Lecture Notes in Computer Science 8885

More information about this series at http://www.springer.com/series/7410

Willi Meier · Debdeep Mukhopadhyay (Eds.)

Progress in Cryptology – INDOCRYPT 2014

15th International Conference
on Cryptology in India
New Delhi, India, December 14–17, 2014
Proceedings

Springer

Editors
Willi Meier
Fachhochschule Nordwestschweiz
Hochschule für Technik
Windisch
Switzerland

Debdeep Mukhopadhyay
Computer Science and Engineering
Indian Institute of Technology
Kharagpur
India

ISSN 0302-9743 ISSN 1611-3349 (electronic)
ISBN 978-3-319-13038-5 ISBN 978-3-319-13039-2 (eBook)
DOI 10.1007/978-3-319-13039-2

Library of Congress Control Number: 2014953958

LNCS Sublibrary: SL4 – Security and Cryptology

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

We are glad to present the proceedings of INDOCRYPT 2014, held during 14–17 December in New Delhi, India. INDOCRYPT 2014 is the 15th edition of the INDOCRYPT series organized under the aegis of the Cryptology Research Society of India (CRSI). The conference has been organized by the Scientific Analysis Group (SAG), DRDO, New Delhi, India. The INDOCRYPT series of conferences began in 2000 under the leadership of Prof. Bimal Roy of Indian Statistical Institute.

In response to the call for papers, we received 101 submissions from around 30 countries around the globe. The submission deadline was July 28, 2014. The review process was conducted in two stages: In the first stage, most papers were reviewed by at least four committee members, while papers from Program Committee members received at least five reviews. This was followed by a week-long online discussion phase to decide on the acceptance of the submissions. The Program Committee was also suitably aided in this tedious task by 94 external reviewers to be able to complete this as per schedule, which was on September 7. Finally, 25 submissions were selected for presentation at the conference.

We would like to thank the Program Committee members and the external reviewers for giving every paper a fair assessment in such a short time. The refereeing process resulted in 367 reviews, along with several comments during the discussion phase. The authors had to revise their papers according to the suggestions of the referees and submit the camera-ready versions by September 22.

We were delighted that Phillip Rogaway, Marc Joye, and María Naya-Plasencia agreed to deliver invited talks on several interesting topics of relevance to INDOCRYPT. The program was also enriched to have Claude Carlet and Florian Mendel as Tutorial speakers on important areas of Cryptography, to make the conference program complete.

We would like to thank the General Chairs, Dr. G. Athithan and Dr. P.K. Saxena, for their advice and for being a prime motivator. We would also like to specially thank the Organizing Chair Saibal K. Pal and the Organizing Secretary Sucheta Chakrabarty for developing the layout of the program and in managing the financial support required for such a conference. Our job as Program Chairs was indeed made much easier by the software, easychair. We also say our thanks to Durga Prasad for maintaining the webpage for the conference. We would also acknowledge Springer for their active cooperation and timely production of the proceedings.

Last but certainly not least, our thanks go to all the authors, who submitted papers to INDOCRYPT 2014, and all the attendees. Without your support the conference would not be a success.

December 2014

Willi Meier
Debdeep Mukhopadhyay

Message from the General Chairs

Commencing from the year 2000, INDOCRYPT — the International Conference on Cryptology — is held every year in India. This event has been one of the regular activities of the Cryptology Research Society of India (CRSI) to promote R&D in the area of Cryptology in the country. The conference is hosted by different organizations including Academic as well as R&D organizations located across the country. The Scientific Analysis Group (SAG), one of the research laboratories of the Defence Research and Development Organization (DRDO), organized the conference in the years 2003 and 2009 in collaboration with the Indian Statistical Institute (Delhi Centre) and Delhi University, respectively. SAG was privileged to get an opportunity to organize INDOCRYPT 2014, the 15th conference in this series. Since its inception, the INDOCRYPT has proved to be a powerful platform for researchers to meet, share their ideas with their peers, and work toward the growth f cryptology, especially in India. For each edition of the conference in the past, the response from the cryptology research community has been overwhelming and the esponse for the current edition is no exception. As is evident from the quality of submissions and the a high rate of rejections due to a transparent and rigorous process of reviewing, the conference has been keeping its standards with proceedings published by LNCS. Even this year, the final set of selected papers amount to a net acceptance ratio of 25 percent.

On the first day of the conference, there were two Tutorials on the topics of S-Boxes and Hash Functions. They were delivered by Claude Carlet of University of Paris, France and Florian Mendel of Graz University of Technology, Austria. Both the Tutorials provided the participants with deep understanding of the chosen topics and stimulated discussions among others. Beginning from the second day, the main conference had three invited talks and 25 paper presentations for 3 days. Maria Naya-Plasencia of Inria (France), Marc Joye of Technicolor (USA), and Phillip Rogaway of University of California (USA) delivered the invited talks on Lightweight Block Ciphers and Their Security, Recent Advances in ID-Based Encryption, and Advances in Authenticated Encryption, respectively. We are grateful to all the Invited and Tutorial Speakers.

Organizing a conference having such wide ranging involvement and participation from international crypto community is not possible without the dedicated efforts of different committees drawn from the hosting and other support agencies. The Organizing Committee took care of all the logistic, coordination, and financial aspects concerning the conference under the guidance of the Organizing Chair Saibal K. Pal and the Organizing Secretary Sucheta Chakrabarty. We thank both of them and all the members of these committees for their stellar efforts.

Equally demanding is the task of the Program Committee in coordinating the submissions and in selecting the papers for presentation. The Program Co-Chairs Willi Meier and Debdeep Mukhopadhyay were the guiding forces behind the efforts of the Program Committee. Their love for the subject and the commitment to the cause of promoting Cryptology Research in India and elsewhere is deep and we thank them for putting together an excellent technical program. We also thank all the members of the Program Committee for their support to the Program Co-chairs. Special thanks are due to the Reviewers for their efforts and for sharing their comments with concerned persons, which led to completing the selection process in time.

We express our heartfelt thanks to DRDO and CRSI for being the mainstay in ensuring that the Conference received all the support that it needed. We also thank NBHM, DST, Deity, ISRO, CSIR, RBI, BEL, ITI, IDRBT, Microsoft, Google, TCS, and others for generously supporting/sponsoring the event. Finally, thanks are due to the authors who submitted their work, especially to those whose papers are included in the present Proceedings of INDOCRYPT 2014 and those who could make it to present their papers personally in the Conference.

December 2014

P.K. Saxena
G. Athithan

Organization

General Chairs

P.K. Saxena	SAG, DRDO, New Delhi, India
G. Athithan	SAG, DRDO, New Delhi, India

Program Chairs

Willi Meier	FHNW, Switzerland
Debdeep Mukhopadhyay	Indian Institute of Technology Kharagpur, India

Program Committee

Martin Albrecht	Technical University of Denmark, Denmark
Subidh Ali	NYU, Abu Dhabi
Elena Andreeva	KU Leuven, Belgium
Frederik Armknecht	Universität Mannheim, Germany
Daniel J. Bernstein	University of Illinois at Chicago, USA
Céline Blondeau	Aalto University School of Science, Finland
Christina Boura	Université de Versailles Saint-Quentin-en-Yvelines, France
C. Pandurangan	Indian Institute of Technology Madras, India
Anne Canteaut	Inria, France
Nishanth Chandran	Microsoft Research, India
Sanjit Chatterjee	Indian Institute of Science Bangalore, India
Abhijit Das	Indian Institute of Technology Kharagpur, India
Sylvain Guilley	TELECOM-ParisTech and Secure-IC S.A.S., France
Abhishek Jain	MIT and BU, USA
Dmitry Khovratovich	University of Luxembourg, Luxembourg
Tanja Lange	Technische Universiteit Eindhoven, The Netherlands
Willi Meier	FHNW, Switzerland
Debdeep Mukhopadhyay	Indian Institute of Technology Kharagpur, India
David Naccache	Université Paris II, Panthéon-Assas, France
Phuong Ha Nguyen	Indian Institute of Technology Kharagpur, India
Saibal K. Pal	SAG, DRDO, New Delhi, India
Goutam Paul	Indian Statistical Institute Kolkata, India
Christiane Peters	ENCS, The Netherlands

Thomas Peyrin	Nanyang Technological University, Singapore
Josef Pieprzyk	ACAC, Australia
Rajesh Pillai	SAG, DRDO, New Delhi, India
Axel Poschmann	NXP Semiconductors, Germany
Bart Preneel	KU Leuven, Belgium
Chester Rebeiro	Columbia University, USA
Vincent Rijmen	KU Leuven and iMinds, Belgium
Bimal Roy	Indian Statistical Institute, Kolkata, India
Dipanwita Roy Chowdhury	Indian Institute of Technology Kharagpur, India
S.S. Bedi	SAG, DRDO, New Delhi, India
Sourav Sen Gupta	Indian Statistical Institute, Kolkata, India
Francois-Xavier Standaert	UCL Crypto Group, Belgium
Ingrid Verbauwhede	KU Leuven, Belgium

External Reviewers

Tamaghna Acharya
Ansuman Banerjee
Ayan Banerjee
Harry Bartlett
Begül Bilgin
Joppe Bos
Seyit Camtepe
Sucheta Chakrabarti
Avik Chakraborti
Kaushik Chakraborty
Anupam Chattopadhyay
Roopika Chaudhary
Chien-Ning Chen
Kang Lang Chiew
Dhananjoy Dey
Manish Kant Dubey
Pooya Farshim
Aurélien Francillon
Lubos Gaspar
Benoît Gérard
Hossein Ghodosi
Santosh Ghosh
Shamit Ghosh
Vincent Grosso
Divya Gupta
Indivar Gupta
Nupur Gupta
Jian Guo
Sartaj Ul Hasan
Gregor Leander
Wang Lei
Feng-Hao Liu
Atul Luykx
Subhamoy Maitra
Bodhisatwa Mazumdar
Florian Mendel
Bart Mennink
Nele Mentens
Prasanna Mishra
Paweł Morawiecki
Imon Mukherjee
Nicky Mouha
Michael Naehrig
Ivica Nikolić
Ventzi Nikov
Omkant Pandey
Sumit Pandey
Tapas Pandit
Kenny Paterson
Arpita Patra
Ludovic Perret
Léo Perrin
Christophe Petit
Bertram Poettering
Romain Poussier
Michaël Quisquater
Francesco Regazzoni
Michał Ren

Yj Huang
Andreas Hülsing
Hassan Jameel Asghar
Kimmo Järvinen
Jeremy Jean
Bhavana Kanukurthi
Sabyasachi Karati
Pierre Karpman
Oleksandr Kazymyrov
Manas Khatua
Dakshita Khurana
Markulf Kohlweiss
Sukhendu Kuila
Manoj Kumar
Vijay Kumar
Yogesh Kuma
Mario Lamberger
Martin M. Lauridsen
Dhiman Saha
Abhrajit Sengupta
Sujoy Sinha Roy
Dale Sibborn
Dave Singelee
Ron Steinfeld
Valentin Suder
Aris Tentes
Tyge Tiessen
Meilof Veeningen
Muthuramakrishnan Venkitasubramaniam
Frederik Vercauteren
Dhinakaran Vinayagamurthy
Jo Vliegen
Qingju Wang
Bohan Yang
Wentao Zhang
Ralf Zimmermann

Local Organizing Committee

Saibal K. Pal (Organizing Chair)
Kanika Bhagchandani
Dhananjoy Dey
Sartaj Ul Hasan
Gopal C. Kandpal
Ashok Kumar
P.R. Mishra
Manoj Kumar Singh
Divya Anand Subba
Sucheta Chakrabarti (Organizing Secretary)
Vivek Devdhar
Indivar Gupta
Mohammad Javed
Sarvjeet Kaur
Girish Mishra
Bhartendu Nandan
Ajay Srivastava

Invited Talks

S-boxes, Their Computation and Their Protection against Side Channel Attacks

Claude Carlet*

First Part of the Talk

*After recalling the necessary background on S-boxes (see below), we shall study the criteria for substitution boxes (*S-boxes*) in block ciphers:*

1. *bijectivity when used in SP networks, and if possible balancedness when used in Feistel ciphers,*
2. *high nonlinearity (for the resistance to linear attacks),*
3. *low differential uniformity (for the resistance to differential attacks),*
4. *not low algebraic degree (for resisting higher order differential attacks).*

We shall give the main properties of APN functions *((n, n)-functions having the best possible differential uniformity) and* AB functions *((n, n)-functions having the best possible nonlinearity, which are APN).*

Second Part of the Talk

We shall list the main known AB, APN, and differentially 4-uniform functions. These functions are defined within the structure of the finite field $\mathbb{F}_{2^n}$. We shall address the question of their implementation.
*Satisfying the criteria 1-4 above is not sufficient for an S-box. It needs also to be fastly computable, for two reasons: (1) it is not always possible to use a look-up-table for implementing it, (2) the condition of being fastly computable more or less coincides with the constraint of allowing counter-measures to side-channel attacks (*SCA*) with minimized cost. The implementation of cryptographic algorithms in devices like smart cards, FPGA or ASIC leaks information on the secret data, leading to very powerful SCA if countermeasures are not included. Such counter-measures are costly in terms of running time and of memory when they need to resist higher order SCA. The most commonly used counter-measure is* masking. *We shall describe how an S-box can be protected with this counter-measure with minimized cost.*

* LAGA, Universities of Paris 8 and Paris 13, CNRS; Address: Department of Mathematics, University of Paris 8, 2 rue de la liberté, 93526 Saint-Denis Cedex, France; e-mail: claude.carlet@univ-paris8.fr.

Background

Let n and m be two positive integers. The functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called *(n,m)-functions.* Such function F being given, the Boolean functions $f_1,\dots,f_m$ defined by $F(x)=(f_1(x),\dots,f_m(x))$, are called the *coordinate functions* of F. The linear combinations of these coordinate functions, with non-all-zero coefficients, are called the *component functions* of F. When the numbers m and n are not specified, (n,m)-functions can be called *vectorial Boolean functions* and in cryptography we use the term of *S-boxes* .

The *Walsh transform* of an (n,m)-function F maps any ordered pair $(u,v)\in\mathbb{F}_2^n\times\mathbb{F}_2^m$ to the sum (calculated in $\mathbb{Z}$): $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)+u\cdot x}$, where the same symbol "$\cdot$" is used to denote inner products in $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$. Note that the function $v\cdot F$ is a component function of F when $v\neq 0$. The *Walsh spectrum* of F is the multi-set of all the values of the Walsh transform of F, for $u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^{m*}$ (where $\mathbb{F}_2^{m*}=\mathbb{F}_2^m\setminus\{0\}$). We call *extended Walsh spectrum* of F the multi-set of their absolute values.

The *algebraic normal form* (ANF) of any (n,m)-function F:

$$\sum_{I\subseteq\{1,\cdots,n\}} a_I\left(\prod_{i\in I}x_i\right);\ a_I\in\mathbb{F}_2^m \tag{1}$$

(this sum being calculated in $\mathbb{F}_2^m$) exists and is unique and satisfies the relation $a_I=\sum_{x\in\mathbb{F}_2^n/\ supp(x)\subseteq I}F(x)$; conversely, we have $F(x)=\sum_{I\subseteq supp(x)}a_I$.

The *algebraic degree* of the function is by definition the global degree of its ANF. It is a right and left *affine invariant* (that is, it does not change when we compose F by affine automorphisms). Vectorial functions for cryptography have better not too low algebraic degrees, to withstand higher order differential attacks.

A second representation of (n,m)-functions exists when $m=n$: we endow $\mathbb{F}_2^n$ with the structure of the field $\mathbb{F}_{2^n}$; any (n,n)-function F then admits a unique *univariate polynomial representation* over $\mathbb{F}_{2^n}$, of degree at most 2^n-1:

$$F(x)=\sum_{j=0}^{2^n-1}b_jx^j\ ,\quad b_j\in\mathbb{F}_{2^n}\ . \tag{2}$$

We denote by $w_2(j)$ the number of nonzero coefficients j_s in the binary expansion $\sum_{s=o}^{n-1}j_s2^s$ of j, *i.e.* $w_2(j)=\sum_{s=0}^{n-1}j_s$ and call it the *2-weight* of j. Then, the function F has algebraic degree $\max_{j=0,\dots,2^n-1/\,b_j\neq 0}w_2(j)$. If m is a divisor of n, then any (n,m)-function F can be viewed as a function from $\mathbb{F}_{2^n}$ to itself, since $\mathbb{F}_{2^m}$ is a sub-field of $\mathbb{F}_{2^n}$. Hence, the function admits a univariate polynomial representation, which can be represented in the form $tr_{n/m}(\sum_{j=0}^{2^n-1}b_jx^j)$, where $tr_{n/m}(x)=x+x^{2^m}+x^{2^{2m}}+x^{2^{3m}}+\cdots+x^{2^{n-m}}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$.

An (n,m)-function F is *balanced* (i.e. takes every value of $\mathbb{F}_2^m$ the same number 2^{n-m} of times) if and only if its component functions are balanced (i.e. have Hamming weight 2^{n-1}).

The *nonlinearity* $nl(F)$ of an (n,m)-function F is the minimum Hamming distance between all the component functions of F and all affine functions on n variables and quantifies the level of resistance of the S-box to the linear attack. We have:

$$nl(F) = 2^{n-1} - \frac{1}{2} \max_{v \in \mathbb{F}_2^{m*};\ u \in \mathbb{F}_2^n} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + u \cdot x} \right| . \tag{3}$$

The two main known upper bounds on the nonlinearity are:
- the *covering radius bound*:

$$nl(F) \leq 2^{n-1} - 2^{n/2-1}$$

which is tight for n even and $m \leq n/2$ (the functions achieving it with equality are called *bent*);
- the *Sidelnikov-Chabaud-Vaudenay bound*, valid only for $m \geq n-1$:

$$nl(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{3 \times 2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}}$$

which equals the covering radius bound when $m = n-1$ and is strictly better when $m \geq n$. It is tight only for $m = n$ (in which case it states that $nl(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$), with n odd (the functions achieving it with equality are called *almost bent* AB).

An (n,m) function is bent if and only if all its *derivatives* $D_aF(x) = F(x) + F(x+a)$, $a \in \mathbb{F}_2^{n*}$, are balanced. For this reason, bent functions are also called *perfect nonlinear* PN. According to Chabaud-Vaudenay's proof of the Sidelnikov-Chabaud-Vaudenay bound, any AB function is *almost perfect nonlinear* APN, that is, all its derivatives D_aF , $a \in \mathbb{F}_2^{n*}$, are 2-to-1 (every element of $\mathbb{F}_2^n$ has 0 or 2 pre-images by D_aF). Such functions, whose notion has been studied by Nyberg, contribute to an optimal resistance to the differential attack . More generally, F is called *differentially δ-uniform* if the equation $D_aF(x) = b$ has at most δ solutions, for every nonzero a and every b.

The nonlinearity and the δ-uniformity are invariant under affine, extended affine and CCZ equivalences (in increasing order of generality). Two functions are called *affine equivalent* if one is equal to the other, composed on the left and on the right by affine permutations. They are called *extended affine equivalent* (EA-equivalent) if one is affine equivalent to the other, added with an affine function. They are called *CCZ-equivalent* if their graphs $\{(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid y = F(x)\}$ and $\{(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid y = G(x)\}$ are affine equivalent, that is, if there exists an affine automorphism $L = (L_1, L_2)$ of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that $y = F(x) \Leftrightarrow L_2(x,y) = G(L_1(x,y))$.

Cryptanalysis of Hash Functions

Florian Mendel

Graz University of Technology, Austria

Abstract. This extended abstract briefly summarizes a talk with the same title and gives literature pointers. In particular, we discuss recent advances in the cryptanalysis of ARX- and AES-based hash functions.

Overview

In the last few years, the cryptanalysis of hash functions has become an important topic within the cryptographic community. Especially the collision attacks on the MD4 family of hash functions (MD5, SHA-1) have weakened the security assumptions of these commonly used hash functions [17, 18]. As a consequence, NIST decided to organize a public competition in order to design a new hash function, which lead to the selection of Keccak as SHA-3 in 2012. In this talk, we discuss some recent advances in the cryptanalysis of hash functions. First, we will review the collision attacks of Wang et al. on the MD4 family and discuss the limitations of the techniques when applied to more complex functions such as the SHA-2 family. Due to the more complex structure of SHA-2 (compared to SHA-1 and MD5), several new challenges arise for the cryptanalyst. We show how to overcome these difficulties and present an automatic approach to construct complex differential characteristics and thus collisions for round-reduced SHA-2 with practical complexity [2, 10, 12]. The same techniques and tools also lead to new collision attacks on the Korean hash function standard HAS-160 [9] and the Chinese hash function standard SM3 [11], among others [6, 8, 13].

While the first part of the talk focuses on the analysis of the MD4 family and similar hash functions, the second part is dedicated to the analysis of AES-based hash functions. In the course of the SHA-3 competition, several advances have been made in the cryptanalysis of AES-based hash functions. In particular, several of the SHA-3 candidates turned out to be susceptible to the rebound attack [14], a new cryptanalytic technique that was introduced during the design of the SHA-3 finalist Grøstl. In the last years, the rebound attack and its extensions [3, 4, 7, 15] have become one of the most important tools for analyzing the security of AES-based hash functions. Even though the rebound attack was originally conceived to attack AES-based hash functions as well as their building blocks, it was later shown to also be applicable to other designs, including the SHA-3 finalists JH [16], Skein [5] and Keccak [1].

Finally, we will discuss directions of future work and open research problems at the end of this talk.

References

1. Duc, A., Guo, J., Peyrin, T., Wei, L.: Unaligned rebound attack: Application to keccak. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 402–421. Springer, Heidelberg (2012)
2. Eichlseder, M., Mendel, F., Schäffer, M.: Branching Heuristics in Differential Collision Search with Applications to SHA-512. IACR Cryptology ePrint Archive 2014, 302 (2014)
3. Gilbert, H., Peyrin, T.: Super-sbox cryptanalysis: Improved attacks for AES-like permutations. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 365–383. Springer, Heidelberg (2010)
4. Jean, J., Naya-Plasencia, M., Peyrin, T.: Improved Cryptanalysis of AES-like Permutations. J. Cryptology 27(4), 772–798 (2014)
5. Khovratovich, D., Nikolic, I., Rechberger, C.: Rotational Rebound Attacks on Reduced Skein. J. Cryptology 27(3), 452–479 (2014)
6. Kölbl, S., Mendel, F., Nad, T., Schläffer, M.: Differential cryptanalysis of keccak variants. In: Stam, M. (ed.) IMACC 2013. LNCS, vol. 8308, pp. 141–157. Springer, Heidelberg (2013)
7. Lamberger, M., Mendel, F., Rechberger, C., Rijmen, V.: Schäffer, M.: The Rebound Attack and Subspace Distinguishers: Application to Whirlpool. J. Cryptology (2013)
8. Mendel, F., Nad, T., Scherz, S., Schläffer, M.: Differential attacks on reduced RIPEMD-160. In: Gollmann, D., Freiling, F.C. (eds.) ISC 2012. LNCS, vol. 7483, pp. 23–38. Springer, Heidelberg (2012)
9. Mendel, F., Nad, T., Schläffer, M.: Cryptanalysis of round-reduced HAS-160. In: Kim, H. (ed.) ICISC 2011. LNCS, vol. 7259, pp. 33–47. Springer, Heidelberg (2012)
10. Mendel, F., Nad, T., Schläffer, M.: Finding SHA-2 characteristics: Searching through a minefield of contradictions. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 288–307. Springer, Heidelberg (2011)
11. Mendel, F., Nad, T., Schläffer, M.: Finding collisions for round-reduced SM3. In: Dawson, E. (ed.) CT-RSA 2013. LNCS, vol. 7779, pp. 174–188. Springer, Heidelberg (2013)
12. Mendel, F., Nad, T., Schläffer, M.: Improving local collisions: New attacks on reduced SHA-256. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 262–278. Springer, Heidelberg (2013)
13. Mendel, F., Peyrin, T., Schläffer, M., Wang, L., Wu, S.: Improved cryptanalysis of reduced RIPEMD-160. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part II. LNCS, vol. 8270, pp. 484–503. Springer, Heidelberg (2013)
14. Mendel, F., Rechberger, C., Schläffer, M., Thomsen, S.S.: The rebound attack: Cryptanalysis of reduced whirlpool and grøstl. In: Dunkelman, O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 260–276. Springer, Heidelberg (2009)
15. Naya-Plasencia, M.: How to improve rebound attacks. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 188–205. Springer, Heidelberg (2011)
16. Naya-Plasencia, M., Toz, D., Varici, K.: Rebound attack on JH42. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 252–269. Springer, Heidelberg (2011)
17. Wang, X., Yin, Y.L., Yu, H.: Finding collisions in the full SHA-1. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 17–36. Springer, Heidelberg (2005)
18. Wang, X., Yu, H.: How to break MD5 and other hash functions. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 19–35. Springer, Heidelberg (2005)

On Lightweight Block Ciphers and Their Security

María Naya-Plasencia

Inria, France
Maria.Naya_Plasencia@inria.fr

Abstract. In order to answer the requirements raised by a large number of applications, like RFID or sensor networks, the design of lightweight primitives has become a major interest of the cryptographic community. A (very) large number of lightweight block ciphers have been proposed. Correctly evaluating their security has become a primordial task requiring the attention of our community. In this talk we will make a survey of these proposed ciphers, some of the proposed cryptanalysis and their actual status. We will also try to provide links between some of these ciphers/attacks and the SHA-3 competition.

Keywords: lightweight block ciphers · cryptanalysis.

Recent Advances in ID-Based Encryption

Marc Joye

Technicolor, USA
marc.joye@technicolor.com

Abstract. Most ID-based cryptosystems make use of bilinear maps. A notable exception is a 2001 publication by Clifford Cocks describing an ID-based cryptosystem that works in standard RSA groups. Its semantic security relies on the quadratic residuosity assumption. Cocks's publication gave rise to several follow-up works aiming at improving the original scheme in multiple directions. This talk reviews Cocks' scheme and presents its known variants and extensions. It also discusses applications thereof. Finally it reports some recent developments the author made in the area.

Contents

Side Channel Analysis

Theory

Block Ciphers

Side Channel Analysis

Cryptanalysis

Efficient Hardware Design

Protected Hardware Design

Elliptic Curves