09031 Abstracts Collection
Symmetric Cryptography
— Dagstuhl Seminar —

Helena Handschuh[1], Stefan Lucks[2], Bart Preneel[3] and Phillip Rogaway[4]

[1] Spansion - Levallois-Perret, F
helena.handschuh@spansion.com
[2] Bauhaus-Universität Weimar, D
stefan.lucks@uni-weimar.de
[3] Katholieke Universiteit Leuven, B
Bart.Preneel@esat.kuleuven.be
[4] Univ. of California - Davis, USA
rogaway@cs.ucdavis.edu

Abstract. From 11.01.09 to 16.01.09, the Seminar 09031 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.

Keywords. Symmetric cryptography, symmetric primitives and cryptoschemes, hash functions, block ciphers, stream ciphers

09031 Executive Summary – Symmetric Cryptography

Research in Symmetric Cryptography is quickly evolving. The seminar was the second of its kind, the first one took place in 2007. 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.

Keywords: Symmetric cryptography, symmetric primitives and cryptoschemes, hash functions, block ciphers, stream ciphers

Joint work of: Handschuh, Helena; Lucks, Stefan; Preneel, Bart; Rogaway, Phillip

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2009/1959

Nostradamus Attack on Tree Hash Functions

Elena Andreeva (Katholieke Universiteit Leuven, BE)

Originally, the Nostradamus attack, also known as chosen target forced prefix preimage attack, was introduced by Kelsey and Kohno in [KeKo06] and applied on strengthened Merkle-Damgard (MD) iterative hash functions. In this work we adapt the attack for the particular case of tree based hash functions. The new Nostradamus attack on tree hash functions differs mainly in the precomputation step from the original attack on the MD construction but has approximately the same complexity (as MD) in its offline, online and memory requirements.

Moreover, we develop a simple long message second preimage attack on tree hash functions and adapt a TMD methods to decrease the computation.

Keywords: Nostradamus attack, tree hash functions

Joint work of: Andreeva, Elena; Dunkelman, Orr; Kelsey, John

See also: [KeKo06] J. Kelsey and T. Kohno, "Herding Hash Functions and the Nostradamus Attack", In EUROCRYPT 2006

Physically Unclonable Pseudorandom Functions

Frederik Armknecht (Ruhr-Universität Bochum, DE)

With the proliferation of physical attacks the implicit assumptions made in traditional security models no longer reflect the real world. To address this issue, a number of new security models, e.g. Algorithmic Tamper-Proof Security, have been proposed. In this work, we take another step and identify the cryptographic properties of a particular family of physical functions, termed as Physically Unclonable Functions (PUFs), that exploit physical phenomena at deep-submicron and nano-scale level. PUFs provide low-cost tamper-evident and tamper-resiliant implementations. Motivated by this fact, we specifcally describe a general method for constructing Pseudorandom Functions (PRFs) from a class of PUFs. We provide a formal model for certain types of PUFs that build the basis for PRFs, which we call PUF-PRFs. Furthermore, we show experimentally that some real world PUF instantiations (e.g.,SRAM PUFs) satisfy the model. This strongly indicates that PUF-PRFs can indeed be physically realized. Finally, we describe two symmetric ciphers that use PUF-PRFs as building blocks.

Keywords: Pseudorandom Functions, Physically Unclonable Functions

Joint work of: Armknecht, Frederik; Roel, Maes; Ahmad, Reza-Sadeghi; Berk, Sunar; Pim, Tuyls

Cube Testers and Key Recovery Attacks On Reduced-Round MD6 and Trivium

Jean-Philippe Aumasson (FH Nordwestschweiz - Brugg, CH)

This talk presents cube testers, a new class of attacks that combines cube attacks and efficient property-testing algorithms. The power of cube testers is illustrated with attacks on reduced-round Trivium and MD6.

Keywords: Cube attacks, property testing, MD6, Trivium

Joint work of: Aumasson, Jean-Philippe; Dinur, Itai; Meier, Willi; Shamir, Adi

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/1944

Bug attacks

Eli Biham (Technion - Haifa, IL)

We present a new kind of cryptanalytic attack which utilizes bugs in the hardware implementation of computer instructions. The best known example of such a bug is the Intel division bug, which resulted in slightly inaccurate results for extremely rare inputs. Whereas in most applications such bugs can be viewed as a minor nuisance, we show that in the case of RSA (even when protected by OAEP), Pohlig-Hellman, elliptic curve cryptography, and several other schemes, such bugs can be a security disaster: Decrypting ciphertexts on *any* computer which multiplies *even one pair of numbers* incorrectly can lead to full leakage of the secret key, sometimes with a single well-chosen ciphertext. The implications to public key cryptosystems and secret key cryptosystems are discussed.

Keywords: Bug attack, Fault attack, Side-channel attack, RSA, ECC, Pohlig-Hellman

Joint work of: Biham, Eli; Carmeli, Yaniv; Shamir, Adi

See also: proceedings of CRYPTO 2008

Design of AES-based hash-functions: LUX and Cheetah

Alex Biryukov (University of Luxembourg, LU)

In this talk we describe design process and ideas behind the two new hash functions LUX and Cheetah.

LUX is a stream based hash function. Cheetah is a block-cipher based one, using MD-HAIFA mode.

We will also discuss issues related to the SHA-3 competition: speed vs. security, parallel vs. sequential attacks, possible selection scenario for the 1st round.

Keywords: Hash functions, design and cryptanalysis

Joint work of: Biryukov, Alex; Khovratovich, Dmitry ; Nikolic, Ivica

MutantXL: Solving Multivariate Polynomial Equations for Cryptanalysis

Johannes A. Buchmann (TU Darmstadt, DE)

MutantXL is an algorithm for solving systems of polynomial equations that was proposed at SCC 2008 and improved in PQC 2008. This article gives an overview over the MutantXL algorithm. It also presents experimental results comparing the behavior of the MutantXL algorithm to the F_4 algorithm on HFE and randomly generated multivariate systems. In both cases MutantXL is faster and uses less memory than the Magma's implementation of F_4.

Keywords: Multivariate systems, MutantXL

Joint work of: Buchmann, Johannes A.; Ding, Jintai; Mohamed, Mohamed Saied Emam; Mohamed, Wael Said Abd Elmageed

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/1945

Sufficient conditions for sound tree hashing modes

Joan Daemen (STMicroelectronics - Zaventem, BE)

We consider the general case of tree hashing modes that make use of an underlying compression function. We consider such a tree hashing mode sound if differentiating it from a random oracle, assuming the underlying compression function is a random oracle can be proven to be hard. We demonstrate two properties that such a tree hashing mode must have for such a proof to exist. For each of the two properties we show that several solutions exist to realize them. For some given solutions we demonstrate that a simple proof of indifferentiability exists and obtain an upper bound on the differentiability probability of $q^2/2^n$ with q the number of queries to the underlying compression function and n its output length. Finally we give two examples of hashing modes for which this proof applies: KeccakTree and Prefix-free Merkle-Damgard.

Keywords: Tree Hashing, Indifferentiability

Joint work of: Guido, Bertoni; Joan, Daemen; Michaël, Peeters; Gilles, Van Assche

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/1946

New Results on Optimal Fixed Length Physical Random Number Post-Processing Functions

Markus Dichtl (Siemens - München, DE)

When functions with n input bits and m output bits are used for post-processing the output of a physical random number generator, which is assumed to produce statistically independent bits with a fixed bias ϵ, the probabilities of the 2^m outputs can be represented as polynomials in ϵ. For a good post-processing function all low powers of ϵ should have coefficients of zero. K. Suzuki and T. Iwata showed in the paper "Bounds on Fixed Input/Output Length Post-Processing Functions for Biased Physical Random Number Generators" presented at SAC 2008 for most cases with $1 \leq m \leq n \leq 16$ how many low powers of ϵ can be maximally eliminated, but there were 13 cases remaining open. This paper solves these 13 cases.

Keywords: Postprocessing, physical random numbers

Some positive and negative results on Cube-style attacks / The pseudo-euclidian algorithm

Thomas Dullien (zynamics GmbH - Bochum, DE)

This talk discusses a few small results related to cube-style algebraic attacks. It is shown that in a white-box scenario with

$$f = ml + r$$

and ($degl = 1$)), the complexity of extracting l is much less than $2^{\deg m}$ oracle queries – this means the attacker does not need to sum over the entire cube, just over a much smaller subset. An algorithm is provided to construct such smaller subsets.

It is further shown that generalizing cube-style attacks to decompositions of the form

$$f = pl + r$$

(where p is a polynomial) is unlikely to yield many benefits over the monomial scenario.

The second talk presents some results that show that the ring of boolean functions, even though it is not euclidian, allows for an algorithm that performs an equivalent task: Given a set of n generators for an ideal, the algorithm can calculate the single generator for the entire ideal (the ring of boolean functions is a principal ideal domain) in n polynomial multiplications and $n + 1$ polynomial additions.

A number of interesting results follow from this:

- Calculating the product of a set of boolean functions which have one solution in common is equivalent to solving them
- Estimating the number of monomials in the product gives information about the hamming weight of the solution
- Restrictions of boolean functions to particular subsets can be calculated easily

Keywords: Cube attacks, algebraic attacks, poset, lattice, boolean functions, euclidian algorithm, principal ideal domain

SHAvite-3 - A New and Secure Hash Function Proposal

Orr Dunkelman (ENS - Paris, FR)

In this work we present SHAvite-3, a secure and efficient hash function based on the HAIFA construction and the AES building blocks. SHAvite-3 uses a well understood set of primitives such as a Feistel block cipher which iterates a round function based on the AES round. SHAvite-3's compression functions are secure against cryptanalysis, while the selected mode of iteration offers maximal security against black box attacks on the hash function. SHAvite-3 is both fast and resource-efficient, making it suitable for a wide range of environments, ranging from 8-bit platforms to 64-bit platforms (and beyond).

Keywords: SHAvite-3, SHA-3, hash function

Joint work of: Dunkelman, Orr; Biham, Eli

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/1947

Aggregation of Message Authentication Codes

Marc Fischlin (TU Darmstadt, DE)

Aggregation schemes combine several MACs into a single value in order to reduce the communication overhead. A prominent example is the MAC scheme by Katz and Lindell (CT-RSA 2008) which supports aggregation in arbitrary order (as opposed to many schemes allowing only sequential aggregation). Here we revisit their unforgeability notion and discuss that the definitions do not prevent "mixing" attacks in which the adversary combines several aggregates. In particular, we show concrete attacks on these schemes.

We thus provide the stronger security notion of aggregation unforgeability, capturing a much broader class of combination attacks. We then present aggregation-unforgeable constructions somewhat lying between non-ordered and sequential solutions.

That is, we propose the notion of history-free sequential aggregation, a refinement which basically says that the aggregation algorithm must not depend on the preceding messages in the sequence but only on the shorter input aggregate and the local message. We finally show how to build such history-free protocols.

Keywords: Aggregation, Message Authentication Code, Unforgeability

Classification of the SHA-3 Candidates

Christian Forler (Sirrix AG Bochum, DE)

In this note we give an overview on the current state of the SHA-3 candidates. First, we classify all publicly known candidates and, second, we outline and summarize the performance data as given in the candidates documentation for 64-bit and 32-bit implementations. We define performance classes and classify the hash algorithms. Note, that this article will be updated as soon as new candidates arrive or new cryptanalytic results get published. Comments to the authors of this article are welcome.

Keywords: Hash function, SHA-3, classification

Joint work of: Forler, Christian; Fleischmann, Ewan; Gorski, Michael

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/1948

Full Paper:
http://eprint.iacr.org/2008/511

The Lane hash function

Sebastiaan Indesteege (Katholieke Universiteit Leuven, BE)

We propose the cryptographic hash function Lane as a candidate for the SHA-3 competition organised by NIST. Lane is an iterated hash function supporting multiple digest sizes. Components of the AES block cipher are reused as building blocks. Lane aims to be secure, easy to understand, elegant and flexible in implementation. We give the specification of Lane, and the rationale behind the important design choices. For a more extended specification, security analysis and a discussion of the implementation aspects, we refer to the Lane submission document.

Keywords: Lane, SHA-3 candidate, hash function

Joint work of: Indesteege, Sebastiaan; Andreeva, Elena; De Cannière, Christophe; Dunkelman, Orr; Käsper, Emilia; Nikova, Svetla; Preneel, Bart; Tischhauser, Elmar

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/1952

Full Paper:
http://www.cosic.esat.kuleuven.be/lane/

Practical Collisions for EnRUPT

Sebastiaan Indesteege (Katholieke Universiteit Leuven, BE)

The EnRUPT hash functions were proposed by O'Neil, Nohl and Henzen as candidates for the SHA-3 competition, organised by NIST. The proposal contains seven hash functions, each having a different digest length. We present a practical collision attack on all of these seven EnRUPT variants.

The time complexity of our attack varies from 2^{36} to 2^{40} round computations, depending on the EnRUPT variant, and the memory requirements are negligible. We demonstrate that our attack is practical by giving an actual collision example for EnRUPT-256.

Keywords: EnRUPT, SHA-3 candidate, hash function, collision attack

Joint work of: Indesteege, Sebastiaan; Preneel, Bart

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/1950

See also: Proceedings of Fast Software Encryption 2009, Lecture Notes in Computer Science, Springer (to appear).

Practical Preimages for Maraca

Sebastiaan Indesteege (Katholieke Universiteit Leuven, BE)

We show a practical preimage attack on the cryptographic hash function Maraca, which was submitted as a candidate to the NIST SHA-3 competition. Our attack has been verified experimentally.

Keywords: Maraca, hash function, preimage attack

Joint work of: Indesteege, Sebastiaan; Preneel, Bart

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2009/1951

On the Impact of Key Check Value on CBC MACs and Others

Tetsu Iwata (Nagoya University, JP)

ANSI X9.24, Annex C, "Retail Financial Services, Symmetric Key Management" specifies the use of a key check value (KCV), which is a part of the ciphertext of a binary zero value.

In this talk, we discuss the impact of using KCV on the security of CBC MAC variants, EMAC and CMAC. We present attacks, provable security results, and possible fixes.

Keywords: CMAC, EMAC, key check value, proof of security.

Key recovery Attack on Interactable Keyed Functions

Shahram Khazaei (EPFL - Lausanne, CH)

In cryptology we commonly face the problem of finding an unknown key K from the output of an interactable keyed function F(V, K). The input parameter V is a publicly controllable value which makes F interactable in the sense that an oracle provides the adversary with the output value of the function for any V of her choice and for any fixed random key. The goal of the adversary is to recover K as efficiently as possible. This talk gives an overview of the recent works done in this direction by Vielhaber [eprint'07], Fischer-Khazaei-Meier [Africacrypt'08], Dinur-Shamir [eprint'08] and Khazaei-Meier [Indocrypt'08]. In particular apply the method to Klomov-Shamir's T-function based self-synchronizing stream cipher.

Keywords: Key recovery attack, interactable function, self-synchronizing stream cipher, cube attack.

Joint work of: Khazaei, Shahram; Meier, Willi

Gaussian cryptanalysis of hash functions: collisions, preimages, distinguishers

Dimitry Khovratovich (University of Luxemburg, LU)

Many attacks on hash functions can be reformulated in finding a hash execution with constraints being fixed values of internal variables. Those variables can be input or output bits, input of active S-boxes or AND operations, etc..

The constraints lead to a system of nonlinear equations, which sometimes can be solved with a fast algorithm resembling the Gaussian elimination. If a system has been solved then solutions can be produced with negligible time costs.

The main condition for the algorithm to succeed is relatively slow diffusion in the attacked primitive. Provided this we show how to attack AES as a hash function and prove that a 30-round MD6 compression function can be distinguished from the random oracle.

I will also show how it worked in practice in a GUI-tool.

Keywords: Hash functions, cryptanalysis, Gauss, AES

Message Authentication for Streams with Delayed Keys

Anja Lehmann (TU Darmstadt, DE)

We consider message authentication codes for streams where the key becomes known only at the end of the stream. This usually happens in key-exchange protocols like SSL and TLS where the exchange phase concludes by sending a MAC for the previous transcript and the newly derived key. SSL and TLS provide tailor-made solutions for this problem (modifying HMAC to insert the key only at the end, as in SSL, or using upstream hashing as in TLS). Here we take a formal approach to this problem of delayed-key MACs and provide solutions which are as secure as schemes where the key would be available right away but still allow to compute the MACs online even if the key becomes known only later.

Joint work of: Fischlin, Marc; Lehmann, Anja

Mini-ciphers: a reliable testbed for cryptanalysis?

Jorge Nakahara (EPFL - Lausanne, CH)

This talk addresses the issue of miniaturized cryptographic primitives, with particular focus on block ciphers. Examples include mini-versions of IDEA and the AES, which are straightforward to derive because they operate word wise. Mini-ciphers are often used as testbeds for new attacks, in order to collect data such as success rate and to corroborate theoretical predictions. An implicit assumption of this approach is that results on mini-ciphers shall equally apply to the original cipher. But, is it always the case? In this talk, I will present some experiments on higher-order square attacks applied to mini-AES versions.

Keywords: Cryptanalysis of block ciphers, mini-ciphers, AES, square attacks

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/1961

Internal collision attack on Maraca

Maria Naya-Plasencia (INRIA Paris-Rocquencourt, FR)

We present an internal collision attack against the new hash function Maraca which has been submitted to the SHA-3 competition.

This attack requires 2^{237} calls to the round function and its complexity is lower than the complexity of the generic collision attack when the length of the message digest is greater than or equal to 512. It is shown that this cryptanalysis mainly exploits some particular differential properties of the inner permutation, which are in some sense in contradiction with the usual security criterion which guarantees the resistance to differential attacks.

Keywords: Hash function, collision attack, differential cryptanalysis, Boolean function

Joint work of: Canteaut, Anne; Naya-Plasencia, Maria

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/1953

Statistical tests for multidimensional extension of Matsui's Algorithm 1

Kaisa Nyberg (Helsinki University of Technology, FI)

We show that extending Matsui's Algorithm 1 to using multiple linear approximations leads to a statistical goodness-of-fit problem. We examine common statistical goodness-of-fit tests, propose a new one based on LLR, estimate their performance, and experiment on key recovery with key ranking using these tests.

Statistical Tests for Key Recovery Using Multidimensional Extension of Matsui's Algorithm 1

Kaisa Nyberg (Helsinki University of Technology, FI)

In one dimension, there is essentially just one binomially distributed statistic, bias or correlation, for testing correctness of a key bit in Matsui's Algorithm 1. In multiple dimensions, different statistical approaches for finding the correct key candidate are available. The purpose of this work is to investigate the efficiency of such test in theory and practice, and propose a new key class ranking statistic using distributions based on multidimensional linear approximation and generalisation of the ranking statistic presented by Selçuk.

Keywords: Block cipher, key recovery attacks, key ranking, linear cryptanalysis, multidimensional approximation

Joint work of: Hermelin, Miia; Cho, Joo Yeon; Nyberg, Kaisa

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/1954

Grøstl - a SHA-3 candidate

Christian Rechberger (TU Graz, AT)

Grøstl is a SHA-3 candidate proposal. Grøstl is an iterated hash function with a compression function built from two fixed, large, distinct permutations. The design of Grøstl is transparent and based on principles very different from those used in the SHA-family.

The two permutations are constructed using the wide trail design strategy, which makes it possible to give strong statements about the resistance of Grøstl against large classes of cryptanalytic attacks. Moreover, if these permutations are assumed to be ideal, there is a proof for the security of the hash function.

Grøstl is a byte-oriented SP-network which borrows components from the AES. The S-box used is identical to the one used in the block cipher AES and the diffusion layers are constructed in a similar manner to those of the AES. As a consequence there is a very strong confusion and diffusion in Grøstl.

Grøstl is a so-called wide-pipe construction where the size of the internal state is significantly larger than the size of the output. This has the effect that all known, generic attacks on the hash function are made much more difficult.

Grøstl has good performance on a wide range of platforms and countermeasures against side-channel attacks are well-understood from similar work on the AES.

Keywords: SHA-3 proposal, hash function

Joint work of: Gauravaram, Praveen; Knudsen, Lars R.; Matusiewicz, Krystian; Mendel, Florian; Rechberger, Christian; Schläffer, Martin; Thomsen Søren S.

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/1955

Full Paper:
http://www.groestl.info

A Provably Secure and Efficient Hash Function Framework

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

This humorous talk presents a hash function called O'Toole. It is only a joke. It is not real.

Keywords: Hash Function

Parallel generation of l-sequences

Andrea Röck (INRIA Paris-Rocquencourt, FR)

The generation of pseudo-random sequences at a high rate is an important issue in modern communication schemes. The representation of a sequence can be scaled by decimation to obtain parallelism and more precisely a sub-sequences generator.

Sub-sequences generators and therefore decimation have been extensively used in the past for linear feedback shift registers (LFSRs). However, the case of automata with a non linear feedback is still in suspend. In this work, we have studied how to transform of a feedback with carry shift register (FCSR) into a

sub-sequences generator. We examine two solutions for this transformation, one based on the decimation properties of ℓ-sequences, *i.e.* FCSR sequences with maximal period, and the other one based on multiple steps implementation.

We show that the solution based on the decimation properties leads to much more costly results than in the case of LFSRs. For the multiple steps implementation, we show how the propagation of carries affects the design.

This work represents a cooperation with Cédric Lauradoux and was presented at the international conference on SEquences and Their Applications (SETA) 2008.

Keywords: Sequences, synthesis, decimation, parallelism, LFSRs, FCSRs

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/1956

Full Paper:
http://www-rocq.inria.fr/secret/Andrea.Roeck/pdfs/articleSETA08.pdf

See also: Parallel Generation of l-Sequences - C. Lauradoux and A. Röck - in Proceedings of SETA 2008, Lexington, Kentucky, USA, September, 4-18, 2008, LNCS vol.5203, pp. 299-312

The Rebound Attack - Cryptanalysis of Whirlpool

Martin Schläffer (TU Graz, AT)

Whirlpool is a block cipher based hash functions with a strong key schedule.

The wide trail design strategy of this hash function makes the application of standard differential and linear attacks seemingly difficult. Hence, virtually no cryptanalytic results on Whirlpool have been published since its proposal eight years ago.

In this work, we propose the Rebound Attack, consisting of a match-in-the-middle technique and a subsequent inside-out approach. We apply the Rebound attack to hash functions and compression function designed according to the wide trail design strategy. We present an attack on Whirlpool for 7.5 of 10 rounds, and apply the attack to 8.5 rounds of the compression function Maelstrom and 5 rounds of the Grøstl compression function.

Keywords: Rebound Attack, Whirlpool, Maelstrom, Grøstl, hash function, collision attack

Joint work of: Mendel, Florian; Rechberger, Christian; Schläffer, Martin; Thomsen, Søren S.

Some Remarks on FCSRs and Implications for Stream Ciphers

Dirk Stegemann (Universität Mannheim, DE)

Feedback with carry shift registers (FCSRs) are extensively discussed in the context of pseudorandom number generation and as building blocks for stream ciphers. Similarly to linear feedback shift registers, FCSRs may be represented in Galois and in Fibonacci architecture. We describe the first formal characterization of periodic Galois states and show an efficient mapping between periodic Galois states and periodic Fibonacci states. Additionally we provide a method for explicitly computing the autocorrelation of maximum-period FCSR sequences and discuss the impact of our findings on the design of stream ciphers.

Keywords: FCSR, F-FCSR, stream cipher design

Algebraic Attacks against Linear RFID Authentication Protocols

Dirk Stegemann (Universität Mannheim, DE)

The limited computational resources available on RFID tags imply a need for specially designed authentication protocols. The light weight authentication protocol HB^+ proposed by Juels and Weis seems currently secure for several RFID applications, but is too slow for many practical settings.

As a possible alternative, authentication protocols based on choosing random elements from L secret linear n-dimensional subspaces of $GF(2)^{n+k}$ (so called linear (n, k, L)-protocols), have been considered. We show that to a certain extent, these protocols are vulnerable to algebraic attacks. Particularly, our approach allows to break Cichoń, Klonowski and Kutyłowski's CKK^2-protocol, a special linear $(n, k, 2)$-protocol, for practically recommended parameters in less than a second on a standard PC. Moreover, we show that even unrestricted (n, k, L)-protocols can be efficiently broken if L is too small.

Keywords: RFID Authentication, HB+, CKK, CKK2

Joint work of: Krause, Matthias; Stegemann, Dirk

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/1957

Making a MAC from a blockcipher that is only a MAC

John Steinberger (Univ. of British Columbia, CA)

We show how to build a variable-input-length MAC (VIL-MAC) from a blockcipher, where the only security requirement on the blockcipher is that it be a MAC, instead of a PRP.

Keywords: Message authentication codes, Shrimpton-Stam construction, Block-ciphers

Joint work of: Dodis, Yevgeniy; Steinberger, John

The Road from Panama to Keccak via RadioGatún

Gilles Van Assche (STMicroelectronics - Zaventem, BE)

In this presentation, we explain the design choices of Panama [1] and RadioGatun [2], which lead to Keccak [3]. After a brief recall of Panama, RadioGatun and the trail backtracking cost, we focus on three important aspects. First, we explain the role of the belt in the light of differential trails. Second, we discuss the relative advantages of a block mode hash function compared to a stream mode one. Finally, we point out why Panama and RadioGatun are not sponge functions and why their design philosophy differs from that of Keccak.

Keywords: Hash function, cryptography

Joint work of: Bertoni, Guido; Daemen, Joan; Peeters, Michael; Van Assche, Gilles

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/1958

See also: [1] J. Daemen and C. S. K. Clapp, FSE 1998; [2] G. Bertoni et al., NIST Hash Workshop 2006; [3] G. Bertoni et al., SHA-3 submission, 2008

Smashing SQUASH-0

Serge Vaudenay (EPFL - Lausanne, CH)

At the RFID Security Workshop 2007, Adi Shamir presented a new challenge-response protocol well suited for RFIDs, although based on the Rabin public-key cryptosystem. This protocol, which we call SQUASH-0, was using a linear mixing function which was subsequently withdrawn. Essentially, we mount an attack against SQUASH-0 with full window which could be used as a "known random coins attack" against Rabin-SAEP. We then extend it for SQUASH-0 with arbitrary window. We apply it with the proposed modulus $2^{1277}-1$ to run a key recovery attack using 1024 chosen challenges. Since the security arguments equally apply to the final version of SQUASH and to SQUASH-0, we challenge the blame-game argument for the security of SQUASH. Nevertheless, our attacks are inefficient when using non-linear mixing so the security of SQUASH remains open.

Keywords: Cryptanalysis, chqllenge-response protocol, Rabin encryption

Joint work of: Ouafi, Khaled; Vaudenay, Serge

AXR - Crypto Made from Modular Additions, XORs and Word Rotations

Ralf-Philipp Weinmann (University of Luxemburg, LU)

Many symmetric cryptographic primitives are composed solely of modular additions, XORs and word rotations - we call these primitives AXR primitives; usually with words sizes of either 32 or 64 bits. With the SHA-3 competition, the number of these primitives has increased again. However, the general problem of solving equations coming from AXR primitives is not studied in the cryptographic literature. This talk shows some preliminary results on how to solve these equations.

Keywords: Non-linear equations AXR AddXorRol

DECT security

Ralf-Philipp Weinmann (University of Luxemburg, LU)

We present the first public analysis of the DECT security standards and implementations thereof. We show how the DECT Standard Cipher (DSC) was reverse engineered and explain severe problems in the authentication mechanisms used by DECT. One of allows an attacker to re-reroute outgoing calls made by handsets, the other is an implementation error that can lead to a practical key-recovery attack on the UAK for various implementations.

Keywords: Dect dsc dsaa cryptanalysis protocol

Joint work of: Weinmann, Ralf-Philipp; Andreas, Schuler; Erik, Tews; Matthias, Wenzel

Musings on wide-block block ciphers

Doug Whiting (Hi/fn Inc.- Carlsbad, US)

A presentation of the Threefish tweakable block cipher used in the Skein hash function submitted to the NIST SHA-3 competition.

In addition, properties of Threefish if scaled up to even larger block sizes were discussed.

Cache Timing Analysis of eStream Finalists

Erik Zenner (Technical University of Denmark, DK)

Cache Timing Attacks have attracted a lot of cryptographic attention due to their relevance for the AES.

However, their applicability to other cryptographic primitives is less well researched. In this talk, we give an overview over our analysis of the stream ciphers that were selected for phase 3 of the eStream project.

Keywords: Cache timing attacks, stream ciphers

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2009/1943