

Symmetric Cryptography

Edited by

Frederik Armknecht¹, Stefan Lucks², Bart Preneel³, and
Phillip Rogaway⁴

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

2 Bauhaus-Universität Weimar, DE, stefan.lucks@uni-weimar.de

3 K.U. Leuven, BE, Bart.Preneel@esat.kuleuven.be

4 University of California, Davis, US, rogaway@cs.ucdavis.edu

Abstract

From 15.01.2012 to 20.01.2012, the Seminar 12031 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 15.–20. January, 2012 – www.dagstuhl.de/12031

1998 ACM Subject Classification E.3 Data Encryption.

Keywords and phrases Hash functions, Feistel networks, BLAKE, KLEIN, Keccak, IDEA, GCM, EAXprime, TLS, KISS

Digital Object Identifier 10.4230/DagRep.2.1.39

Edited in cooperation with Ewan Fleischmann


1 Executive Summary

Frederik Armknecht

Stefan Lucks

Bart Preneel

Phillip Rogaway

License  Creative Commons BY-NC-ND 3.0 Unported license
© Armknecht, Frederik; Lucks, Stefan; Preneel, Bart; Rogaway, Phillip

Research in Symmetric Cryptography is quickly evolving. The seminar was the third of its kind, the first one took place in 2007, the second in 2009. We observe a steadily increasing interest in Symmetric Cryptography, as well as a growing practical demand for symmetric algorithms and protocols. The seminar was very successful in discussing recent results and sharing new ideas. Furthermore, it inspired the participants to consider how Symmetric Cryptography has evolved in the past, and how they would like it to evolve in the future.

Two intense discussions dealt with Authenticated Encryption and the issue of a 'valid' attack on a symmetric primitive. The participants agreed on Authenticated Encryption becoming a major research topic for Symmetric Cryptography in the next few years, because current Authenticated Encryption Schemes are not always suitable for practical demands – especially are the relevant attack modes and models not yet well-understood (e.g., misuse attacks, blockwise adaptive attacks, etc.). Regarding the issue of 'valid' attacks, the participants



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

Symmetric Cryptography, *Dagstuhl Reports*, Vol. 2, Issue 1, pp. 39–49

Editors: Frederik Armknecht, Stefan Lucks, Bart Preneel, and Phillip Rogaway



DAGSTUHL
REPORTS

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

agreed that the current development of academic cryptanalysis with a growing number of increasingly 'marginal' attacks, is unsatisfactory.

2 Table of Contents

Executive Summary

Armknecht, Frederik; Lucks, Stefan; Preneel, Bart; Rogaway, Phillip 39

Overview of Talks

BLAKE SIMD: past, present, future

Jean-Philippe Aumasson 42

Attacking KLEIN

Jean-Philippe Aumasson 42

Practical Collisions in Round-Reduced Keccak

Itai Dinur 43

Getting Results under Weak Expectations

Yevgeniy Dodis 43

An IDEA to Consider

Orr Dunkelman 43

Oracle Reducibility of Hash Functions

Marc Fischlin 44

GCM Security, Revisited

Tetsu Iwata 44

Cryptanalysis of EAXprime

Tetsu Iwata 45

On The Distribution of Linear Biases: Three Instructive Examples

Gregor Leander 45

New Results on EAX-Prime

Stefan Lucks 46

The Preimage Security of Double-Block-Length Compression Functions

Frederik Armknecht 46

Tag Size Does Matter: Attacks and Proofs for the TLS Record Protocol

Kenneth G. Paterson 46

KISS: A Bit Too Simple

Greg Rose 47

Bounds for Balanced Feistel Networks

Kyoji Shibutani 47

Collisions are not Incidental: A Compression Function Exploiting Discrete Geometry


Martijn Stam 48

Participants 49

3 Overview of Talks

3.1 BLAKE SIMD: past, present, future

Jean-Philippe Aumasson (Nagravision – Cheseaux, CH)

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

Joint work of Aumasson, Jean-Philippe; Neves, Samuel


Main reference Third SHA-3 Conference (to appear)

The SHA-3 candidate hash function BLAKE is based on a keyed permutation whose data-level parallelism allows implementers to exploit SIMD instructions sets, as available in popular general-purpose processors. We will first review previous implementations that used Intel’s streaming SIMD extensions (SSE), as well as recent implementations using ARM’s NEON SIMD instruction set.

We will then present the recent 256-bit-wide AVX and the upcoming AVX2 extensions (expected in 2013 in Intel’s Haswell microarchitecture) and how we used them to write new assembly implementations of BLAKE.

3.2 Attacking KLEIN

Jean-Philippe Aumasson (Nagravision – Cheseaux, CH)

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

Joint work of Aumasson, Jean-Philippe; María Naya-Plasencia; Markku-Juhani O. Saarinen

Main reference J.-P. Aumasson, M. Naya-Plasencia, M.-J. O. Saarinen, “Practical Attack on 8 Rounds of the Lightweight Block Cipher KLEIN,” INDOCRYPT 2011, pp. 134–145, LNCS, vol. 7107, Springer, 2011.

URL http://dx.doi.org/10.1007/978-3-642-25578-6_11

KLEIN is a family of lightweight block ciphers presented at RFIDSec 2011 that combines a 4-bit Sbox with Rijndael’s byte-oriented MixColumn. This approach allows compact implementations of KLEIN in both low-end software and hardware. We show that interactions between those two components lead to the existence of differentials of unexpectedly high probability: using an iterative collection of differential characteristics and neutral bits in plaintexts, we find conforming pairs for four rounds with amortized cost below 2^{12} encryptions, whereas at least 2^{30} was expected by the preliminary analysis of KLEIN. We exploit this observation by constructing practical ($\approx 2^{35}$ encryptions), experimentally verified, chosen-plaintext key-recovery attacks on up to 8 rounds of KLEIN-64 – the instance of KLEIN with 64-bit keys and 12 rounds. We also investigate the extension of the attack to 9 rounds.

3.3 Practical Collisions in Round-Reduced Keccak

Itai Dinur (Weizmann Institute – Rehovot, IL)

License © © ⊖ Creative Commons BY-NC-ND 3.0 Unported license
© Itai Dinur

Main reference I. Dinur, O. Dunkelman, A. Shamir, “New attacks on Keccak-224 and Keccak-256,” Cryptology ePrint Archive: Report 2011/624.

URL <http://eprint.iacr.org/2011/624.pdf>

The Keccak hash function is one of the five finalists in NIST’s SHA-3 competition, and so far it showed remarkable resistance against practical collision finding attacks: After several years of cryptanalysis and a lot of effort, the largest number of Keccak rounds for which actual collisions were found was only 2.

We describe improved collision finding techniques which enable us to double this number. More precisely, we can now find within a few minutes on a single PC actual collisions in standard Keccak-224 and Keccak-256, where the only modification is to reduce their number of rounds to 4. When we apply our techniques to 5-round Keccak, we can get in a few days excellent near collisions, where the Hamming distance is 5 in the case of Keccak-224 and 10 in the case of Keccak-256. Our new attack combines differential and algebraic techniques, and uses the fact that each round of Keccak is only a quadratic mapping in order to efficiently find pairs of messages which follow a high probability differential characteristic.

3.4 Getting Results under Weak Expectations

Yevgeniy Dodis (New York University, US)

License © © ⊖ Creative Commons BY-NC-ND 3.0 Unported license
© Yevgeniy Dodis

Recently, there has been renewed interest in basing cryptographic primitives on weak secrets, where the only information about the secret is some non-trivial amount of (min-)entropy.

From a formal point of view, such results require to upper bound the expectation of some function $f(X)$, where X is a weak source in question. We show an elementary inequality which essentially upper bounds such “weak expectation” by two terms, the first of which is *independent* of f , while the second only depends on the “variance” of f under *uniform* distribution. Quite remarkably, as relatively simple corollaries of this elementary inequality, we obtain some “unexpected” results, in several cases noticeably simplifying/improving prior techniques for the same problem. Examples include non-malleable extractors, leakage-resilient symmetric encryption, seed-dependent condensers and improved entropy loss for the leftover hash lemma.

3.5 An IDEA to Consider

Orr Dunkelman (University of Haifa, IL)

License © © ⊖ Creative Commons BY-NC-ND 3.0 Unported license
© Orr Dunkelman

Joint work of Biham, Eli; Keller, Nathan; Shamir, Adi


IDEA is a 64-bit block cipher with 128-bit keys which is widely used due to its inclusion in several cryptographic packages such as PGP. After its introduction by Lai and Massey in

1991, it was subjected to an extensive cryptanalytic effort, but so far the largest variant on which there are any published attacks contains only 6 of its 8.5-rounds. The first 6-round attack, described in the conference version of this paper in 2007, was extremely marginal: It required essentially the entire codebook, and saved only a factor of two compared to the time complexity of exhaustive search.

In 2009, Sun and Lai reduced the data complexity of the 6-round attack from 2^{64} to 2^{49} chosen plaintexts and simultaneously reduced the time complexity from 2^{127} to $2^{112.1}$ encryptions. In this revised version of our paper, we combine a highly optimized meet-in-the-middle attack with a keyless version of the Biryukov-Demirci relation to obtain new key recovery attacks on reduced-round IDEA, which dramatically reduce their data complexities and increase the number of rounds to which they are applicable. In the case of 6-round IDEA, we need only two known plaintexts (the minimal number of 64-bit messages required to determine a 128-bit key) to perform full key recovery in $2^{123.4}$ time. By increasing the number of known plaintexts to sixteen, we can reduce the time complexity to $2^{111.9}$, which is slightly faster than the Sun and Lai data-intensive attack. By increasing the number of plaintexts to about one thousand, we can now attack 6.5 rounds of IDEA, which could not be attacked by any previously published technique. By pushing our techniques to extremes, we can attack 7.5 rounds using 2^{63} plaintexts and 2^{114} time, and by using an optimized version of a distributive attack, we can reduce the time complexity of exhaustive search on the full 8.5-round IDEA to $2^{126.8}$ encryptions using only 16 plaintexts.

3.6 Oracle Reducibility of Hash Functions

Marc Fischlin (TU Darmstadt, DE)


License  Creative Commons BY-NC-ND 3.0 Unported license
© Marc Fischlin

Recently, Baecher and Fischlin (Crypto 2011) used the notion of random oracle reducibility to relate the random oracles in different schemes. Roughly, a random oracle in a scheme B reduces to that in another scheme A if any (oracle-based or standard-model based) instantiation of the hash function making scheme A secure, also makes scheme B secure.

Here we discuss that the same idea applies to other oracle objects such as the ideal cipher model. In particular, we look at the constructions of hash functions (resp. compression functions) out of ideal ciphers, and how the ideal ciphers in different constructions such as the PGV schemes, or (Tandem-)DM compared to Hirose, relate. Our results concerning reducibility are partially positive, and in some cases negative, showing that the hash function constructions rely on different properties of the cipher.

3.7 GCM Security, Revisited

Tetsu Iwata (Nagoya University, JP)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Tetsu Iwata

Joint work of Iwata, Tetsu; Ohashi, Keisuke; Minematsu, Kazuhiko

GCM is the authenticated encryption mode developed by McGrew and Viega. In 2007, GCM was adopted as a recommendation mode by NIST, and it is widely used in practice.

The designers presented proofs of security, and despite extensive security analyses by the cryptographic community, its provable security results are considered to be sound.

In this talk, we revisit the provable security results of GCM, and discuss in detail their correctness.

3.8 Cryptanalysis of EAXprime

Tetsu Iwata (Nagoya University, JP)

License © © ⊖ Creative Commons BY-NC-ND 3.0 Unported license
© Tetsu Iwata

Joint work of Minematsu, Kazuhiko; Morita, Hiraku; Iwata, Tetsu

Main reference K. Minematsu, S. Lucks, H. Morita, T. Iwata, “Cryptanalysis of EAXprime,” Cryptology ePrint Archive: Report 2012/018.

URL eprint.iacr.org/2012/018.pdf

EAX’ (EAXprime) is an authenticated encryption (AE) specified by ANSI C12.22 as a standard security function used for a smart grid. EAX’ is based on EAX, a provably secure AE proposed by Bellare, Rogaway, and Wagner.

In this talk, we present simple and efficient forgery and distinguishing attacks against EAX’ using one-block cleartext and plaintext.

3.9 On The Distribution of Linear Biases: Three Instructive Examples

Gregor Leander (Technical University of Denmark – Lyngby, DK)

License © © ⊖ Creative Commons BY-NC-ND 3.0 Unported license
© Gregor Leander


Joint work of Abdelraheem, Mohamed Ahmed; Ågren, Martin; Beelen, Peter; Leander, Gregor

Despite the fact that we evidently have very good block ciphers at hand today, many fundamental questions on their security are still unsolved.

One such fundamental problem is to precisely assess the security of a given block cipher with respect to linear cryptanalysis. In by far most of the cases we have to make (clearly wrong) assumptions, e.g., assume independent round-keys. Besides being unsatisfactory from a scientific perspective, the lack of fundamental understanding has a direct consequence on the performance of the ciphers we use. As we do not understand the security sufficiently enough, we are forced to embed a security margin – from an efficiency perspective nothing else than wasted performance. The aim of this paper is to stimulate research on the fundamental lack of understanding of block ciphers. We do this by presenting three examples of ciphers that behave differently to what is normally assumed. Thus, on the one hand these examples serve as counter examples to common beliefs and on the other hand serve as a guideline for future work.

3.10 New Results on EAX-Prime

Stefan Lucks (Bauhaus-Universität Weimar, DE)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Stefan Lucks


Main reference K. Minematsu, S. Lucks, H. Morita, T. Iwata, “Cryptanalysis of EAXprime,” Cryptology ePrint Archive: Report 2012/018.

URL eprint.iacr.org/2012/018.pdf

Starting from previous results presented by Tetsu Iwata at this Seminar, we present an improved cryptanalysis of EAX-Prime. The main observation is that the forgery attacks presented by Tetsu can be extended and turned into Chosen Ciphertext Message Recovery Attacks. These results have been found during the Seminar.

3.11 The Preimage Security of Double-Block-Length Compression Functions

Frederik Armknecht (University Mannheim, DE)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Frederik Armknecht

Joint work of Fleischmann, Ewan; Krause, Matthias; Lee, Jooyoung; Stam, Martijn; Steinberger, John P.


Main reference F. Armknecht, E. Fleischmann, M. Krause, J. Lee, M. Stam, J. Steinberger, “The Preimage Security of Double-Block-Length Compression Functions,” ASIACRYPT 2011, pp. 233–251, LNCS, vol. 7073, Springer, 2011.

URL http://dx.doi.org/10.1007/978-3-642-25385-0_13

We present new techniques for deriving preimage resistance bounds for block cipher based double-block-length, double-call hash functions. We give improved bounds on the preimage security of the three ‘classical’ double-block-length, double-call, block cipher-based compression functions, these being Abreast-DM, Tandem-DM and Hirose’s scheme. For Hirose’s scheme, we show that an adversary must make at least 2^{2n-5} block cipher queries to achieve chance 0.5 of inverting a randomly chosen point in the range. For Abreast-DM and Tandem-DM we show that at least 2^{2n-10} queries are necessary. These bounds improve upon the previous best bounds of $\Omega(2^n)$ queries, and are optimal up to a constant factor since the compression functions in question have range of size 2^{2n} .

3.12 Tag Size Does Matter: Attacks and Proofs for the TLS Record Protocol

Kenneth G. Paterson (RHUL – London, GB)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Kenneth G. Paterson

Joint work of Paterson, Kenneth G.; Ristenpart, Tom; Shrimpton, Tom

Main reference K.G. Paterson, T.E. Shrimpton, T. Ristenpart, “Tag Size Does Matter: Attacks and Proofs for the TLS Record Protocol,” Asiacypt 2011, pp. 372-389, LNCS, vol. 7073, Springer, 2011.

URL http://dx.doi.org/10.1007/978-3-642-25385-0_20





We analyze the security of the TLS Record Protocol, a MAC-then-Encode-then-Encrypt (MEE) scheme whose design targets confidentiality and integrity for application layer communications on the Internet. Our main results are twofold. First, we give a new distinguishing

attack against TLS when variable length padding and short (truncated) MACs are used. This combination will arise when standardized TLS 1.2 extensions (RFC 6066) are implemented.

Second, we show that when tags are longer, the TLS Record Protocol meets a new length-hiding authenticated encryption security notion that is stronger than IND-CCA.

3.13 KISS: A Bit Too Simple

Greg Rose (Qualcomm Inc. – San Diego, US)

License     Creative Commons BY-NC-ND 3.0 Unported license
© Greg Rose





Main reference G. Rose, “KISS: A Bit Too Simple,” Cryptology ePrint Archive: Report 2011/007.

URL <http://eprint.iacr.org/2011/007.pdf>

KISS (‘Keep it Simple Stupid’) is an efficient pseudo-random number generator specified by G. Marsaglia and A. Zaman in 1993. G. Marsaglia in 1998 posted a C version to various USENET newsgroups, including `sci.crypt`. Marsaglia himself has never claimed cryptographic security for the KISS generator, but many others have made the intellectual leap and claimed that it is of cryptographic quality. In this paper we show a number of reasons why the generator does not meet the KISS authors’ claims, why it is not suitable for use as a stream cipher, and that it is not cryptographically secure. Our best attack requires about 70 words of generated output and a few hours of computation to recover the initial state. A further attack on a newer version of KISS is also presented.

3.14 Bounds for Balanced Feistel Networks




Kyoji Shibutani (Sony – Tokyo, JP)

License     Creative Commons BY-NC-ND 3.0 Unported license
© Kyoji Shibutani

Feistel ciphers are among the most popular block cipher constructions in use today. We explore the optimality of balanced Feistel networks with SP-type F-functions with respect to their resistance against differential and linear cryptanalysis. Instantiations of Feistel ciphers with the wide class of (SP)u and (SP)uS F-functions is considered: One F-function can contain an arbitrary number of S-box layers interleaved with linear diffusion. For the matrices with maximum diffusion, it is proven that SPS and SPSP F-functions are optimal in terms of the proportion of active S-boxes in all S-boxes – a common efficiency metric for substitution-permutation ciphers. Interestingly, one SP-layer in the F-function is not enough to attain optimality whereas taking more than two S-box layers does not increase the efficiency either.

3.15 Collisions are not Incidental: A Compression Function Exploiting Discrete Geometry

Martijn Stam (University of Bristol, GB)

License    Creative Commons BY-NC-ND 3.0 Unported license

© Martijn Stam

Joint work of Jetchev, Dimitar; Özen, Onur; Stam, Martijn

We present a new construction of a compression function $h: \{0, 1\}^{3n} \rightarrow \{0, 1\}^{2n}$ that uses two parallel calls to an ideal primitive (an ideal blockcipher or a public random function) from $2n$ to n bits. This is similar to the well-known MDC-2 or the recently proposed MJH by Lee and Stam (CT-RSA'11). However, unlike these constructions, we show already in the compression function that an adversary limited (asymptotically in n) to $O(2^{2n(1-\delta)/3})$ queries (for any $\delta > 0$) has disappearing advantage to find collisions.

A key component of our construction is the use of the Szemerédi–Trotter theorem over finite fields to bound the number of full compression function evaluations an adversary can make, in terms of the number of queries to the underlying primitives.

Moreover, for the security proof we rely on a new abstraction that refines and strengthens existing techniques.

We believe that this framework elucidates existing proofs and we consider it of independent interest.

Participants

- Elena Andreeva
K.U. Leuven, BE
- Frederik Armknecht
Universität Mannheim, DE
- Jean-Philippe Aumasson
Nagravision – Cheseaux, CH
- Daniel J. Bernstein
Univ. of Illinois – Chicago, US
- Eli Biham
Technion – Haifa, IL
- Alex Biryukov
University of Luxembourg, LU
- Andrey Bogdanov
K.U. Leuven, BE
- Joan Daemen
STMicroelectronics –
Zaventem, BE
- Itai Dinur
Weizmann Inst. – Rehovot, IL
- Yevgeniy Dodis
New York University, US
- Orr Dunkelman
University of Haifa, IL
- Marc Fischlin
TU Darmstadt, DE
- Ewan Fleischmann
Bauhaus-Universität Weimar, DE
- Christian Forler
Bauhaus-Universität Weimar, DE
- Matthias Hamann
Universität Mannheim, DE
- Tetsu Iwata
Nagoya University, JP
- Antoine Joux
University of Versailles, FR
- Lars Ramkilde Knudsen
Technical Univ. of Denmark –
Lyngby, DK
- Matthias Krause
Universität Mannheim, DE
- Rudolphe Lampe
University of Versailles, FR
- Gregor Leander
Technical Univ. of Denmark –
Lyngby, DK
- Stefan Lucks
Bauhaus-Universität Weimar, DE
- Florian Mendel
K.U. Leuven, BE
- Vasily Mikhalev
Universität Mannheim, DE
- Tilo Müller
Univ. Erlangen-Nürnberg, DE
- Maria Naya-Plasencia
University of Versailles, FR
- Kaisa Nyberg
Aalto University, FI
- Jacques Patarin
University of Versailles, FR
- Kenneth G. Paterson
RHUL – London, GB
- Bart Preneel
K.U. Leuven, BE
- Christian Rechberger
ENS – Paris, FR
- Phillip Rogaway
Univ. of California – Davis, US
- Sondre Ronjom
NSM Norway, NO
- Greg Rose
Qualcomm Inc. – San Diego, US
- Yu Sasaki
NTT Labs. – Tokyo, JP
- Adi Shamir
Weizmann Inst. – Rehovot, IL
- Kyoji Shibusaki
Sony – Tokyo, JP
- Martijn Stam
University of Bristol, GB
- John Steinberger
Univ. of British Columbia, CA
- Deniz Toz
K.U. Leuven, BE
- Kerem Varici
K.U. Leuven, BE
- Bogdan Warinschi
University of Bristol, GB
- Jakob Wenzel
Bauhaus-Universität Weimar, DE
- Kan Yasuda
NTT Labs. – Tokyo, JP
- Erik Zenner
Hochschule Offenburg, DE

