In today's world computers are ubiquitous. They can be found in virtually any industry and most households own at least one personal computer or have a mobile phone. Apart from these fairly large and complex devices, we also see computers on a much smaller scale appear in everyday objects in the form of micro-controllers and RFID chips.

What truly transformed our society are large scale networks, like the Internet or mobile telephone networks, which can link billions of devices. Our ways of communicating and conducting business have severely changed over the last decades due to this development. However, most of this communication happens over inherently insecure channels requiring methods to protect our communication. A further issue is the vast amount of data generated, which raises serious privacy concerns.

Cryptography provides the key components for protecting our communication. From securing our passwords and personal data to protecting mobile communication from eavesdroppers and our electronic bank transactions from manipulation. These applications would be impossible without cryptography.

The main topic of this thesis is the design and security analysis of the most fundamental algorithms used in cryptography, namely block ciphers and cryptographic hash functions. These algorithms are the building blocks for a vast amount of applications and play a vital role in providing both confidentiality and integrity for our communication.

This work is organized in two parts. First, an introduction to block ciphers and cryptographic hash functions is given to provide an overview over the state-of-the-art, the terminology, and how we can evaluate the security of an algorithm. The second part is a collection of scientific publications that have been written during the PhD studies and published.

In the first publication we analyze the security of cryptographic hash functions based on the AES and demonstrate practical attacks on reduced-round versions of these algorithms. The second publication provides cryptanalysis of the lightweight block cipher SIMON in particular how resistant this type of block ciphers are against differential and linear cryptanalysis. In the fourth publication we present a short-input hash function utilizing AES-specific instructions on modern CPUs in order to improve the performance of hash-based signature schemes. The last publication deals with the design of the tweakable lightweight block cipher Skinny which provides strong security bounds against differential and linear attacks while also competing with the performance of SIMON.
Secure Block Ciphers - Cryptanalysis and Design

The rapid evolution of computational devices and the widespread adoption of digital communication have deeply transformed the way we conduct both business and everyday life and they continue to do so. The ability to ensure confidentiality and integrity of information sent over digital channels is fundamental to this development and is absolutely essential for all private and corporate communication, ranging from bank transactions, digital citizen services, and remote computer access, to cell phone calls and instant messaging. The vast majority of secured data sent over all types of networks is encrypted using so-called symmetric ciphers. The security of our digital infrastructure thus rests at its very base on their security.

The central topic of this thesis is the security of block ciphers – the most prominent form of symmetric ciphers. This thesis is separated in two parts. The first part is an introduction to block ciphers and their cryptanalysis, the second part contains publications written and published during the PhD studies. The first publication evaluates the security of a modification of the AES in which the choice of S-box is unknown to the attacker. We find that some of the attacks that can be applied to the AES can be transferred to this block cipher, albeit with a higher attack complexity. The second publication introduces a new block cipher family which is targeted for new applications in fully homomorphic encryption and multi-party computation. We demonstrate the soundness of the design and its superior performance in these applications. The third publication treats the cryptanalysis of Simon, a cipher proposed by the NSA. In particular we discuss how the methods of differential and linear cryptanalysis can correctly be applied to ciphers of this type. The fourth publication introduces a cryptanalytic framework which generalizes differential cryptanalysis. We demonstrate that attacks based on impossible transitions in this framework can competitively break round-reduced block ciphers in the low-data setting.
Design and Analysis of Symmetric Primitives
The subject of this thesis is the study of symmetric cryptographic primitives. We investigate these objects from three different perspectives: cryptanalysis, design and implementation aspects.

The first part deals with cryptanalysis of symmetric primitives, where one tries to leverage a property of the design to achieve some adversarial goal. Two of the most successful types of cryptanalysis are differential- and linear attacks. We apply variants of differential cryptanalysis to the lightweight block cipher SIMON which was proposed by researchers from the National Security Agency (NSA) in 2013. In particular, we present a search heuristic to find differentials of high probability, and we investigate the clustering of characteristics known as the differential effect. Finally, we apply impossible differential attacks using truncated differentials to a number of SIMON variants. Next, we define a theoretical model for key-less linear distinguishers, which captures the meaning of distinguishing a block cipher from an ideal permutation using linear cryptanalysis, when the key is either known or chosen by the adversary. Such models exist using differential properties but were never before defined using linear cryptanalysis. We apply this model to the standardized block cipher PRESENT. Finally, we present very generic attacks on two authenticated encryption schemes, AVALANCHE and RBS, by pointing out severe design flaws that can be leveraged to fully recover the secret key with very low complexity.

In the second part, we delve into the matter of the various aspects of designing a symmetric cryptographic primitive. We start by considering generalizations of the widely acclaimed Advanced Encryption Standard (AES) block cipher. In particular, our focus is on a component operation in the cipher which permutes parts of the input to obtain dependency between the state bits. With this operation in focus, we give a range of theoretical results, reducing the possible choices for the operation in generalized ciphers to a particular set of classes. We then employ a computer-aided optimization technique to determine the best choices for the operation in terms of resistance towards differential- and linear cryptanalysis. Also in the vein of symmetric primitive design we present PRØST, a new and highly secure permutation. Employing existing third-party modes of operation, we present six proposals based on PRØST for the ongoing CAESAR competition for authenticated encryption with associated data. We describe the design criteria, the usage modes and give proofs of security.

Finally, in the third part, we consider implementation aspects of symmetric cryptography, with focus on high-performance software. In more detail, we analyze and implement modes recommended by the National Institute of Standards and Technology (NIST), as well as authenticated encryption modes from the CAESAR competition, when instantiated with the AES. The data processed in our benchmarking has sizes representative to that of typical Internet traffic. Motivated by a significant improvement to special AES instructions in the most recent microarchitecture from Intel, codenamed Haswell, our implementations are tailored for this platform. Finally, we introduce the comb scheduler which is a low-overhead look-ahead strategy for processing multiple messages in parallel. We show that it significantly increases the throughput for sequential modes of operation especially, but also for parallel modes to a lesser extent.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science , Cryptology
Authors: Lauridsen, M. M. (Intern), Rechberger, C. (Intern), Knudsen, L. R. (Intern)
Number of pages: 213
Publication date: 2016

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
Series: DTU Compute PHD-2015
Number: 382
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Electronic versions:
phd382_Lauridsen_MM.pdf
Publication: Research › Ph.D. thesis – Annual report year: 2016

MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity
We explore cryptographic primitives with low multiplicative complexity. This is motivated by recent progress in practical applications of secure multi-party computation (MPC), fully homomorphic encryption (FHE), and zero-knowledge proofs (ZK) where primitives from symmetric cryptography are needed and where linear computations are, compared to non-linear operations, essentially “free”. Starting with the cipher design strategy “LowMC” from Eurocrypt 2015, a number of bitoriented proposals have been put forward, focusing on applications where the multiplicative depth of the circuit describing the cipher is the most important optimization goal.

Surprisingly, albeit many MPC/FHE/2K-protocols natively support operations in GF(p) for large p, very few primitives, even considering all of symmetric cryptography, natively work in such fields. To that end, our proposal for both block ciphers
and cryptographic hash functions is to reconsider and simplify the round function of the Knudsen-Nyberg cipher from 1995. The mapping \( F(x) := x^3 \) is used as the main component there and is also the main component of our family of proposals called "MiMC". We study various attack vectors for this construction and give a new attack vector that outperforms others in relevant settings.

Due to its very low number of multiplications, the design lends itself well to a large class of applications, especially when the depth does not matter but the total number of multiplications in the circuit dominates all aspects of the implementation. With a number of rounds which we deem secure based on our security analysis, we report on significant performance improvements in a representative use-case involving SNARKs.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Royal Holloway University of London, Graz University of Technology
Authors: Albrecht, M. (Ekstern), Grassi, L. (Ekstern), Rechberger, C. (Intern), Roy, A. (Intern), Tiessen, T. (Intern)
Pages: 191-219
Publication date: 2016

Host publication information
ISBN (Print): 978-3-662-53886-9
ISBN (Electronic): 978-3-662-53887-6

Series: Lecture Notes in Computer Science
Volume: 10031
ISSN: 0302-9743
BFI conference series: International Conference on the Theory and Application of Cryptology and Information Security (5020046)
Main Research Area: Technical/natural sciences

Distributed cryptography, Cryptanalysis, Block ciphers, Hash functions, Zero knowledge
Electronic versions:
492.pdf. Embargo ended: 10/11/2017
DOIs:
10.1007/978-3-662-53887-6_7
Source: FindIt
Source-ID: 2349693830
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Practical Low Data-Complexity Subspace-Trail Cryptanalysis of Round-Reduced PRINCE
Subspace trail cryptanalysis is a very recent new cryptanalysis technique, and includes differential, truncated differential, impossible differential, and integral attacks as special cases.

In this paper, we consider PRINCE, a widely analyzed block cipher proposed in 2012. After the identification of a 2.5 rounds subspace trail of PRINCE, we present several (truncated differential) attacks up to 6 rounds of PRINCE. This includes a very practical attack with the lowest data complexity of only 8 plaintexts for 4 rounds, which co-won the final round of the PRINCE challenge in the 4-round chosen-plaintext category. The attacks have been verified using a C implementation.

Of independent interest, we consider a variant of PRINCE in which ShiftRows and MixLayer operations are exchanged in position. In particular, our result shows that the position of ShiftRows and MixLayer operations influences the security of PRINCE. The same analysis applies to follow-up designs inspired by PRINCE.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Graz University of Technology
Authors: Grassi, L. (Ekstern), Rechberger, C. (Intern)
Pages: 322-342
Publication date: 2016

Host publication information
Title of host publication: Progress in Cryptology – INDOCRYPT 2016: Proceedings of the 17th International Conference on Cryptology in India
Analyzing Permutations for AES-like Ciphers: Understanding ShiftRows

Designing block ciphers and hash functions in a manner that resemble the AES in many aspects has been very popular since Rijndael was adopted as the Advanced Encryption Standard. However, in sharp contrast to the MixColumns operation, the security implications of the way the state is permuted by the operation resembling ShiftRows has never been studied in depth.

Here, we provide the first structured study of the influence of ShiftRows-like operations, or more generally, word-wise permutations, in AES-like ciphers with respect to diffusion properties and resistance towards differential- and linear attacks. After formalizing the concept of guaranteed trail weights, we show a range of equivalence results for permutation layers in this context. We prove that the trail weight analysis when using arbitrary word-wise permutations, with rotations as a special case, reduces to a consideration of a specific normal form. Using a mixed-integer linear programming approach, we obtain optimal parameters for a wide range of AES-like ciphers, and show improvements on parameters for Rijndael-192, Rijndael-256, PRIMATEs-80 and Prøst-128. As a separate result, we show for specific cases of the state geometry that a seemingly optimal bound on the trail weight can be obtained using cyclic rotations only for the permutation layer, i.e. in a very implementation friendly way.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Ruhr-Universität Bochum, Universität Passau, Ruhr-University Bochum
Authors: Beierle, C. (Ekstern), Jovanovic, P. (Ekstern), Lauridsen, M. M. (Intern), Leander, G. (Ekstern), Rechberger, C. (Intern)
Pages: 37-58
Publication date: 2015
Ciphers for MPC and FHE
Designing an efficient cipher was always a delicate balance between linear and non-linear operations. This goes back to the design of DES, and in fact all the way back to the seminal work of Shannon.

Here we focus, for the first time, on an extreme corner of the design space and initiate a study of symmetric-key primitives that minimize the multiplicative size and depth of their descriptions. This is motivated by recent progress in practical instantiations of secure multi-party computation (MPC), fully homomorphic encryption (FHE), and zero-knowledge proofs (ZK) where linear computations are, compared to non-linear operations, essentially “free”.

We focus on the case of a block cipher, and propose the family of block ciphers "LowMC", beating all existing proposals with respect to these metrics by far. We sketch several applications for such ciphers and give implementation comparisons suggesting that when encrypting larger amounts of data the new design strategy translates into improvements in computation and communication complexity by up to a factor of 5 compared to AES-128, which incidentally is one of the most competitive classical designs. Furthermore, we identify cases where “free XORs” can no longer be regarded as such but represent a bottleneck, hence refuting this commonly held belief with a practical example.

Linear Distinguishers in the Key-less Setting: Application to PRESENT
The application of the concept of linear cryptanalysis to the domain of key-less primitives is largely an open problem. In this paper we, for the first time, propose a model in which its application is meaningful for distinguishing block ciphers. Combining our model with ideas from message modification and rebound-like approaches, we initiate a study of cryptographic primitives with respect to this new attack vector and choose the lightweight block cipher PRESENT as an example target. This leads to known-key distinguishers over up to 27 rounds, whereas the best previous result is up to 18 rounds in the chosen-key model.
Practical Attacks on AES-like Cryptographic Hash Functions

Despite the great interest in rebound attacks on AES-like hash functions since 2009, we report on a rather generic, albeit keyschedule-dependent, algorithmic improvement: A new message modification technique to extend the inbound phase, which even for large internal states makes it possible to drastically reduce the complexity of attacks to very practical values for reduced-round versions. Furthermore, we describe new and practical attacks on Whirlpool and the recently proposed GOST R hash function with one or more of the following properties: more rounds, less time/memory complexity, and more relevant model. To allow for easy verification, we also provide a source-code for them.

State-Recovery Analysis of Spritz

RC4 suffered from a range of plaintext-recovery attacks using statistical biases, which use substantial, albeit close-to-practical, amounts of known keystream in applications such as TLS or WEP/WPA. Spritz was recently proposed at the rump session of CRYPTO 2014 as a slower redesign of RC4 by Rivest and Schuldt, aiming at reducing the statistical biases that lead to these attacks on RC4.

Even more devastating than those plaintext-recovery attacks from large amounts of keystream would be state- or key-recovery attacks from small amounts of known keystream. For RC4, there is unsubstantiated evidence that they may exist, the situation for Spritz is however not clear, as resistance against such attacks was not a design goal.

In this paper, we provide the first cryptanalytic results on Spritz and introduce three different state recovery algorithms. Our first algorithm recovers an internal state, requiring only a short segment of keystream, with an approximated complexity of 2^1400, which is much faster than exhaustive search through all possible states, but is still far away from a practical attack. Furthermore, we introduce a second algorithm that uses a pattern in the keystream to reduce the number of guessed values in our state recovery algorithm. Our third algorithm uses a probabilistic approach by considering the permutation table as probability distribution.
All in all, rather than showing a weakness, our analysis supports the conjecture that compared to RC4, Spritz may also provide higher resistance against potentially devastating state-recovery attacks.

### General information
- **State:** Published
- **Organisations:** Department of Applied Mathematics and Computer Science, Cryptology, Graz University of Technology
- **Authors:** Ankele, R. (Ekstern), Kölbl, S. (Intern), Rechberger, C. (Intern)
- **Pages:** 204-221
- **Publication date:** 2015

### Host publication information
- **Title of host publication:** Progress in Cryptology – LATINCRYPT 2015: Proceedings of the 4th International Conference on Cryptology and Information Security in Latin America
- **Publisher:** Springer
- **ISBN (Print):** 978-3-319-22173-1
- **ISBN (Electronic):** 978-3-319-22174-8

### The Rebound Attack and Subspace Distinguishers: Application to Whirlpool
We introduce the rebound attack as a variant of differential cryptanalysis on hash functions and apply it to the hash function Whirlpool, standardized by ISO/IEC. We give attacks on reduced variants of the 10-round Whirlpool hash function and compression function. Our results are collisions for 5.5 and near-collisions for 7.5 rounds on the hash function, as well as semi-free-start collisions for 7.5 and semi-free-start near-collisions for 9.5 rounds on the compression function. Additionally, we introduce the subspace problem as a generalization of near-collision resistance. Finally, we present the first distinguishers that apply to the full compression function and the full underlying block cipher W of Whirlpool.

### General information
- **State:** Published
- **Organisations:** Department of Applied Mathematics and Computer Science, Cryptology, NXP Semiconductors Austria, Graz University of Technology, Katholieke Universiteit
- **Authors:** Lamberger, M. (Ekstern), Mendel, F. (Ekstern), Schläffer, M. (Ekstern), Rechberger, C. (Intern), Rijmen, V. (Ekstern)
- **Number of pages:** 40
- **Pages:** 257-296
- **Publication date:** 2015
- **Main Research Area:** Technical/natural sciences

### Publication information
- **Journal:** Journal of Cryptology
- **Volume:** 28
- **Issue number:** 2
- **ISSN (Print):** 0933-2790
- **BFI (2018):** BFI-level 2
- **Web of Science (2018):** Indexed yes
- **BFI (2017):** BFI-level 2
- **Web of Science (2017):** Indexed Yes
- **BFI (2016):** BFI-level 2
- **Scopus rating (2016):** SJR 0.861 SNIP 2.607 CiteScore 2.68
Rotational Rebound Attacks on Reduced Skein

In this paper we combine two powerful methods of symmetric cryptanalysis: rotational cryptanalysis and the rebound attack. Rotational cryptanalysis was designed for the analysis of bit-oriented designs like ARX (Addition-Rotation-XOR) schemes. It has been applied to several hash functions and block ciphers, including the new standard SHA-3 (Keccak). The rebound attack is a start-from-the-middle approach for finding differential paths and conforming pairs in byte-oriented designs like Substitution-Permutation networks and AES.

We apply our new compositional attack to the reduced version of the hash function Skein, a finalist of the SHA-3 competition. Our attack penetrates more than two thirds of the Skein core—the cipher Threefish, and made the designers to change the submission in order to prevent it.

The rebound part of our attack has been significantly enhanced to deliver results on the largest number of rounds. We also use neutral bits and message modification methods from the practice of collision search in MD5 and SHA-1 hash functions. These methods push the rotational property through more rounds than previous analysis suggested, and eventually establish a distinguishing property for the reduced Threefish cipher. We formally prove that such a property cannot be found for an ideal cipher within the complexity limits of our attack. The complexity estimates are supported by extensive experiments.
The LOCAL attack: Cryptanalysis of the authenticated encryption scheme ALE

We show how to produce a forged (ciphertext, tag) pair for the scheme ALE with data and time complexity of $2^{102}$ ALE encryptions of short messages and the same number of authentication attempts. We use a differential attack based on a local collision, which exploits the availability of extracted state bytes to the adversary. Our approach allows for a time-data complexity tradeoff, with an extreme case of a forgery produced after $2^{119}$ attempts and based on a single authenticated message. Our attack is further turned into a state recovery and a universal forgery attack with a time complexity of $2^{120}$ verification attempts using only a single authenticated 48-byte message.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, University of Luxembourg
Authors: Khovratovich, D. (Ekstern), Rechberger, C. (Intern)
Pages: 174-184
Publication date: 2014

Host publication information
Title of host publication: Selected Areas in Cryptography - SAC 2013. Revised Selected Papers
Publisher: Springer
ISBN (Print): 978-3-662-43413-0
ISBN (Electronic): 978-3-662-43414-7

Series: Lecture Notes in Computer Science
Volume: 8282
ISSN: 0302-9743
BFI conference series: Selected Areas in Cryptography (5000230)
Main Research Area: Technical/natural sciences
Conference: 20th International Workshop on Selected Areas of Cryptography, Burnaby, Canada, 14/08/2013 - 14/08/2013
Data Encryption, Systems and Data Security, Algorithm Analysis and Problem Complexity, Coding and Information Theory

DOIs: 10.1007/978-3-662-43414-7_9
Source: FindIt
Source-ID: 2199676910
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014
Improved cryptanalysis of the block cipher KASUMI

KASUMI is a block cipher which consists of eight Feistel rounds with a 128-bit key. Proposed more than 10 years ago, the confidentiality and integrity of 3G mobile communications systems depend on the security of KASUMI. In the practically interesting single key setting, only up to 6 rounds have been attacked so far. In this paper we use some observations on the FL and FO functions. Combining these observations with a key schedule weakness, we select some special input and output values to refine the general 5-round impossible differentials and propose the first 7-round attack on KASUMI with time and data complexities similar to the previously best 6-round attacks. This leaves now only a single round of security margin. The new impossible differential attack on the last 7 rounds needs 2114.3 encryptions with 252.5 chosen plaintexts. For the attack on the first 7 rounds, the data complexity is 262 known plaintexts and the time complexity is 2115.8 encryptions. © 2013 Springer-Verlag Berlin Heidelberg.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Tsinghua University, Shandong University
Authors: Jia, K. (Ekstern), Li, L. (Ekstern), Rechberger, C. (Intern), Chen, J. (Ekstern), Wang, X. (Ekstern)
Pages: 222-233
Publication date: 2013
Conference: 19th International Conference on Selected Areas in Cryptography, Windsor, Canada, 15/08/2012 - 15/08/2012
BFI conference series: Selected Areas in Cryptography (5000230)
Main Research Area: Technical/natural sciences

Publication information
Journal: Lecture Notes in Computer Science
Volume: 7707
ISSN (Print): 0302-9743
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 0.67 SJR 0.315 SNIP 0.552
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.328 SNIP 0.618 CiteScore 0.37
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.325 SNIP 0.678 CiteScore 0.42
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.329 SNIP 0.699 CiteScore 0.49
ISI indexed (2013): ISI indexed no
Web of Science (2013): Indexed yes
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.323 SNIP 0.708 CiteScore 0.49
ISI indexed (2012): ISI indexed no
Web of Science (2012): Indexed yes
BFI (2011): BFI-level 1
Scopus rating (2011): SJR 0.325 SNIP 0.721 CiteScore 0.49
ISI indexed (2011): ISI indexed no
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.314 SNIP 0.634
Web of Science (2010): Indexed yes
BFI (2009): BFI-level 1
Scopus rating (2009): SJR 0.305 SNIP 0.548
Web of Science (2009): Indexed yes
BFI (2008): BFI-level 1
Scopus rating (2008): SJR 0.281 SNIP 0.447
Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 Family

We present a new concept of biclique as a tool for preimage attacks, which employs many powerful techniques from differential cryptanalysis of block ciphers and hash functions. The new tool has proved to be widely applicable by inspiring many authors to publish new results of the full versions of AES, KASUMI, IDEA, and Square. In this paper, we show how our concept leads to the first cryptanalysis of the round-reduced Skein hash function, and describe an attack on the SHA-2 hash function with more rounds than before.

Narrow-Bicliques: Cryptanalysis of Full IDEA

We apply and extend the recently introduced biclique framework to IDEA and for the first time describe an approach to noticeably speed-up key-recovery for the full 8.5 round IDEA. We also show that the biclique approach to block cipher cryptanalysis not only obtains results on more rounds, but also improves time and data complexities over existing attacks. We consider the first 7.5 rounds of IDEA and demonstrate a variant of the approach that works with practical data complexity. The conceptual contribution is the narrow-bicliques technique: the recently introduced independent-biclique approach extended with ways to allow for a significantly reduced data complexity with everything else being equal. For this
we use available degrees of freedom as known from hash cryptanalysis to narrow the relevant differential trails. Our cryptanalysis is of high computational complexity, and does not threaten the practical use of IDEA in any way, yet the techniques are practically verified to a large extent.

**General information**

**State:** Published  
**Organisations:** Department of Mathematics, Discrete mathematics  
**Authors:** Khovratovich, D. (Ekstern), Leurent, G. (Ekstern), Rechberger, C. (Intern)  
**Pages:** 392-410  
**Publication date:** 2012  
**Conference:** EUROCRYPT 2012, Cambridge, United Kingdom, 15/04/2012 - 15/04/2012  
**Main Research Area:** Technical/natural sciences

**Publication information**

**Journal:** Lecture Notes in Computer Science  
**Volume:** 7237  
**ISSN (Print):** 0302-9743  
**Ratings:**  
BFI (2018): BFI-level 1  
Web of Science (2018): Indexed yes  
BFI (2017): BFI-level 1  
BFI (2016): BFI-level 1  
Scopus rating (2016): CiteScore 0.67 SJR 0.315 SNIP 0.552  
Web of Science (2016): Indexed yes  
BFI (2015): BFI-level 1  
Scopus rating (2015): SJR 0.328 SNIP 0.618 CiteScore 0.37  
BFI (2014): BFI-level 1  
Scopus rating (2014): SJR 0.325 SNIP 0.678 CiteScore 0.42  
BFI (2013): BFI-level 1  
Scopus rating (2013): SJR 0.329 SNIP 0.699 CiteScore 0.49  
ISI indexed (2013): ISI indexed no  
Web of Science (2013): Indexed yes  
BFI (2012): BFI-level 1  
Scopus rating (2012): SJR 0.323 SNIP 0.708 CiteScore 0.49  
ISI indexed (2012): ISI indexed no  
Web of Science (2012): Indexed yes  
BFI (2011): BFI-level 1  
Scopus rating (2011): SJR 0.325 SNIP 0.721 CiteScore 0.49  
ISI indexed (2011): ISI indexed no  
BFI (2010): BFI-level 1  
Scopus rating (2010): SJR 0.314 SNIP 0.634  
Web of Science (2010): Indexed yes  
BFI (2009): BFI-level 1  
Scopus rating (2009): SJR 0.305 SNIP 0.548  
Web of Science (2009): Indexed yes  
BFI (2008): BFI-level 1  
Scopus rating (2008): SJR 0.281 SNIP 0.447  
Scopus rating (2007): SJR 0.294 SNIP 0.494  
Web of Science (2007): Indexed yes  
Scopus rating (2006): SJR 0.315 SNIP 0.615  
Web of Science (2006): Indexed yes  
Scopus rating (2005): SJR 0.333 SNIP 0.712  
Web of Science (2005): Indexed yes  
Scopus rating (2004): SJR 0.346 SNIP 0.756  
Web of Science (2004): Indexed yes  
Scopus rating (2003): SJR 0.412 SNIP 0.812  
Web of Science (2003): Indexed yes
On security arguments of the second round SHA-3 candidates
In 2007, the US National Institute for Standards and Technology (NIST) announced a call for the design of a new cryptographic hash algorithm in response to vulnerabilities like differential attacks identified in existing hash functions, such as MD5 and SHA-1. NIST received many submissions, 51 of which got accepted to the first round. 14 candidates were left in the second round, out of which five candidates have been recently chosen for the final round. An important criterion in the selection process is the SHA-3 hash function security. We identify two important classes of security arguments for the new designs: (1) the possible reductions of the hash function security to the security of its underlying building blocks and (2) arguments against differential attack on building blocks. In this paper, we compare the state of the art provable security reductions for the second round candidates and review arguments and bounds against classes of differential attacks. We discuss all the SHA-3 candidates at a high functional level, analyze, and summarize the security reduction results and bounds against differential attacks. Additionally, we generalize the well-known proof of collision resistance preservation, such that all SHA-3 candidates with a suffix-free padding are covered.
PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications: Extended Abstract

This paper presents a block cipher that is optimized with respect to latency when implemented in hardware. Such ciphers are desirable for many future pervasive applications with real-time security needs. Our cipher, named PRINCE, allows encryption of data within one clock cycle with a very competitive chip area compared to known solutions. The fully unrolled fashion in which such algorithms need to be implemented calls for innovative design choices. The number of rounds must be moderate and rounds must have short delays in hardware. At the same time, the traditional need that a cipher has to be iterative with very similar round functions disappears, an observation that increases the design space for the algorithm. An important further requirement is that realizing decryption and encryption results in minimum additional costs. PRINCE is designed in such a way that the overhead for decryption on top of encryption is negligible. More precisely for our cipher it holds that decryption for one key corresponds to encryption with a related key. This property we refer to as α-reflection is of independent interest and we prove its soundness against generic attacks.

General information
State: Published
Organisations: Department of Mathematics, Discrete mathematics, Ruhr-University Bochum, NXP Semiconductors
Authors: Borghoff, J. (Intern), Canteaut, A. M. (Intern), Guneysu, T. (Ekstern), Kavun, E. (Ekstern), Knezevic, M. (Ekstern), Knudsen, L. R. (Intern), Leander, G. (Intern), Nikov, V. (Ekstern), Paar, C. (Ekstern), Rechberger, C. (Intern)
Pages: 208-225
Publication date: 2012

Host publication information
Publisher: Springer
ISBN (Print): 978-3-642-34960-7
ISBN (Electronic): 978-3-642-34961-4
Series: Lecture Notes in Computer Science
Volume: 7658
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, 02/12/2012 - 02/12/2012
DOIs: 10.1007/978-3-642-34961-4_14
Source: dtu
Source-ID: n:oai:DTIC-ART:bl/374901893::24304
Publication: Research - peer-review › Article in proceedings – Annual report year: 2012

A 3-Subset Meet-in-the-Middle Attack: Cryptanalysis of the Lightweight Block Cipher KTANTAN

In this paper we describe a variant of existing meet-in-the-middle attacks on block ciphers. As an application, we propose meet-in-the-middle attacks that are applicable to the KTANTAN family of block ciphers accepting a key of 80 bits. The
attacks are due to sonic weaknesses in its bitwise key schedule(1). We report an attack of time complexity $2^{75.170}$ encryptions on the full KTANTAN32 cipher with only 3 plaintext/ciphertext pairs and well as $2^{75.044}$ encryptions on the full KTANTAN48 and $2^{75.584}$ encryptions on the full KTANTAN69 with 2 plaintext/ciphertext pairs. All these attacks work in the classical attack model without any related keys. In the differential related-key model, we demonstrate 218- and 174-round differentials holding with probability 1. This shows that a strong related-key property can translate to a successful attack in the non-related-key setting. Having extremely low data requirements, these attacks are valid even in RFID-like environments where only a very limited amount of text material may be available to an attacker.

**General information**

State: Published
Organisations: Department of Mathematics, Discrete mathematics
Authors: Bogdanov, A. (Intern), Rechberger, C. (Intern)
Pages: 229-240
Publication date: 2011
Workshop: 17th International Workshop on Selected Areas in Cryptography, Waterloo, Canada, 12/08/2010 - 12/08/2010
Main Research Area: Technical/natural sciences

**Publication information**

Journal: Lecture Notes in Computer Science
Volume: 6544
ISSN (Print): 0302-9743
Ratings:
- BFI (2018): BFI-level 1
- Web of Science (2018): Indexed yes
- BFI (2017): BFI-level 1
- BFI (2016): BFI-level 1
- Scopus rating (2016): CiteScore 0.67 SJR 0.315 SNIP 0.552
- Web of Science (2016): Indexed yes
- BFI (2015): BFI-level 1
- Scopus rating (2015): SJR 0.328 SNIP 0.618 CiteScore 0.37
- BFI (2014): BFI-level 1
- Scopus rating (2014): SJR 0.325 SNIP 0.678 CiteScore 0.42
- BFI (2013): BFI-level 1
- Scopus rating (2013): SJR 0.329 SNIP 0.699 CiteScore 0.49
- ISI indexed (2013): ISI indexed no
- Web of Science (2013): Indexed yes
- BFI (2012): BFI-level 1
- Scopus rating (2012): SJR 0.323 SNIP 0.708 CiteScore 0.49
- ISI indexed (2012): ISI indexed no
- Web of Science (2012): Indexed yes
- BFI (2011): BFI-level 1
- Scopus rating (2011): SJR 0.325 SNIP 0.721 CiteScore 0.49
- ISI indexed (2011): ISI indexed no
- BFI (2010): BFI-level 1
- Scopus rating (2010): SJR 0.314 SNIP 0.634
- Web of Science (2010): Indexed yes
- BFI (2009): BFI-level 1
- Scopus rating (2009): SJR 0.305 SNIP 0.548
- Web of Science (2009): Indexed yes
- BFI (2008): BFI-level 1
- Scopus rating (2008): SJR 0.281 SNIP 0.447
- CiteScore rating (2007): SJR 0.294 SNIP 0.494
- Web of Science (2007): Indexed yes
- Scopus rating (2006): SJR 0.315 SNIP 0.615
- Web of Science (2006): Indexed yes
- Scopus rating (2005): SJR 0.333 SNIP 0.712
- Web of Science (2005): Indexed yes
Biclique cryptanalysis of the full AES

Since Rijndael was chosen as the Advanced Encryption Standard (AES), improving upon 7-round attacks on the 128-bit key variant (out of 10 rounds) or upon 8-round attacks on the 192/256-bit key variants (out of 12/14 rounds) has been one of the most difficult challenges in the cryptanalysis of block ciphers for more than a decade. In this paper, we present the novel technique of block cipher cryptanalysis with bicliques, which leads to the following results: The first key recovery method for the full AES-128 with computational complexity $2^{126.1}$. The first key recovery method for the full AES-192 with computational complexity $2^{189.7}$. The first key recovery method for the full AES-256 with computational complexity $2^{254.4}$. Key recovery methods with lower complexity for the reduced-round versions of AES not considered before, including cryptanalysis of 8-round AES-128 with complexity $2^{124.9}$. Preimage search for compression functions based on the full AES versions faster than brute force. In contrast to most shortcut attacks on AES variants, we do not need to assume related-keys. Most of our techniques only need a very small part of the codebook and have low memory requirements, and are practically verified to a large extent. As our cryptanalysis is of high computational complexity, it does not threaten the practical use of AES in any way. © 2011 International Association for Cryptologic Research.
This paper presents ongoing work towards extensions of meet-in-the-middle (MITM) attacks on block ciphers. Exploring developments in MITM attacks in hash analysis such as: (i) the splice-and-cut technique; (ii) the indirect-partial-matching technique. Our first contribution is that we show corrections to previous cryptanalysis and point out that the key schedule is more vulnerable to MITM attacks than previously reported. Secondly we further improve the time complexities of previous attacks with (i) and (ii), now the 80-bit secret key of the full rounds KTANTAN-{32, 48, 64} can be recovered at time complexity of $2^{(72.9)}$, $2^{(73.8)}$ and $2^{(74.4)}$ respectively, each requiring 4 chosen-plaintexts.

Improved Meet-in-the-Middle Cryptanalysis of KTANTAN

This paper presents ongoing work towards extensions of meet-in-the-middle (MITM) attacks on block ciphers. Exploring developments in MITM attacks in hash analysis such as: (i) the splice-and-cut technique; (ii) the indirect-partial-matching technique. Our first contribution is that we show corrections to previous cryptanalysis and point out that the key schedule is more vulnerable to MITM attacks than previously reported. Secondly we further improve the time complexities of previous attacks with (i) and (ii), now the 80-bit secret key of the full rounds KTANTAN-{32, 48, 64} can be recovered at time complexity of $2^{(72.9)}$, $2^{(73.8)}$ and $2^{(74.4)}$ respectively, each requiring 4 chosen-plaintexts.

General information

State: Published
Organisations: Nanyang Technological University, Katholieke Universiteit, Agency for Science, Technology and Research
Authors: Wei, L. (Ekstern), Rechberger, C. (Intern), Guo, J. (Ekstern), Wu, H. (Ekstern), Wang, H. (Ekstern), Ling, S. (Ekstern)
Pages: 433-438
Publication date: 2011
Conference: 16th Australasian Conference on Information Security and Privacy, ACISP 2011, Melbourne, Australia, 01/01/2011
Main Research Area: Technical/natural sciences

Publication information
Journal: Lecture Notes in Computer Science
Volume: 6812
ISSN (Print): 0302-9743
Advanced meet-in-the-middle preimage attacks: First results on full Tiger, and improved results on MD4 and SHA-2

We revisit narrow-pipe designs that are in practical use, and their security against preimage attacks. Our results are the best known preimage attacks on Tiger, MD4, and reduced SHA-2, with the result on Tiger being the first cryptanalytic shortcut attack on the full hash function. Our attacks runs in time $2^{188.8}$ for finding preimages, and $2^{188.2}$ for second-preimages. Both have memory requirement of order 28, which is much less than in any other recent preimage attacks on reduced Tiger. Using pre-computation techniques, the time complexity for finding a new preimage or second-preimage for MD4 can now be as low as $2^{78.4}$ and $2^{69.4}$ MD4 computations, respectively. The second-preimage attack works for all messages longer than 2 blocks. To obtain these results, we extend the meet-in-the-middle framework recently developed by Aoki and Sasaki in a series of papers. In addition to various algorithm-specific techniques, we use a number of conceptually new ideas that are applicable to a larger class of constructions. Among them are (1) incorporating multi-target scenarios into the MITM framework, leading to faster preimages from pseudo-preimages, (2) a simple precomputation technique that allows for finding new preimages at the cost of a single pseudo-preimage, and (3) probabilistic initial structures, to reduce the attack time complexity. All the techniques developed await application to other hash functions. To illustrate this, we give as another example improved preimage attacks on SHA-2 members. © 2010 International Association for Cryptologic Research.
Cryptanalysis of the 10-Round Hash and Full Compression Function of SHAvite-3-512

In this paper, we analyze SHAvite-3-512 hash function, as proposed for round 2 of the SHA-3 competition. We present cryptanalytic results on 10 out of 14 rounds of the hash function SHAvite-3-512, and on the full 14 round compression function of SHAvite-3-512. We show a second preimage attack on the hash function reduced to 10 rounds with a complexity of $2^{497}$ compression function evaluations and $2^{16}$ memory. For the full 14-round compression function, we give a chosen counter, chosen salt preimage attack with $2^{384}$ compression function evaluations and $2^{128}$ memory (or complexity $2^{448}$ without memory), and a collision attack with $2^{192}$ compression function evaluations and $2^{128}$ memory.

General information
State: Published
Organisations: Discrete mathematics, Department of Mathematics, Ecole Normale Superieure, TU Graz, Fachhochschule Nordwestschweiz, Ingenico
Authors: Gauravaram, P. (Intern), Leurent, G. (Ekstern), Mendel, F. (Ekstern), Plasencia, M. N. (Ekstern), Peyrin, T. (Ekstern), Rechberger, C. (Intern), Schläffer, M. (Ekstern)
Pages: 419-436
Publication date: 2010
Conference: Third International Conference on Cryptology in Africa, Stellenbosch, South Africa, 03/05/2010 - 03/05/2010
Main Research Area: Technical/natural sciences

Publication information
Journal: Lecture Notes in Computer Science
Volume: 6055
ISSN (Print): 0302-9743
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 0.67 SJR 0.315 SNIP 0.552
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.328 SNIP 0.618 CiteScore 0.37
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.325 SNIP 0.678 CiteScore 0.42
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.329 SNIP 0.699 CiteScore 0.49
Rebound Attacks on the Reduced Grøstl Hash Function

Grøstl is one of 14 second round candidates of the NIST SHA-3 competition. Cryptanalytic results on the wide-pipe compression function of Grøstl-256 have already been published. However, little is known about the hash function, arguably a much more interesting cryptanalytic setting. Also, Grøstl-512 has not been analyzed yet. In this paper, we show the first cryptanalytic attacks on reduced-round versions of the Grøstl hash functions. These results are obtained by several extensions of the rebound attack. We present a collision attack on 4/10 rounds of the Grøstl-256 hash function and 5/14 rounds of the Grøstl-512 hash functions. Additionally, we give the best collision attack for reduced-round (7/10 and 7/14) versions of the compression function of Grøstl-256 and Grøstl-512.

General information
State: Published
Organisations: Department of Mathematics, Discrete mathematics, Graz University of Technology
Authors: Mendel, F. (Ekstern), Rechberger, C. (Intern), Schlaffer, M. (Ekstern), Thomsen, S. S. (Intern)
Pages: 350–365
Publication date: 2010
Publication information
Journal: Lecture Notes in Computer Science
Volume: 5985
ISSN (Print): 0302-9743
Ratings:
  BFI (2018): BFI-level 1
  Web of Science (2018): Indexed yes
  BFI (2017): BFI-level 1
  BFI (2016): BFI-level 1
  Scopus rating (2016): CiteScore 0.67 SJR 0.315 SNIP 0.552
  Web of Science (2016): Indexed yes
  BFI (2015): BFI-level 1
  Scopus rating (2015): SJR 0.328 SNIP 0.618 CiteScore 0.37
  BFI (2014): BFI-level 1
  Scopus rating (2014): SJR 0.325 SNIP 0.678 CiteScore 0.42
  BFI (2013): BFI-level 1
  Scopus rating (2013): SJR 0.329 SNIP 0.699 CiteScore 0.49
  ISI indexed (2013): ISI indexed no
  Web of Science (2013): Indexed yes
  BFI (2012): BFI-level 1
  Scopus rating (2012): SJR 0.323 SNIP 0.708 CiteScore 0.49
  ISI indexed (2012): ISI indexed no
  Web of Science (2012): Indexed yes
  BFI (2011): BFI-level 1
  Scopus rating (2011): SJR 0.325 SNIP 0.721 CiteScore 0.49
  ISI indexed (2011): ISI indexed no
  BFI (2010): BFI-level 1
  Scopus rating (2010): SJR 0.314 SNIP 0.634
  Web of Science (2010): Indexed yes
  BFI (2009): BFI-level 1
  Scopus rating (2009): SJR 0.305 SNIP 0.548
  Web of Science (2009): Indexed yes
  BFI (2008): BFI-level 1
  Scopus rating (2008): SJR 0.281 SNIP 0.447
  Scopus rating (2007): SJR 0.294 SNIP 0.494
  Web of Science (2007): Indexed yes
  Scopus rating (2006): SJR 0.315 SNIP 0.615
  Web of Science (2006): Indexed yes
  Scopus rating (2005): SJR 0.333 SNIP 0.712
  Web of Science (2005): Indexed yes
  Scopus rating (2004): SJR 0.346 SNIP 0.756
  Web of Science (2004): Indexed yes
  Scopus rating (2003): SJR 0.412 SNIP 0.812
  Web of Science (2003): Indexed yes
  Scopus rating (2002): SJR 0.377 SNIP 0.708
  Scopus rating (2001): SJR 0.388 SNIP 0.692
  Scopus rating (2000): SJR 0.31 SNIP 0.643
  Scopus rating (1999): SJR 0.301 SNIP 0.653
Original language: English
Hash function, Cryptanalysis, Collisions, Rebound attack
DOIs:
10.1007/978-3-642-11925-5_24
Rotational Rebound Attacks on Reduced Skein

In this paper we combine a recent rotational cryptanalysis with the rebound attack, which results in the best cryptanalysis of Skein, a candidate for the SHA-3 competition. The rebound attack approach was so far only applied to AES-like constructions. For the first time, we show that this approach can also be applied to very different constructions. In more detail, we develop a number of techniques that extend the reach of both the inbound and the outbound phase, leading to cryptanalytic results on an estimated 53/57 out of the 72 rounds of the Skein-256/512 compression function and the Threefish cipher. The new techniques include an analytical search for optimal input values in the rotational cryptanalysis, which allows to extend the outbound phase of the attack with a precomputation phase, an approach never used in any rebound-style attack before. Further we show how to combine multiple inside-out computations and neutral bits in the inbound phase of the rebound attack, and give well-defined rotational distinguishers as certificates of weaknesses for the compression functions and block ciphers.

Second-Preimage Analysis of Reduced SHA-1

Many applications using cryptographic hash functions do not require collision resistance, but some kind of preimage resistance. That's also the reason why the widely used SHA-1 continues to be recommended in all applications except digital signatures after 2010. Recent work on preimage and second preimage attacks on reduced SHA-1 succeeding up to 48 out of 80 steps (with results barely below the $2^{(n)}$ time complexity of brute-force search) suggest that there is plenty of security margin left. In this paper we show that the security margin is actually somewhat lower, when only second preimages are the goal. We do this by giving two examples, using known differential properties of SHA-1. First, we reduce the complexity of a 2nd-preimage shortcut attack on 34-step SHA-1 from an impractically high complexity to practical complexity. Next, we show a property for up to 61 steps of the SHA-1 compression function that violates some variant of a natural second preimage resistance assumption, adding 13 steps to previously best known results.
Cryptanalysis of Vortex

Vortex is a hash function that was first presented at ISC'2008, then submitted to the NIST SHA-3 competition after some modifications. This paper describes several attacks on both versions of Vortex, including collisions, second preimages, preimages, and distinguishers. Our attacks exploit flaws both in the high-level design and in the lower-level algorithms.
Grøstl Addendum
This document is an addendum to the submission document of Grøstl, which was selected for the second round of NIST’s SHA-3 competition [18]. We stress that we do not change the specification of Grøstl. In other words, Grøstl is defined exactly as specified in the original submission document [8]. In this document we mention a few alternative descriptions of our SHA-3 candidate Grøstl and

General information
State: Published
Organisations: Department of Mathematics, Discrete mathematics
Authors: Gauravaram, P. (Intern), Knudsen, L. R. (Intern), Matusiewicz, K. (Intern), Mendel, F. (Ekstern), Rechberger, C. (Intern), Schläffer, M. (Ekstern), Thomsen, S. S. (Intern), Archives, T. P. S. U. C. (Ekstern)
Number of pages: 5
Publication date: 2009

Publication information
Original language: English
Main Research Area: Technical/natural sciences
Electronic versions:
10.1.1.208.642_1.pdf
Source: dtu
Source-ID: n:oai:DTIC-ART:citeseer/317107626::19492
Publication: Research › Other contribution – Annual report year: 2009

Projects:

Trusted Cryptography
Technical University of Denmark
Period: 01/12/2013 → 12/12/2016
Number of participants: 6
Phd Student:
Kölbl, Stefan (Intern)
Supervisor:
Knudsen, Lars Ramkilde (Intern)
Main Supervisor:
Rechberger, Christian (Intern)
Examiner:
Mödersheim, Sebastian Alexander (Intern)
Johansson, Thomas (Ekstern)
Rijmen, Vincent (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Eksternt finansieret virksomhed

Relations
Publications:
Design and analysis of cryptographic algorithms
Project: PhD

 Trusted Cryptography
Technical University of Denmark
Period: 01/07/2013 → 25/08/2016
Number of participants: 6
Phd Student:
Tiessen, Tyge (Intern)
Supervisor:
Knudsen, Lars Ramkilde (Intern)
Main Supervisor:
Rechberger, Christian (Intern)
Examiner:
Jensen, Christian D. (Intern)
Daemen, Joan (Ekstern)
Johansson, Thomas (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Eksternt finansieret virksomhed

Relations
Publications:
Secure Block Ciphers - Cryptanalysis and Design
Project: PhD

Design and Analysis of Symmetric Primitives
Technical University of Denmark
Period: 01/09/2012 → 19/11/2015
Number of participants: 6
Phd Student:
Lauridsen, Martin Mehl (Intern)
Supervisor:
Knudsen, Lars Ramkilde (Intern)
Main Supervisor:
Rechberger, Christian (Intern)
Examiner:
Beelen, Peter (Intern)
Canteaut, Anne Michele (Intern)
Johansson, Thomas (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Institut stipendie (DTU) Samf.
Project: PhD

Block Cipher Cryptanalysis
Technical University of Denmark
Period: 15/11/2010 → 04/03/2015
Number of participants: 5
Phd Student:
Alkhzaimi, Hoda A. (Intern)
Main Supervisor:
Knudsen, Lars Ramkilde (Intern)
Examiner:
Rechberger, Christian (Intern)
Johansson, Thomas (Ekstern)
Preneel, Bart Karel Benedikt (Ekstern)

**Financing sources**
Source: Internal funding (public)
Name of research programme: Stipendie fra udlandet
Project: PhD

**Cryptanalysis of Some Lightweight Symmetric Ciphers**
Department of Informatics and Mathematical Modeling
Period: 01/01/2010 → 22/03/2013
Number of participants: 7
Phd Student:
Abdelraheem, Mohamed Ahmed A. M. A. (Intern)
Supervisor:
Leander, Gregor (Intern)
Zenner, Erik (Intern)
Main Supervisor:
Knudsen, Lars Ramkilde (Intern)
Examiner:
Rechberger, Christian (Intern)
Canteaut, Anne Michele (Intern)
Johansson, Thomas (Ekstern)

**Financing sources**
Source: Internal funding (public)
Name of research programme: Institut stipendie (DTU)
Project: PhD

**Activities:**

**New Directions in Cryptography**
Period: 7 Dec 2012
Christian Rechberger (Panel member)
Department of Mathematics
Discrete mathematics

**Related event**

**International View of the State-of-the-Art of Cryptography and Security and its Use in Practice**
06/12/2012 → 07/12/2012
Beijing, China
Activity: Talks and presentations › Conference presentations

**New meet-in-the-middle attacks in symmetric cryptanalysis**
Period: 30 Nov 2012
Christian Rechberger (Keynote speaker)
Department of Mathematics
Discrete mathematics

Related event

15th Annual International Conference on Information Security and Cryptology
28/11/2012 → 30/11/2012
Seoul, Korea, Republic of
Activity: Talks and presentations › Conference presentations

PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications
Period: 21 Nov 2012
Christian Rechberger (Invited speaker)
Department of Mathematics

Related event

Workshop on Cryptography for the Internet of Things
20/11/2012 → 21/11/2012
Antwerp, Belgium
Activity: Talks and presentations › Conference presentations

Related-key and Biclique cryptanalysis of AES
Period: 18 Oct 2012
Christian Rechberger (Invited speaker)
Department of Mathematics

Related event

ECRYPT II AES Day 2012
18/10/2012 → ...
Brugges, Belgium
Activity: Talks and presentations › Conference presentations

Yet another cryptanalysis of the AES
Period: 27 Sep 2012
Christian Rechberger (Invited speaker)
Department of Mathematics

Related event

6th Yet Another Conference on Cryptography 2012
24/09/2012 → 28/09/2012
Porquerolles Island, France
Activity: Talks and presentations › Conference presentations

The SHA-3 Competition
Period: 21 Sep 2012
Christian Rechberger (Keynote speaker)
Department of Mathematics

Related event

Bulgarian Cryptography Days
Cryptanalytic ideas for SHA and AES
Period: 11 Aug 2012
Christian Rechberger (Keynote speaker)
Department of Mathematics
Discrete mathematics

Related event

Chinacrypt 2012
09/08/2012 → 12/08/2012
Hefei, China
Activity: Talks and presentations › Conference presentations

Narrow-Bicliques: Cryptanalysis of Full IDEA
Period: 17 Apr 2012
Christian Rechberger (Speaker)
Department of Mathematics
Discrete mathematics

Related event

EUROCRYPT 2012
15/04/2012 → 19/04/2012
Cambridge, United Kingdom
Activity: Talks and presentations › Conference presentations