round AES. Although the key recovery attack is no better than the previous attacks with 4-round distinguishers, it is the first integral key-recovery attack on 6-round based on 5-round distinguisher.

### 3.27 On Sboxes sharing the same DDT

Anne Canteaut (INRIA – Paris, FR)

License  Creative Commons BY 3.0 Unported license  
© Anne Canteaut

Joint work of Christina Boura, Anne Canteaut, Jérémy Jean, Valentin Suder

In this work, we discuss two notions of differential equivalence on Sboxes. First, we introduce the notion of DDT-equivalence which applies to vectorial Boolean functions that share the same difference distribution table (DDT). It is worth noticing that this property equivalently means that the two functions share the same squared Walsh transform. Next, we compare this notion to what we call the  $\gamma$ -equivalence, applying to vectorial Boolean functions whose DDTs have the same support. This second property has been studied by Gorodilova for quadratic APN functions and in particular for the Gold family of functions. We discuss the relation between these two equivalence notions, demonstrate that the number of DDT- or  $\gamma$ -equivalent functions is invariant under EA- and CCZ-equivalence. This answers an open problem raised by Gorodilova. In parallel, we also provide an algorithm for computing the DDT-equivalence and the  $\gamma$ -equivalence classes of a given function. We study the sizes of these classes for some families of Sboxes.

### 3.28 Boomerang Connectivity Table (BCT) for Boomerang Attacks

Yu Sasaki (NTT – Tokyo, JP)

License  Creative Commons BY 3.0 Unported license  
© Yu Sasaki

Joint work of Carlos Cid, Tao Huang, Thomas Peyrin, Ling Song

A boomerang attack is a cryptanalysis framework that regards a block cipher  $E$  as the composition of two sub-ciphers  $E_1 \circ E_0$  and builds a particular characteristic for  $E$  with probability  $p^2q^2$  by combining differential characteristics for  $E_0$  and  $E_1$  with probability  $p$  and  $q$ , respectively. Crucially the validity of this figure is under the assumption that the characteristics for  $E_0$  and  $E_1$  can be chosen independently. Indeed, Murphy has shown that independently chosen characteristics may turn out to be incompatible. On the other hand, several researchers observed that the probability can be improved to  $p$  or  $q$  around the boundary between  $E_0$  and  $E_1$  by considering a positive dependency of the two characteristics, e.g. the ladder switch and S-box switch by Biryukov and Khovratovich. This phenomenon was later formalised by Dunkelman et al. as a sandwich attack that regards  $E$  as  $E_1 \circ E_m \circ E_0$ , where  $E_m$  satisfies some differential propagation among four texts with probability  $r$ , and the entire probability is  $p^2q^2r$ . In this paper, we revisit the issue of dependency of two characteristics in  $E_m$ , and propose a new tool called *Boomerang Connectivity Table (BCT)*,

which evaluates  $r$  in a systematic and easy-to-understand way when  $E_m$  is composed of a single S-box layer. With the BCT, previous observations on the S-box including the incompatibility, the ladder switch and the S-box switch are represented in a unified manner. Moreover, the BCT can detect a new switching effect, which shows that the probability around the boundary may be even higher than  $p$  or  $q$ .

### 3.29 QCCA on Feistel

*Tetsu Iwata (Nagoya University, JP)*

**License** © Creative Commons BY 3.0 Unported license  
© Tetsu Iwata

**Joint work of** Gembu Ito, Tetsu Iwata, Ryutaroh Matsumoto

Kuwakado and Morii considered quantum chosen plaintext attacks and showed an efficient distinguishing attack against the three-round Feistel cipher by using Simon's period finding algorithm [1]. In this talk, we consider quantum chosen ciphertext attacks, and present an efficient distinguishing attack against the four-round Feistel cipher.

#### References

- 1 Hidenori Kuwakado and Masakatu Morii. Quantum distinguisher between the 3-round Feistel cipher and the random permutation. ISIT 2010, pp. 2682–2685, IEEE, 2010.

### 3.30 Some Feistel structures with low degree round functions

*Arnab Roy (University of Bristol, GB)*

**License** © Creative Commons BY 3.0 Unported license  
© Arnab Roy

We consider several generalized Feistel constructions with low-degree round function. In particular, we study cases of the form  $x \rightarrow x^r$  for various  $r$ , with focus on the simplest case  $r = 3$ . Our analysis allows us to propose more efficient generalizations of the MiMC design (Asiacrypt'16). We evaluate the new designs in three application areas. Whereas MiMC was not competitive at all in a recently proposed new class of PQ-secure signature scheme, our new construction leads to about 30 times smaller signatures than MiMC. For MPC use cases, where MiMC seems to outperform all other competitors to start with, we observe substantial improvements in throughput by a factor of around 5 and simultaneously a 10-fold reduction of pre-processing effort, at the cost of a higher latency. Another use case where MiMC already outperforms other designs, in the area of SNARKs, only sees modest improvements.

### 3.31 Generalized Feistel Networks with Optimal Diffusion

Léo Paul Perrin (INRIA – Paris, FR)

**License** © Creative Commons BY 3.0 Unported license  
© Léo Paul Perrin

**Joint work of** Léo Perrin, Angela Promitzer, Sebastian Ramacher, Christian Rechberger  
**Main reference** Léo Perrin, Angela Promitzer, Sebastian Ramacher, Christian Rechberger: “Improvements to the Linear Layer of LowMC: A Faster Picnic”, IACR Cryptology ePrint Archive, Vol. 2017, p. 1148, 2017.

**URL** <http://eprint.iacr.org/2017/1148>

Generalized Feistel networks are a common block cipher structure. In [2], Suzaki and Minematsu introduced an improved branch permutation which allowed a faster diffusion in generalized Feistel networks. While such structures usually need  $b$  rounds to achieve full diffusion over  $b$  branches, Suzaki and Minematsu’s requires only about  $2 \log_2(b)$ .

In this talk, we presented a different method for building generalized Feistel networks with fast diffusion. The round function is simple: it can be seen as a simple two-branched Feistel network where the Feistel function consists in an S-Box layer followed by a rotation of the corresponding words. The core idea consists in using different rotation amounts in each round. Indeed, if those are chosen carefully then we can prove a fast diffusion. For example, if the rotation sequence is  $\{0, 1, 0, 2, 0, 4, 0, 8, 0, \dots\}$ , then diffusion is essentially as fast as in [2]. Furthermore, if the sequence is instead the Fibonacci sequence  $\{0, 1, 1, 2, 3, 5, 8, \dots\}$ , then diffusion is even faster and reaches an optimal bound first identified by Suzaki and Minematsu. The latter construction was used in [1] to build linear layers with full diffusion allowing a constant time implementation with a speed comparable to a table-based one.

#### References

- 1 Léo Perrin, Angela Promitzer, Sebastian Ramacher, and Christian Rechberger. Improvements to the Linear Layer of LowMC: A Faster Picnic. Cryptology ePrint Archive, Report 2017/1148, 2017.
- 2 Tomoyasu Suzaki and Kazuhiko Minematsu. Improving the Generalized Feistel. FSE 2010, pp 19–39. Springer, 2010.

### 3.32 An Improved Affine Equivalence Algorithm

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

**License** © Creative Commons BY 3.0 Unported license  
© Itai Dinur

**Main reference** Itai Dinur: “An Improved Affine Equivalence Algorithm for Random Permutations”, IACR Cryptology ePrint Archive, Vol. 2018, p. 115, 2018.

**URL** <https://eprint.iacr.org/2018/115>

In this work we study the affine equivalence problem, where given two functions  $\vec{F}, \vec{G} : \{0, 1\}^n \rightarrow \{0, 1\}^n$ , the goal is to determine whether there exist invertible affine transformations  $A_1, A_2$  over  $GF(2)^n$  such that  $\vec{G} = A_2 \circ \vec{F} \circ A_1$ . Algorithms for this problem have several well-known applications in the design and analysis of Sboxes, cryptanalysis of white-box ciphers and breaking a generalized Even-Mansour scheme.

We describe a new algorithm for the affine equivalence problem and focus on the variant where  $\vec{F}, \vec{G}$  are permutations over  $n$ -bit words, as it has the widest applicability. The complexity of our algorithm is about  $n^3 2^n$  bit operations with very high probability whenever  $\vec{F}$  (or  $\vec{G}$ ) is a random permutation. This improves upon the best known algorithms for this problem (published by Biryukov et al. at EUROCRYPT 2003), where the first algorithm has



time complexity of  $n^3 2^{2n}$  and the second has time complexity of about  $n^3 2^{3n/2}$  and roughly the same memory complexity.

Our algorithm is based on a new structure (called a *rank table*) which is used to analyze particular algebraic properties of a function that remain invariant under invertible affine transformations. Besides its standard application in our new algorithm, the rank table is of independent interest and we discuss several of its additional potential applications.

### 3.33 Invariant Attacks and (Non-)linear Approximations

*Christof Beierle*

**License** © Creative Commons BY 3.0 Unported license  
© Christof Beierle

**Joint work of** Christof Beierle, Anne Canteaut, Gregor Leander

This work discusses nonlinear approximations for block cipher cryptanalysis by embedding it into the better-understood framework of linear cryptanalysis.

In the first part we show that, in some cases, a deterministic nonlinear approximation (aka. nonlinear invariant attack) over a keyed instance of a cipher implies the existence of a (non-trivial) highly-biased linear approximation over the same instance. In the second part, we present a framework for studying non-deterministic nonlinear approximations. In particular, by transforming the cipher under consideration by conjugating each keyed instance with a fixed permutation, we are able to transfer many methods from linear cryptanalysis to the nonlinear case. Using this framework we in particular show that there exist ciphers for which some transformed versions are significantly weaker with respect to linear cryptanalysis than their original counterparts. This suggests that the basic security argument of counting the minimum number of active S-boxes may not be sufficient to avoid such kind of attacks.

### 3.34 Recent results on reduced versions of Ketje

*Maria Naya-Plasencia (INRIA – Paris, FR)*

**License** © Creative Commons BY 3.0 Unported license  
© Maria Naya-Plasencia

**Joint work of** Thomas Fuhr, María Naya-Plasencia, Yann Rotella


**Main reference** Thomas Fuhr, María Naya-Plasencia, Yann Rotella: “State-Recovery Attacks on Modified Ketje Jr”, IACR Trans. Symmetric Cryptol., Vol. 2018(1), pp. 29–56, 2018.

**URL** <http://dx.doi.org/10.13154/tosc.v2018.i1.29-56>

In this article we study the security of the authenticated encryption algorithm Ketje against divide-and-conquer attacks. Ketje is a third-round candidate in the ongoing CAESAR competition, which shares most of its design principles with the SHA-3 hash function. Several versions of Ketje have been submitted, with different sizes for its internal state. We describe several state-recovery attacks on the smaller variant, called Ketje Jr. We show that if one increases the amount of keystream output after each round from 16 bits to 40 bits, Ketje Jr becomes vulnerable to divide-and-conquer attacks with time complexities  $2^{71.5}$  for the original version and  $2^{82.3}$  for the current tweaked version, both with a key of 96 bits. We also propose a similar attack when considering rates of 32 bits for the non-tweaked version. Our findings do not threaten the security of Ketje, but should be taken as a warning against potential future modifications that would aim at increasing the performance of the algorithm.

### 3.35 On the security of LINE messaging application

*Kazuhiko Minematsu*

License  Creative Commons BY 3.0 Unported license  
© Kazuhiko Minematsu

Joint work of Takanori Isobe, Kazuhiko Minematsu

In this talk, we study the security of LINE messaging application (a.k.a. text messaging or instant messaging). LINE is by far the common messaging application in Japan, and is also popular in some East Asian countries, such as Taiwan, Thailand and Indonesia. There are 217 million monthly active users, as of Jan. 2017.

LINE provides an End-to-End (E2E) encryption scheme called Letter Sealing since 2015. After the reverse engineering work on Letter Sealing by Curtiss [1], LINE corporation has published a whitepaper [3] describing the specification of Letter Sealing in 2016. Recently, Espinoza et. al [2] proposed a replay attack against Letter Sealing.

We investigated this whitepaper, and found several vulnerabilities not covered by prior work. With these vulnerabilities, we found practical attacks against LINE's one-to-one messaging and group messaging. The vulnerabilities are listed as follows.

- The key and IV for symmetric-key encryption are derived from a group-shared key  $K_g$  and senders public information
- In the one-to-one key exchange phase, after individually computing “Shared Secret” at both sides, there is no key confirmation.
- In the symmetric-key encryption, the sender key ID and recipient key ID are not authenticated.

Some of our attacks are possible with the help of malicious messaging server (E2E adversary). We remark that many messaging application have equipped with an E2E encryption scheme, and the main purpose is to provide a protection against E2E adversary. In addition, we found some attacks that even do not need the help of E2E adversary, which is a severe security flaw.

We have informed our findings to LINE corporation in advance. LINE corporation has confirmed the attacks are valid as long as E2E adversary is involved, while those w/o E2E adversary seem to be thwarted with additional operations not described in the whitepaper, which is hard for us to verify at this point.

#### References

- 1 Tyler Curtiss. Encryption out of LINE Reverse engineering end-to-end encrypted messaging. Ekoparty 2016, 2016.
- 2 Antonio M. Espinoza, William J. Tolley, Jedidiah R. Crandall, Masashi Crete-Nishihata, and Andrew Hilt. Alice and bob, who the FOCI are they?: Analysis of end-to-end encryption in the LINE messaging application. In USENIX FOCI 17, USENIX Association, 2017.
- 3 LINE Corporation. LINE Encryption Overview, 2016.

### 3.36 Multiplication Operated Encryption with Trojan Resilience

Virginie Lallemand (*Ruhr-Universität Bochum, DE*)

**License** © Creative Commons BY 3.0 Unported license  
© Virginie Lallemand

**Joint work of** Olivier Bronchain, Sebastian Faust, Virginie Lallemand, Gregor Leander, Léo Perrin, François-Xavier Standaert

As most hardware design companies cannot afford having their own foundries, a common strategy consists in outsourcing the production of integrated circuits to external factories. If this solution allows to reduce the production costs, it brings up the problem of trust in the third party. One of the most feared threats in this respect goes under the name of hardware Trojan, defined as a malicious modification of the circuit design. Possible actions of Trojans include moves as devastating as key exfiltration. In this talk, we present a new block cipher construction designed especially to help addressing this problem: our proposal can be implemented using (mostly) untrusted low-cost chips and provides robustness more efficiently than by exploiting secret sharing and multi-party computation on a standard block cipher. Our concrete proposal is called MOE, acronym for “Multiplication Operated Encryption”: its round structure only consists in a modular multiplication and a multiplication with a binary matrix. These two operations being linear (with respect to different groups), they allow efficient secret sharing and a reduced hardware cost in comparison to previous solutions. One of our main contribution is the analysis of the cryptographic properties of the modular multiplication, an operation that was used back in the 90s (for the round structure of the ciphers IDEA and MMB for instance) but that to the best of our knowledge was never studied in detail.

### 3.37 Instantiating the Whitened Swap-Or-Not Construction

Nils Gregor Leander (*Ruhr-Universität Bochum, DE*)

**License** © Creative Commons BY 3.0 Unported license  
© Nils Gregor Leander

**Joint work of** Virginie Lallemand, Gregor Leander, Patrick Neumann, Friedrich Wiemer


We discussed how to instantiate the Whitened Swap-Or-Not Construction by S. Tessaro [1]. We first discussed some inherent limitations and restrictions before showing a first attempt how the framework could be instantiated.

#### References

- 1 Stefano Tessaro. Optimally Secure Block Ciphers from Ideal Primitives. ASIACRYPT (2) 2015: 437–462, Springer, 2015.

### 3.38 Better proofs for rekeying

*Daniel J. Bernstein (University of Illinois – Chicago, US)*


**License**  Creative Commons BY 3.0 Unported license  
 © Daniel J. Bernstein  
**URL** <https://blog.cr.yp.to/20170723-random.html>

The current mess of proofs of the cascade (FOCS 1996 Bellare–Canetti–Krawczyk), NMAC (Crypto 1996 Bellare–Canetti–Krawczyk), PRNGs (CCS 2005 Barak–Halevi), and NMAC again (Crypto 2006 Bellare) can be replaced by one simple tight multi-user security proof.

## 4 Panel discussions

### 4.1 Discussion on Mass Surveillance and the Real-World Impact of the Symmetric-Crypto Research Community

*Joan Daemen (Radboud University Nijmegen, NL, and STMicroelectronics – Diegem, BE)*

**License**  Creative Commons BY 3.0 Unported license  
 © Joan Daemen

On Friday morning there was a group discussion open for all seminar participants on a number of questions related to the real-world relevance of the symmetric crypto community and its research. Here a short summary of the outcome of these discussions. We thank Maria Eichlseder for input and taking notes during the discussion. The discussion centered around three themes.

The first theme was education of the general public. All agreed that it is impossible to protect our privacy and security without awareness. This is the case in general and applies specifically to the deployment of cryptography. Whether we, the symmetric cryptographic community, can actually have an impact here, is another thing. A good example is educating the general public about privacy (see mass surveillance, social media, etc.). However, privacy is a very subtle notion and even education on something much simpler as security has failed (see, e.g., how public key cryptography is deployed, or password policies, how people use passwords, etc.). Of course educating developers and policy makers would be easier maybe as they are professionals where a certain level of competence can be expected. Many of us are teaching at universities and there we can make a difference and hope our students will end up in policy-making positions. As a second aspect, the question was raised on what the main messages would be that we want to communicate. Or in other words, is there even a consensus (possible) in the academic community? For example, should companies be allowed to use private data in exchange for services (even after users have agreed to some terms of use)?


The second theme was about the education of protocol designers and programmers. The starting point was that there are many new standards being drafted even now and many repeat the same mistakes over and over again. Often the cryptographic knowledge of people in the standardization committees is very limited. There was discussion where different opinions were expressed and little agreement was reached. What we did agree on is that details of cryptosystems for public use should be made public, and be publicly analyzed. In the past, even public specifications have not always been carefully reviewed. Here the ‘provably secure’ WPA2, that was recently very badly broken, serves as a good example. As a possible reason for this miserable situation was given that there are ‘too many irrelevant standards’. This raised the question: which are the relevant standards that the cryptographic

community should focus on? The point was raised that NIST has usage data that could give us some guidance in this. Another interesting follow-up to this that was raised is that all are encouraged to contribute to updated versions of the ECRYPT CSA document Algorithms, Key Size and Protocol Report.

The third theme was the problem that an activity that is very important for the public and that requires specialized skills and great effort, that of building secure implementations, gives little academic reward. Here it was noted that papers reporting on implementations may be accepted at conferences such as FSE and there are also efforts to create sites with pointers to crypto libraries and tools.

## 4.2 Discussion on Robustness of CAESAR Candidates

*Damian Vizár (EPFL – Lausanne, CH)*

License  Creative Commons BY 3.0 Unported license  
© Damian Vizár

CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) explicitly names “robustness” as one of the desirable properties that an AE scheme should possess. The call for submissions mentions nonce-misuse resistance, and any candidate may target “any additional security goals and robustness goals that the submitters wish to point out”. However, no explicit minimal requirements concerning robustness were *requested* from the CAESAR candidates.

It is not clear whether there is any minimal degree of robustness that any candidate should possess, what kinds of robustness are relevant, and what importance should “robustness” play in the selection of CAESAR finalists. The goal of this discussion is to collect the opinions related to the role of robustness in CAESAR, and to attempt to find a consensus (or a compromise) for the answers to these questions.

### Summary of the Discussion

The initial questions of the discussion were the following:

1. What should be understood under “robustness” in the context of CAESAR?
2. Should there be a degree of “robustness” that is absolutely required from all candidates? (I.e. should there be any hard filtering based on “robustness”?)
3. If “robustness” is required, which particular properties is required, and what degree of resilience is required?

Even though the discussion did not converge to a clear answer to any of the three questions, it did generate a limited number of potential answers to these questions and further useful comments.

**On robustness itself.** As it was pointed out, the term “robustness” is not robust itself. We can mostly agree that informally, robustness means resilience against the improper use of a scheme (or more generally, as Barwell et al. put it “Robustness characterises the ability of a construct to be pushed right to the edge of its intended use case (and possibly beyond)”). Identifying a satisfyingly exact definition in the context of CAESAR seems difficult. These were the comments related to robustness:

- No scheme can be universally robust. There will always be misuse cases that trivially break any scheme (e.g. leaking the secret key in a silly way).

- Currently, robustness is evaluated through formal frameworks (MRAE, OAE, RAE and RUP in CAESAR) which each capture a very precise level of resilience against one or more specific types of misuse.
  - Schemes either claim security in the sense of one of these notions, or they give no guarantees and no information on what happens in case of the related misuse. This could thus be labelled explicit robustness.
- Another possible definition of robustness is that a robust scheme mitigates the damage done by a powerful attack that is outside of its security guarantees. E.g. a nonce based AEAD scheme that only suffers from a non-reusable decryption attack under nonce misuse is more robust (w.r.t. nonce misuse) than one that allows a low-complexity key recovery in the same setting. As this exact level of (in)security is not always advertised by the authors, this could be labelled e.g. implicit robustness.
  - For schemes that make the same claims w.r.t. to explicit robustness, the actual level of (in)security against a strong attack may differ greatly.
- Everyone agrees that side channel resistance is highly desirable. Everyone also agrees that, because side channel protection is platform and implementation-specific, it is best not to include it in this already complicated discussion.
  - It was agreed that the ease of protection against side channel attacks should not be mandatory for all candidates, but should be seen as a strong advantage.
  - Rendering side channel information useless by measures on the protocol level was proposed as a potential research avenue (e.g. using two independent authentication keys to verify firmware updates).

**Required level of robustness.** Especially in this point, no consensus could be reached. However, three general opinions recurred in the discussion:

- **The selection of the finalists should be conservative; the final portfolio should not contain schemes that suffer from devastating attacks, even though these may be outside of their guarantees.** E.g. exclude schemes that allow low-complexity recovery of the secret key or a secret state under nonce misuse. These were the arguments in favour of this opinion:
  - We have to assume that the users of CAESAR recommendations will be inexperienced. They may not understand or may ignore the usage conditions of the finalists. “The good engineers will not need the portfolio.”
  - There are bound to be cases of misuse, and we should try to mitigate the damage, at least for those kinds of misuse that we understand.
  - There are bound to be cases of (nonce) misuse, in which the devastating attacks may undermine the credibility of the symmetric cryptography. This will be the opposite effect of what CAESAR aims for.
  - The current pool of candidates contain schemes that do not suffer from devastating attacks, why not take those?
- **There should be no default level of robustness required from the candidates. We should not eliminate candidates based on a default robustness criterion.** These were the arguments in favour of this opinion:
  - It is enough that the finalists come with simple labels that clearly state what must and what must not be done to preserve security. It is the responsibility of the users to follow the (simple) instructions.
  - There are simple ways of making sure that the relevant misuse never occurs (e.g. device-specific prefixes in nonces).

- This was not demanded at the beginning, or during the competition. We should not introduce improvements over AES-GCM's robustness now.
- We already have the use cases to take care of this. In particular, this is not the primary concern in the "high-performance applications" use case.
- We cannot thwart every kind of misuse (e.g. using key as a random IV), thus we should not make particular forms of robustness compulsory.
- **Something in between.** There were two major proposals of the in-between kind:
  - **No default robustness requirement. Take into account the cryptanalysis, consider each case individually. Use the cryptanalysis to break ties.** The idea of using the results on exact (in)security of CAESAR candidates for breaking ties between similar schemes in the final decision process seemed to be generally well accepted.
  - **No default robustness requirement. When issuing final portfolio, give 2 kinds of labels to all finalists: (1) "regular schemes" and (2) "experts-only schemes" (or "brittle schemes").** The regular schemes would be those with no devastating low complexity nonce reuse attacks or nonce respecting birthday attacks. These would be recommended for a common user. The expert-only schemes would get a warning of dire consequences in case of misuse and their brittleness.

**The most desirable forms of robustness.** This point was not addressed in much detail, as the discussion focused mostly on the issue of having or not having default robustness requirement. However, most of the examples, counter examples and comments worked with nonce reuse.



## Participants

- Frederik Armknecht  
Universität Mannheim, DE
- Tomer Ashur  
KU Leuven, BE
- Christof Beierle  
Ruhr-Universität Bochum, DE
- Daniel J. Bernstein  
University of Illinois –  
Chicago, US
- Eli Biham  
Technion – Haifa, IL
- Alex Biryukov  
University of Luxembourg, LU
- Anne Canteaut  
INRIA – Paris, FR
- Joan Daemen  
Radboud University Nijmegen,  
NL, and STMicroelectronics –  
Diegem, BE
- Itai Dinur  
Ben Gurion University –  
Beer Sheva, IL
- Christoph Dobraunig  
TU Graz, AT
- Orr Dunkelman  
University of Haifa, IL
- Maria Eichlseder  
TU Graz, AT
- Henri Gilbert  
ANSSI – Paris, FR
- Tetsu Iwata  
Nagoya University, JP
- Jérémy Jean  
ANSSI – Paris, FR
- Dmitry Khovratovich  
University of Luxembourg, LU
- Stefan Kölbl  
Technical University of Denmark  
– Lyngby, DK
- Virginie Lallemand  
Ruhr-Universität Bochum, DE
- Tanja Lange  
TU Eindhoven, NL
- Nils Gregor Leander  
Ruhr-Universität Bochum, DE
- Gaëtan Leurent  
INRIA – Paris, FR
- Stefan Lucks  
Bauhaus-Universität Weimar, DE
- Willi Meier  
FH Nordwestschweiz –  
Windisch, CH
- Bart Mennink  
Radboud University  
Nijmegen, NL
- Vasily Mikhalev  
Universität Mannheim, DE
- Kazuhiko Minematsu  
NEC – Kawasaki, JP
- Nicky Mouha  
NIST – Gaithersburg, US
- Mridul Nandi  
Indian Statistical Institute –  
Kolkata, IN
- Maria Naya-Plasencia  
INRIA – Paris, FR
- Kaisa Nyberg  
Aalto University, FI
- Stav Perle  
Technion – Haifa, IL
- Léo Paul Perrin  
INRIA – Paris, FR
- Thomas Peyrin  
Nanyang TU – Singapore, SG
- Christian Rechberger  
TU Graz, AT
- Arnab Roy  
University of Bristol, GB
- Yu Sasaki  
NTT – Tokyo, JP
- Yannick Seurin  
ANSSI – Paris, FR
- Adi Shamir  
Weizmann Institute –  
Rehovot, IL
- Marc Stevens  
CWI – Amsterdam, NL
- Stefano Tessaro  
University of California –  
Santa Barbara, US
- Yosuke Todo  
NTT – Tokyo, JP
- Gilles Van Assche  
STMicroelectronics –  
Diegem, BE
- Damian Vizár  
EPFL – Lausanne, CH
- Meiqin Wang  
Shandong University – Jinan, CN
- Kan Yasuda  
NTT – Tokyo, JP

