

# Symmetric Cryptography

Edited by

Frederik Armknecht<sup>1</sup>, Helena Handschuh<sup>2</sup>, Tetsu Iwata<sup>3</sup>, and  
Bart Preneel<sup>4</sup>

**1** Universität Mannheim, DE, [armknecht@uni-mannheim.de](mailto:armknecht@uni-mannheim.de)

**2** Cryptography Research Inc. – San Francisco, US

**3** Nagoya University, JP, [iwata@cse.nagoya-u.ac.jp](mailto:iwata@cse.nagoya-u.ac.jp)

**4** K. U. Leuven, BE, [Bart.Preneel@esat.kuleuven.be](mailto:Bart.Preneel@esat.kuleuven.be)

---

## Abstract

From 05.01.2014 to 10.01.2014, the Seminar 14021 in Symmetric Cryptography was held in Schloss Dagstuhl – Leibniz Center for Informatics. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. The first section describes the seminar topics and goals in general. Links to extended abstracts or full papers are provided, if available.

**Seminar** January 5–10, 2014 – <http://www.dagstuhl.de/14021>

**1998 ACM Subject Classification** E.3 Data Encryption, C.2 Computer-Communications Networks – General – Security and Protection, D.4.6 Security and Protection, H Information Systems – Security

**Keywords and phrases** Authenticity, Integrity, Privacy, Hash Functions, Block Ciphers, Provable Security, Cryptanalysis

**Digital Object Identifier** 10.4230/DagRep.4.1.1

**Edited in cooperation with** Qingju Wang

## 1 Executive Summary

*Frederik Armknecht*

*Helena Handschuh*

*Tetsu Iwata*

*Bart Preneel*

**License** © Creative Commons BY 3.0 Unported license  
© Frederik Armknecht, Helena Handschuh, Tetsu Iwata and Bart Preneel

*Symmetric* cryptography deals with the case that both the sender and the receiver of a message are using the same key—the setting for symmetric encryption or authentication—as well as the case where there is no key at all—the setting for cryptographic hash functions. 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.” Although asymmetric cryptographic schemes provide in principle more flexibility, but are normally by orders of magnitude less efficient than symmetric cryptographic schemes. Thus, symmetric cryptosystems are the main workhorses of cryptography and highly relevant not only for academia, but also for industrial research, too.

The seminar was the fourth of its kind, the first one took place in 2007, the second in 2009, and the third in 2012. It concentrates on the design and analysis of



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

Symmetric Cryptography, *Dagstuhl Reports*, Vol. 4, Issue 1, pp. 1–16

Editors: Frederik Armknecht, Helena Handschuh, Tetsu Iwata, and Bart Preneel



Dagstuhl Reports

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

- *symmetric primitives* (block and stream ciphers, message authentication codes and hash functions), as well as
- *complex cryptosystems and cryptographic protocols* based on symmetric primitives.

One major topic was authenticated encryption. As already discussed at January 2012 Dagstuhl Seminar on Symmetric Cryptography, there is a demand for encryption schemes that ensure the confidentiality and integrity of data. This eventually led to an open cryptographic competition named CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness)<sup>1</sup> The goal of CAESAR is to identify a portfolio of authenticated ciphers that offer advantages over standard approaches like AES-GCM and (2) are suitable for widespread adoption. To this end cryptographic algorithm designers are invited to submit proposals of authenticated ciphers to CAESAR. All proposals will be made public for evaluation. As the deadline for first round submissions was in March 2014, i.e., only several weeks after the seminar, several groups were actively working on designing and analyzing new proposals for authenticated encryption schemes. Moreover, there was a discussion session that was mainly devoted to current CAESAR submissions. One result was a better understanding of necessary requirements and the current state of these schemes.

Another major topic was the analysis of Even-Mansour encryption schemes. Such schemes generalize common design approaches by reducing these to the composition of simple, idealized components like random permutations. Other topics focused during the discussion session include random number generation and provable security complex cryptosystems.

---

<sup>1</sup> See <http://competitions.cr.yp.to/caesar.html>.

## 2 Table of Contents

### Executive Summary

<i>Frederik Armknecht, Helena Handschuh, Tetsu Iwata and Bart Preneel . . . . .</i>	1
---	---

### Overview of Talks

Solving LWE with BKW <i>Martin R. Albrecht . . . . .</i>	5
On Increasing the Throughput of Stream Ciphers <i>Frederik Armknecht . . . . .</i>	5
NORX <i>Jean-Philippe Aumasson . . . . .</i>	6
New Mobile Authentication and Key Agreement Algorithm <i>Steve Babbage . . . . .</i>	6
Color Visual Cryptography with Scotch Tape and Polarizers <i>Alex Biryukov . . . . .</i>	6
Complexity of Statistical Attacks <i>Celine Blondeau . . . . .</i>	7
About non-uniformity in anti-DPA threshold implementations <i>Joan Daemen . . . . .</i>	7
Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64 <i>Itai Dinur . . . . .</i>	8
Key Recovery Attack against HMAC/NMAC with Reduced Whirlpool <i>Jian Guo . . . . .</i>	8
Black-box, White-box, and Public-key ASASA schemes <i>Dmitry Khovratovich . . . . .</i>	9
Tight Security Bounds for Triple Encryption <i>Jooyoung Lee . . . . .</i>	9
New Generic Attacks on Hash-based MACs <i>Gaetan Leurent . . . . .</i>	10
Pipelineable On-Line Encryption (POE) <i>Eik List . . . . .</i>	10
Near-collisions in stream ciphers <i>Willi Meier . . . . .</i>	11
APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography <i>Bart Mennink . . . . .</i>	11
Triple and Quadruple Encryption: Bridging the Gaps <i>Bart Mennink . . . . .</i>	12
Towards Finding Optimal Differential Characteristics for ARX: Application to Salsa20 <i>Nicky Mouha . . . . .</i>	12
LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations <i>Francois-Xavier Standaert . . . . .</i>	13

**4 14021 – Symmetric Cryptography**

Ketje and Keyak <i>Gilles Van Assche</i> . . . . .	13
Uniformity on a diet <i>Gilles Van Assche</i> . . . . .	13
Distance Bounding Protocols <i>Serge Vaudenay</i> . . . . .	14
Automatic Search for Differential Trails in ARX Ciphers <i>Vesselin Velichkov</i> . . . . .	14
Catena: A Memory-Consuming Password-Scrambling Framework <i>Jakob Wenzel</i> . . . . .	15
<b>Participants</b> . . . . .	<b>16</b>

## 3 Overview of Talks

### 3.1 Solving LWE with BKW

*Martin R. Albrecht (Technical University of Denmark – Lyngby, DK)*

**License** © Creative Commons BY 3.0 Unported license  
© Martin R. Albrecht

**Joint work of** Albrecht, Martin R.; Cid, Carlos; Faugère, Jean-Charles; Fitzpatrick, Robert; Perret, Ludovic  
**Main reference** M. R. Albrecht, J.-C. Faugère, R. Fitzpatrick, L. Perret, “Lazy Modulus Switching for the BKW Algorithm on LWE,” in Proc. of the 17th Int’l Conf. on Practice and Theory in Public-Key Cryptography (PKC’14), LNCS, Vol. 8383, pp. 429–445, Springer, 2014.

**URL** [http://dx.doi.org/10.1007/978-3-642-54631-0\\_25](http://dx.doi.org/10.1007/978-3-642-54631-0_25)

Some recent constructions based on LWE do not sample the secret uniformly at random but rather from some distribution which produces small entries. The most prominent of these is the binary-LWE problem where the secret vector is sampled from  $\{0, 1\}^*$  or  $\{-1, 0, 1\}^*$ . We present a variant of the BKW algorithm for binary-LWE and other small secret variants and show that this variant reduces the complexity for solving binary-LWE. We also give estimates for the cost of solving binary-LWE instances in this setting and demonstrate the advantage of this BKW variant over standard BKW and lattice reduction techniques applied to the SIS problem. Our variant can be seen as a combination of the BKW algorithm with a lazy variant of modulus switching which might be of independent interest.

### 3.2 On Increasing the Throughput of Stream Ciphers

*Frederik Armknecht (Universität Mannheim, DE)*

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

**Joint work of** Armknecht, Frederik; Mikhalev, Vasily  
**Main reference** F. Armknecht, V. Mikhalev, “On Increasing the Throughput of Stream Ciphers,” in Topics in Cryptology – Proc. of the Cryptographer’s Track at the RSA Conf. 2014 (CT-RSA’14), LNCS, Vol. 8366, pp. 132–151, Springer, 2014.

**URL** [http://dx.doi.org/10.1007/978-3-319-04852-9\\_7](http://dx.doi.org/10.1007/978-3-319-04852-9_7)

Important practical characteristics of a stream cipher are its throughput and its hardware size. A common hardware implementation technique for improving the throughput is to parallelize computations but this usually requires to insert additional memory cells for storing the intermediate results, hence at the expense of an increased hardware size.

For stream ciphers with feedback shift registers (FSRs), we present an alternative approach for parallelizing operations with almost no grow of the hardware size by cleverly re-using existing structures. It is based on the fact that FSRs are usually specified in Fibonacci configuration, meaning that at each clock-cycle all but one state entries are simply shifted. The idea is to temporarily store values of the stream cipher outside of the FSR, e.g., intermediate results of the output function, directly into the FSRs.

We formally describe the transformation and its preconditions and prove its correctness. Moreover, we demonstrate our technique on Grain-128, one of the eSTREAM finalists with low hardware size. Our technique allows implementations, realized by the Cadence RTL Compiler considering UMC L180 GII technology, where the throughput is increased in the initialization mode by 18% and in the keystream generation mode by 24%, when the compiler was set to optimize the timing, and by 20 % in both modes when the compiler was set to optimize the area. As opposed to other solutions, no additional memory is required. In fact the hardware size even decreased from 1794 GE to 1748 GE in the time- optimized implementation and only slightly increased from 1627 GE to 1656 GE in the area-optimized implementation.

### 3.3 NORX

*Jean-Philippe Aumasson (Kudelski Security, CH)*

**License**  Creative Commons BY 3.0 Unported license  
© Jean-Philippe Aumasson

**Joint work of** Aumasson, Jean-Philippe; Jovanovic, Philipp; Neves, Samuel

**Main reference** NORX, submission to the CAESAR competition, submitted for publication.

**URL** <https://norx.io>

NORX is a parallel and scalable authenticated encryption algorithm with associated data (AEAD). The cipher is not patented and will be freely available for all applications. Likewise, its source code will be put under a public domain licence.

### 3.4 New Mobile Authentication and Key Agreement Algorithm

*Steve Babbage (Vodafone Group – Newbury, GB)*

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

Steve is the chair of ETSI SAGE (Security Algorithms Group of Experts), the standards group that specifies cryptographic algorithms for the 3GPP family of mobile telecoms standards (GSM, GPRS, UMTS, LTE) amongst other things. This talk is about a new authentication and key agreement algorithm that has recently been designed and ratified as a 3GPP standard. We explain the context in which the new algorithm operates, the motivation for standardising a new algorithm, and the rationale behind its design. The new algorithm (called TUAK) is built using the Keccak-f [1600] sponge function.

#### References

- 1 3GPP. *Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions  $f_1$ ,  $f_1^*$ ,  $f_2$ ,  $f_3$ ,  $f_4$ ,  $f_5$  and  $f_5^*$ ; Document 1: Algorithm specification*. <http://www.3gpp.org/DynaReport/35231.htm>, 2013

### 3.5 Color Visual Cryptography with Scotch Tape and Polarizers

*Alex Biryukov (University of Luxembourg, LU)*

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

In this talk we have shown how to achieve color visual cryptography in practice without loss of resolution and contrast. Wide range of interference colors can be produced by placing variable thickness wave-plates between two crossed linear polarizers. We demonstrated simple arithmetic on this range of colors which can be used for symmetric encryption and secret sharing.

### 3.6 Complexity of Statistical Attacks

*Celine Blondeau (Aalto University, FI)*

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

**Joint work of** Blondeau, Céline; Nyberg, Kaisa

**Main reference** C. Blondeau, K. Nyberg, “Links Between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities,” in Proc. of 33rd Annual Int’l Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT’14), to appear.

The various number of apparently different statistical attacks on block ciphers has raised the question about their relationships which would allow to classify them and determine those that give essentially complementary information about the security of block ciphers. While mathematical links between some of these attacks have been derived in the last couple of years, in this talk we present a relation between truncated differential and multidimensional linear attacks. By studying the data, time and memory complexities of a multidimensional linear key-recovery attack and its relation with the truncated differential one, we also show that in most cases a known-plaintext attack can be transformed into a less costly chosen-plaintext attack. In particular, we present a differential attack on 26 rounds of PRESENT in the chosen-plaintext model with less memory complexity than the previous attack.

Part of this presentation is also dedicated to the statistical saturation attack. In particular, we show that this attack is the same as a truncated differential attack, which allows us, for the first time, to provide a justifiable analysis of the complexity of the statistical saturation attack and discuss its validity on 24 rounds of the PRESENT block cipher. The link between the known plaintext multidimensional linear attack and the chosen plaintext truncated differential one can be generalized to the other statistical attacks and give further examples of attacks where the method used to sample the data required by the statistical test is more differentiating than the method used for finding the distinguishing property.

This is a joint work with Kaisa Nyberg accepted at Eurocrypt 2014.

### 3.7 About non-uniformity in anti-DPA threshold implementations

*Joan Daemen (STMicroelectronics – Diegem, BE)*

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

**Joint work of** Daemen, Joan; Bertoni, Guido; Nikov, Ventsislav; Nikova, Svetla; Peeters, Michaël; Van Assche, Gilles

We study threshold sharing schemes against DPA and investigate in what way the failure to meet the uniformity condition may jeopardize the immunity against first-order DPA.

For this we introduce a treatment of discrete distributions and vector Boolean mappings in the spectral domain using the Walsh-Hadamard transform that is of independent interest. We identify the characteristic properties of discrete distributions and mappings that are important in the macroscopic analysis: the total imbalance and imbalance contribution. We show that the total imbalance of the result of applying an iterated mapping to an input is the sum of the imbalance of that input plus the sum of the imbalances of the rounds of the iterated mappings. In the microscopic analysis we make use of (reduced) correlation matrices and imbalance vectors that are inherent in lossy mappings.

We apply this theory on non-uniform sharing and use the one for Keccak as a test bench for our techniques. It turns out that quantitatively the entropy loss in the 3-share Keccak architecture is not a problem, but that at the microscopic level some anomalies should be fixed.

### 3.8 Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64

*Itai Dinur (ENS – Paris, FR)*

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

**Joint work of** Dinur, Itai; Dunkelman, Orr; Keller, Nathan; Shamir, Adi

**Main reference** I. Dinur, O. Dunkelman, N. Keller, A. Shamir, “Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64,” *Cryptology ePrint Archive: Report 2013/634*, 2013.

**URL** <http://eprint.iacr.org/2013/634>

In this paper, we present advanced meet-in-the-middle (MITM) attacks against the lightweight block cipher LED-64, improving the best known attacks on several step-reduced variants of the cipher in both single-key and related-key models. In particular, we present a known-plaintext attack on 2-step LED-64 with complexity of  $2^{48}$  and a related-key attack on 3-step LED-64 with complexity of  $2^{49}$ . In both cases, the previously known attacks have complexity of  $2^{60}$ , i.e., only 16 times faster than exhaustive key search.

While our attacks are applied to the specific scheme of LED-64, they contain several general methodological contributions: First, we present the linear key sieve technique, which allows to exploit linear dependencies between key bits to obtain filtering conditions in MITM attacks on block ciphers. While similar ideas have been previously used in the domain of hash functions, this is the first time that such a technique is applied in block cipher cryptanalysis. As a second contribution, we demonstrate for the first time that a splice-and-cut attack (which so far seemed to be an inherently chosen-plaintext technique) can be used in the known-plaintext model, with data complexity which is significantly below the code-book size. Finally, we extend the differential MITM attack on AES-based designs, and apply it independently in two stages from both sides of the cipher, while using the linear key sieve and other enhancements.

### 3.9 Key Recovery Attack against HMAC/NMAC with Reduced Whirlpool

*Jian Guo (Nanyang TU – Singapore, SG)*

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

**Joint work of** Guo, Jian; Sasaki, Yu; Wang, Lei; Wang, Meiqin; Wen, Long; Wu, Shuang

**Main reference** J. Guo, Y. Sasaki, L. Wang, S. Wu, “Cryptanalysis of HMAC/NMAC-Whirlpool,” in *Proc. of the 19th Int’l Conf. on the Theory and Application of Cryptology and Information Security – Part II (ASIACRYPT’13)*, LNCS, Vol. 8270, pp. 21–40, Springer, 2013.

**URL** [http://dx.doi.org/10.1007/978-3-642-42045-0\\_2](http://dx.doi.org/10.1007/978-3-642-42045-0_2)

We presented the first key recovery attack against HMAC instantiated with Whirlpool hash function. Combining the generic state recovery attack developed recently, and progress in preimage attacks against Whirlpool, we are able to recover the original key with Whirlpool reduced to 6 rounds, and equivalent keys for 7 rounds. The later was based on recent progress in the MITM attacks against AES and AES-like block ciphers.

This talk is based on two pieces of work:

1. Jian Guo, Yu Sasaki, Lei Wang, Shuang Wu: Cryptanalysis of HMAC/NMAC-Whirlpool. ASIACRYPT 2013.
2. Jian Guo, Yu Sasaki, Lei Wang, Meiqin Wang, Long Wen: Equivalent Key Recovery Attacks against HMAC and NMAC with Whirlpool Reduced to 7 Rounds. FSE 2014.



### 3.10 Black-box, White-box, and Public-key ASASA schemes

*Dmitry Khovratovich (University of Luxembourg, LU)*

License © Creative Commons BY 3.0 Unported license  
© Dmitry Khovratovich

Joint work of Khovratovich, Dmitry; Biryukov, Alex; Bouillaguet, Charles

The informal notion of white-box cryptography was coined by Chow et al. 2002 as a method to protect cryptographic keys in a public implementation of encryption algorithms, which is fully accessed by an adversary. White-box implementations of the AES and DES ciphers were presented, but they were all badly broken. Subsequent attempts were no better. Whereas some theoretical foundations of white-box cryptography have been given recently in Wyseur's PhD thesis, so far they have not lead to any practical scheme.

I present an overview of the white-box cryptography concept along with the most common applications and proposed designs. I try to answer the question if the security of a white-box scheme can be relied on public scrutiny in contrast to the hardness assumptions behind RSA and other public-key schemes.

Alongside the theoretical results, I present some well-known attempts to construct a white-box cryptographic scheme from the AES and DES ciphers, and show their inherent weaknesses. Finally, I discuss some potential methods to construct a secure white-box cipher from scratch. Our first construction uses the results from finite fields theory and public-key cryptography and satisfies the strongest notion of white-box security. The second construction introduces the concept of a memory-hard cipher, that consumes a specified amount of memory and prohibits the adversary from recovering a compact representation of the scheme.

### 3.11 Tight Security Bounds for Triple Encryption

*Jooyoung Lee (Sejong University – Seoul, KR)*

License © Creative Commons BY 3.0 Unported license  
© Jooyoung Lee

Main reference J. Lee, "Tight Security Bounds for Triple Encryption," Cryptology ePrint Archive: Report 2014/015, 2014.

URL <http://eprint.iacr.org/2014/015>

In this talk, we revisit the old problem asking the exact provable security of triple encryption in the ideal cipher model. For a blockcipher with key length  $k$  and block size  $n$ , triple encryption is known to be secure up to  $2^{k+\min\{k/2, n/2\}}$  queries, while the best attack requires  $2^{k+\min\{k, n/2\}}$  query complexity. So there is a gap between the upper and lower bounds for the security of triple encryption. We close this gap by proving the security up to  $2^{k+\min\{k, n/2\}}$  query complexity. With the DES parameters, triple encryption is secure up to  $2^{82.5}$  queries, greater than the current bound of  $2^{78.3}$  and comparable to  $2^{83.5}$  for 2-XOR-cascade.

We also analyze the security of two-key triple encryption, where the first and the third keys are identical. We prove that two-key triple encryption is secure up to  $2^{k+\min\{k, n/2\}}$  queries to the underlying block cipher and  $2^{\min\{k, n/2\}}$  queries to the outer permutation. For the DES parameters, this result is interpreted as the security of two-key triple encryption up to  $2^{32}$  plaintext-ciphertext pairs and  $2^{81.7}$  block cipher encryptions.

## References

- 1 Mihir Bellare and Phillip Rogaway, The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs, EUROCRYPT'06, LNCS, Vol. 4004, pp. 409–426, DOI: 10.1007/11761679\_25, Springer, 2006.
- 2 Peter Gazi and Ueli M. Maurer, Cascade Encryption Revisited, ASIACRYPT'09, LNCS, Vol. 5912, pp. 37–51, DOI: 0.1007/978-3-642-10366-7\_3, Springer, 2009.

## 3.12 New Generic Attacks on Hash-based MACs

*Gaetan Leurent (University of Louvain, BE)*

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

**Joint work of** Leurent, Gaetan; Peyrin, Thomas; Wang Lei

**Main reference** New Generic Attacks on Hash-based MACs, Asiacrypt 2013, LNCS 8270, pages 1-20

**URL** [http://dx.doi.org/10.1007/978-3-642-42045-0\\_1](http://dx.doi.org/10.1007/978-3-642-42045-0_1)

In this paper we study the security of hash-based MAC algorithms (such as HMAC and NMAC) above the birthday bound. Up to the birthday bound, HMAC and NMAC are proven to be secure under reasonable assumptions on the hash function. On the other hand, if an  $n$ -bit MAC is built from a hash function with a  $l$ -bit state ( $l < n$ ), there is a well-known existential forgery attack with complexity  $2^{l/2}$ . However, the remaining security after  $2^{l/2}$  computations is not well understood. In particular it is widely assumed that if the underlying hash function is sound, then a generic universal forgery attack should still require  $2^n$  computations and some distinguishing (e.g. distinguishing-H but not distinguishing-R) and state-recovery attacks should still require  $2^l$  (or  $2^k$  if  $k < l$ ) computations.

In this work, we show that above the birthday bound, hash-based MACs offer significantly less security than previously believed. Our main result is a generic distinguishing-H and state-recovery attack against hash-based MACs with a complexity of only  $\tilde{O}(2^{l/2})$ . In addition, we show a key-recovery attack with complexity  $\tilde{O}(2^{3l/4})$  against HMAC used with a hash functions with an internal checksum, such as GOST.

This surprising result shows that the use of checksum might actually weaken a hash function when used in a MAC. We stress that our attacks are generic, and they are in fact more efficient than some previous attacks proposed on concrete hash functions.

We use techniques similar to the cycle-detection technique proposed by Peyrin et al. at Asiacrypt 2012 to attack HMAC in the related-key model. However, our attack works in the single-key model for both HMAC/NMAC and without restriction on the key size.

## 3.13 Pipelineable On-Line Encryption (POE)

*Eik List (Bauhaus-Universität Weimar, DE)*

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

Correct authenticated decryption requires the receiver to buffer the decrypted message until the authenticity check has been performed. In high-speed networks, which must handle large message frames at low latency, this behavior becomes practically infeasible. This presentation proposes CCA-secure on-line ciphers as a practical alternative to AE schemes since the former

provide some defense against malicious message modifications. Unfortunately, all published on-line ciphers so far are either inherently sequential, or lack a CCA-security proof.

This paper introduces POE, a family of on-line ciphers that combines provable security against chosen-ciphertext attacks with pipelineability to support efficient implementations. POE combines a block cipher and an e-AXU family of hash functions. Different instantiations of POE are given, based on different universal hash functions and suitable for different platforms. Moreover, this presentation introduces POET, a provably secure on-line AE scheme, which inherits pipelineability and chosen-ciphertext-security from POE and provides additional resistance against nonce-misuse attacks.

### 3.14 Near-collisions in stream ciphers

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

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

**Joint work of** Zhang, Bin; Li Zhenqi; Meier, Willi

**Main reference** B. Zhang, Z. Li, “Near Collision Attacks on Grain v1m,” in Proc. of the 20th Int’l Workshop on Fast Software Encryption (FSE’13), to appear.

Near-collision attacks on the stream cipher Grain v1 have been proposed by Zhang and Li at FSE 2013. The main idea is to identify near-collision internal states of a stream cipher at different time instants, and to retrieve the internal state. The original attacks on Grain v1 were based on assumptions that seem hard to verify. An improved framework for near-collision analysis of Grain v1 is developed that does not rely on assumptions and has assured success probability. The analysis is based on newly detected properties of Grain v1 and is a dedicated time-memory-data tradeoff attack that has lower data requirements than generic time-memory-data tradeoffs on stream ciphers.

### 3.15 APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography

*Bart Mennink (KU Leuven, BE)*


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

**Joint work of** E. Andreeva, B. Bilgin, A. Bogdanov, A. Luykx, B. Mennink, N. Mouha, K. Yasuda, Kan, “APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography,” in Proc. of the 21st Int’l Workshop on Fast Software Encryption (FSE’14), to appear.

The domain of lightweight cryptography focuses on cryptographic algorithms for extremely constrained devices. It is very costly to avoid nonce reuse in such environments, because this requires either a hardware source of randomness, or non-volatile memory to store a counter. At the same time, a lot of cryptographic schemes actually require the nonce assumption for their security. In this paper, we propose APE as the first permutation-based authenticated encryption scheme that is resistant against nonce misuse. We formally prove that APE is secure, based on the security of the underlying permutation. To decrypt, APE processes the ciphertext blocks in reverse order, and uses inverse permutation calls. APE therefore requires a permutation that is both efficient for forward and inverse calls. We instantiate APE with the permutations of three recent lightweight hash function designs: Quark, Photon, and Spongnet. For any of these permutations, an implementation that supports both encryption and decryption requires less than 1.9 kGE and 2.8 kGE for 80-bit and 128-bit security levels, respectively.

### 3.16 Triple and Quadruple Encryption: Bridging the Gaps

*Bart Mennink (KU Leuven, BE)*

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

Triple encryption is a cascade of three block cipher evaluations with independent keys, in order to enlarge its key size. This design is proven secure up to approximately  $2^{\kappa + \min\{\kappa/2, n/2\}}$  queries (by Bellare and Rogaway, EUROCRYPT 2006, and Gaži and Maurer, ASIACRYPT 2009), where  $\kappa$  denotes the key size and  $n$  the block length of the underlying block cipher. On the other hand, the best known attack requires about  $2^{\kappa + n/2}$  queries (by Lucks, FSE 1998, and Gaži, CRYPTO 2013). These bounds are non-tight for  $\kappa \leq n$ . In this work, we close this gap. By strengthening the best known attack as well as tightening the security bound, we prove that triple encryption is tightly secure up to  $2^{\kappa + \min\{\kappa, n/2\}}$  queries. Additionally, we prove that the same tight security bound holds for quadruple encryption (which consists of four sequentially evaluated block ciphers), and derive improved security and attack bounds for cascades consisting of five or more rounds. This work particularly solves the longstanding open problem of proving tight security of the well-known Triple-DES construction in the ideal model.

### 3.17 Towards Finding Optimal Differential Characteristics for ARX: Application to Salsa20

*Nicky Mouha (KU Leuven, BE)*

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

**Joint work of** Mouha, Nicky; Preneel, Bart

**Main reference** N. Mouha, B. Preneel, “Towards Finding Optimal Differential Characteristics for ARX: Application to Salsa20,” Cryptology ePrint Archive: Report 2013/328, 2013.

**URL** <https://eprint.iacr.org/2013/328>

An increasing number of cryptographic primitives are built using the ARX operations: addition modulo  $2^n$ , bit rotation and XOR. Because of their very fast performance in software, ARX ciphers are becoming increasingly common. However, there is currently no rigorous understanding of the security of ARX ciphers against one of the most common attacks in symmetric-key cryptography: differential cryptanalysis. In this paper, we introduce a tool to search for optimal differential characteristics for ARX ciphers. Our technique is very easy to use, as it only involves writing out simple equations for every addition, rotation and XOR operation in the cipher, and applying an off-the-shelf SAT solver. As is commonly done for ARX ciphers, our analysis assumes that the probability of a characteristic can be computed by multiplying the probabilities of each operation, and that the probability of the best characteristic is a good estimate for the probability of the corresponding differential. Using extensive experiments for Salsa20, we find that these assumptions are not always valid. To overcome these issues, we propose a method to accurately estimate the probability of ARX differentials.

### 3.18 LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations

*Francois-Xavier Standaert (University of Louvain, BE)*

**License** © Creative Commons BY 3.0 Unported license  
 © Francois-Xavier Standaert  
**Joint work of** Standaert, Francois-Xavier; Vincent Grosso, Gaëtan Leurent and Kerem Varici  
**Main reference** V. Grosso, G. Leurent, F.-X. Standaert, K. Varici, “LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations,” in Proc. of the 21st Int’l Workshop on Fast Software Encryption (FSE’14), to appear; pre-print available from the author’s webpage.  
**URL** <http://perso.uclouvain.be/fstandae/PUBLIS/142.pdf>

Side-channel analysis is an important issue for the security of embedded cryptographic devices, and masking is one of the most investigated solutions to mitigate such attacks. In this context, efficient masking has recently been considered as a possible criteria for new block cipher designs. Previous proposals in this direction were applicable to different types of masking schemes (e.g. Boolean and polynomial). In this paper, we study possible optimizations when specializing the designs to Boolean masking. For this purpose, we first observe that bitslice ciphers have interesting properties for improving both the efficiency and the regularity of masked software implementations. Next we specify a family of block ciphers (denoted as LS-designs) that can systematically take advantage of bitslicing in a principled manner. Eventually, we evaluate both the security and performance of such designs and two of their instances, confirming excellent properties for physically secure applications.

### 3.19 Ketje and Keyak

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

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

In this presentation, we propose two variants of Keccak, called Ketje and Keyak, tailored for authenticated encryption. We focus on the design decisions behind these two proposals, which differ in the size of the state and consequently in the set of platforms they are best suited for: high-end platforms for Keyak and low-end platforms for Ketje.

Keyak uses the DuplexWrap construction, which is an improved version of SpongeWrap [SAC11]. Some of the Keyak instances are parallelizable, while others are serial. Cryptanalysis can be argued to be based on provable modes and a hermetic permutation.

Ketje uses a dedicated construction called MonkeyWrap. In contrast to Keyak, Ketje works at the round function level and cryptanalysis requires ad-hoc techniques for the function as a whole.

### 3.20 Uniformity on a diet

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

**License** © Creative Commons BY 3.0 Unported license  
 © Gilles Van Assche  
**Joint work of** Bilgin, Begül; Daemen, Joan; Nikov, Ventzislav; Nikova, Svetla; Rijmen, Vincent; Van Assche, Gilles  
**Main reference** B. Bilgin, J. Daemen, V. Nikov, S. Nikova, V. Rijmen, G. Van Assche, “Efficient and First-Order DPA Resistant Implementations of Keccak,” in Proc. of the 12th Smart Card Research and Advanced Application Conf. (CARDIS’13), to appear.

Besides hashing, Keccak can be used in many other modes, including ones operating on a secret value. Many applications of such modes require protection against side-channel

attacks, preferably at low cost. In this presentation, we present threshold implementations (TI) of Keccak with three and four shares that build further on unprotected parallel and serial architectures. We improve upon earlier TI implementations of Keccak in the sense that the latter did not achieve uniformity of shares. In our proposals we do achieve uniformity at the cost of an extra share in a four-share version or at the cost of injecting a small number of fresh random bits for each computed round. The proposed implementations are efficient and provably secure against first-order side-channel attacks.

### 3.21 Distance Bounding Protocols

*Serge Vaudenay (EPFL – Lausanne, CH)*

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

**Joint work of** Boureanu, Ioana; Mitrokotsa, Aikaterini; Vaudenay, Serge

**Main reference** Series of work presented at LATINCRYPT'12, FSE'13, LIGHTSEC'13, PROVSEC'13, ISC'13.

**URL** <http://lasec.epfl.ch/infoscience/>

Distance-bounding is the prominent solution to relay attacks against access control systems. In this talk, we review security models and existing protocols for distance-bounding. We identify two existing protocols with complete security results: SKI and FO. We compare them and identify open problems.

### 3.22 Automatic Search for Differential Trails in ARX Ciphers

*Vesselin Velichkov (University of Luxembourg, LU)*

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

**Joint work of** Biryukov, Alex; Velichkov, Vesselin

**Main reference** A. Biryukov, V. Velichkov, “Automatic Search for Differential Trails in ARX Ciphers”, in Topics in Cryptology – Proc. of the Cryptographer’s Track at the RSA Conf. 2014 (CT-RSA’14), LNCS, Vol. 8366, pp. 227–250, Springer, 2014; pre-print available at Cryptology ePrint Archive (Report 2013/328).

**URL** [http://dx.doi.org/10.1007/978-3-319-04852-9\\_12](http://dx.doi.org/10.1007/978-3-319-04852-9_12)

**URL** <http://eprint.iacr.org/2013/853>

In this talk we describe a tool for automatic search for differential trails in ARX (Addition, Rotation, XOR) ciphers. It is based on the well-known branch-and-bound technique, proposed by Mitsuru Matsui at EUROCRYPT’94 and used to find the best trails for up to 16 rounds of DES. Finding (near) optimal differential trails in symmetric-key primitives is critical for the accurate assessment of the security of the latter against one of the most powerful attacks – differential cryptanalysis. Being able to do this for ARX ciphers has always been a difficult problem. To the best of our knowledge this is the first application of Matsui’s algorithm to ciphers that do not have S-boxes, such as ARX.

In the first part of the talk we briefly describe Matsui’s algorithm and comment on the problems that arise when it is applied in its original form to ARX primitives. Next we present two solutions that address those problems: (1) partial difference distribution tables (pDDT) and (2) what we refer to as “The Highways and Country Roads Analogy”. The latter two are combined into a modified version of Matsui’s search technique called Threshold Search that is applicable to ARX.

Finally, we present results from the application of the threshold search tool to four ARX-based ciphers: TEA, XTEA, RAIDEN and SPECK. For TEA, the best trail found by our tool covers more than two times the number of rounds of the previous best (truncated) trail: 18 vs. 8. The best found trail for RAIDEN is 3-round iterative and covers all 32 rounds of the cipher. For three versions of the recently proposed cipher SPECK, namely SPECK-32/48/64, the best found trails cover 9, 10 and 13 rounds respectively. Those figures are comparable to a recent result by Abed et al. resp. 8, 10 and 13 rounds. The latter are however reported for differentials, while our results are for single trails. We also confirm the best known differential trail for XTEA that is on 14 rounds.

The source code of the tool is publicly available as part of a larger toolkit for the analysis of ARX at the following address: <https://github.com/vesselinux/yaarx>.

Extended version of the paper is available at IACR: <http://eprint.iacr.org/2013/853>.

### 3.23 Catena: A Memory-Consuming Password-Scrambling Framework

*Jakob Wenzel (Bauhaus-Universität Weimar, DE)*

License  Creative Commons BY 3.0 Unported license  
© Jakob Wenzel

It is a common wisdom that servers should better store the one-way hash of their clients' passwords, rather than storing the password in the clear. In this paper we introduce a set of functional properties a key-derivation function (password scrambler) should have. Unfortunately, none of the existing algorithms satisfies our requirements. Therefore, we introduce a novel and provably secure password-scrambling framework called Catena and derive an instantiation based, namely Catena- $\lambda$ , which is based on a memory-consuming one-way function called  $\lambda$ -bit-reversal graph ( $\lambda$ -BRG). It is characterized by its memory hardness, i.e., if one has only  $1/c$  of memory available, one needs  $c^\lambda$  processor units to gain the same time-memory trade-off. Thus, Catena- $\lambda$  excellently thwarts massively parallel attacks on cheap memory-constrained hardware, such as recent graphical processing units (GPUs). Additionally, we show that Catena- $\lambda$  is also a good key derivation function, since in the random oracle model it is indistinguishable from a random function. Furthermore, the memory access pattern of the  $\lambda$ -BRG is password-independent and therefore resistance against cache-timing attacks. Moreover, Catena supports (1) client-independent updates (the server can increase the security parameters and update the password hash without user interaction or knowing the password), (2) a server relief protocol (saving the server's resources at the cost of the client), and (3) a variant Catena-KG for secure key derivation (to securely generate many cryptographic keys of arbitrary lengths such that compromising some keys does not help to break others).



## Participants

- Martin R. Albrecht  
Technical Univ. of Denmark – Lyngby, DK
- Elena Andreeva  
KU Leuven, BE
- Frederik Armknecht  
Universität Mannheim, DE
- Tomer Ashur  
KU Leuven, BE
- Jean-Philippe Aumasson  
Kudelski Security, CH
- Steve Babbage  
Vodafone Group – Newbury, GB
- Daniel J. Bernstein  
University of Chicago, US
- Eli Biham  
Technion – Haifa, IL
- Alex Biryukov  
University of Luxembourg, LU
- Céline Blondeau  
Aalto University, FI
- Andrey Bogdanov  
Technical Univ. of Denmark, DK
- Carlos Cid  
Royal Holloway University of London, GB
- Joan Daemen  
STMicroelectronics – Diegem, BE
- Itai Dinur  
ENS – Paris, FR
- Orr Dunkelman  
University of Haifa, IL
- Henri Gilbert  
ANSSI – Paris, FR
- Jian Guo  
Nanyang TU – Singapore, SG
- Tetsu Iwata  
Nagoya University, JP
- Pascal Junod  
HEIG-VD – Yverdon-les-Bains, CH
- Dmitry Khovratovich  
University of Luxembourg, LU
- Matthias Krause  
Universität Mannheim, DE
- Tanja Lange  
TU Eindhoven, NL
- Nils Gregor Leander  
Ruhr-Universität Bochum, DE
- Jooyoung Lee  
Sejong University – Seoul, KR
- Gaetan Leurent  
University of Louvain, BE
- Eik List  
Bauhaus-Universität Weimar, DE
- Stefan Lucks  
Bauhaus-Universität Weimar, DE
- Willi Meier  
FH Nordwestschweiz – Windisch, CH
- Florian Mendel  
TU Graz, AT
- Bart Mennink  
KU Leuven, BE
- Nicky Mouha  
KU Leuven, BE
- Kaisa Nyberg  
Aalto University, FI
- Kenneth G. Paterson  
Royal Holloway University of London, GB
- Thomas Peyrin  
Nanyang TU – Singapore, SG
- Bart Preneel  
KU Leuven, BE
- Christian Rechberger  
Technical Univ. of Denmark – Lyngby, DK
- Greg Rose  
Qualcomm Inc. – San Diego, US
- Yu Sasaki  
NTT Labs – Tokyo, JP
- Francois-Xavier Standaert  
University of Louvain, BE
- John Steinberger  
Tsinghua Univ. – Beijing, CN
- Gilles Van Assche  
STMicroelectronics – Diegem, BE
- Serge Vaudenay  
EPFL – Lausanne, CH
- Vesselin Velichkov  
University of Luxembourg, LU
- Qingju Wang  
KU Leuven, BE
- Jakob Wenzel  
Bauhaus-Universität Weimar, DE
- Kan Yasuda  
NTT Labs. – Tokyo, JP

