Lecture Notes in Computer Science **11356**

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Debrup Chakraborty · Tetsu Iwata (Eds.)

Progress in Cryptology – INDOCRYPT 2018

19th International Conference on Cryptology in India
New Delhi, India, December 9–12, 2018
Proceedings

Springer

Editors
Debrup Chakraborty
Indian Statistical Institute
Kolkata, India

Tetsu Iwata
Nagoya University
Nagoya, Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-05377-2 ISBN 978-3-030-05378-9 (eBook)
https://doi.org/10.1007/978-3-030-05378-9

Library of Congress Control Number: 2018962936

LNCS Sublibrary: SL4 – Security and Cryptology

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

INDOCRYPT 2018, the 19th edition of the International Conference on Cryptology in India, was held during December 9–12, 2018, in India Habitat Center, New Delhi. Indocrypt is organized under the aegis of the Cryptology Research Society of India (CRSI). It began in 2000 under the leadership of Prof. Bimal Roy of the Indian Statistical Institute, Kolkata, and since then this annual event has gained its place among prestigious cryptology conferences and is considered as the leading Indian conference for cryptology. In the past, the conference took place in various cities of India: Kolkata (2000, 2006, 2012, 2016), Chennai (2001, 2004, 2007, 2011, 2017), Hyderabad (2002, 2010), New Delhi (2003, 2009, 2014), Bangalore (2005, 2015), Kharagpur (2008), and Mumbai (2013).

INDOCRYPT 2018 attracted 60 submissions from 14 different countries. Out of these 60 submissions, papers that were withdrawn before the submission deadline and those submitted after the submission deadline were not reviewed, and after the review process, 20 papers were accepted for inclusion in the program. All the papers that satisfied the submission guidelines were reviewed by at least three reviewers. Submissions of the Program Committee members were reviewed by at least four reviewers. The individual review phase was followed by a discussion phase that generated additional comments from the Program Committee members and the external reviewers. A total of 44 Program Committee members and 48 external reviewers took part in the process of reviewing and the subsequent discussions. We take this opportunity to thank the Program Committee members and the external reviewers for their tremendous job in selecting the current program. The submissions and reviews were managed using the "Web Submission and Review Software" written and maintained by Shai Halevi. We thank him for providing us the software.

The proceedings include the revised versions of the 20 contributed papers. Revisions were not checked by the Program Committee members and the authors bear the full responsibility for the contents of the respective papers. In addition to the 20 papers, the program included three invited talks. Gilles Van Assche gave a talk about "On dec(k) Functions," Takahiro Matsuda spoke on "Public Key Encryption Secure Against Related Randomness Attacks," and Mridul Nandi's talk was about "How to Make a Single-Key Beyond Birthday Secure Nonce-Based MAC." The abstracts of the invited talks are also included in these proceedings.

We would like to thank the general chairs, Dr. Anu Khosla and Prof. Brishbhan Singh Panwar, and the organizing chairs, Prof. Shri Kant and Dr. Indivar Gupta, along with the Organizing Committee comprising members of Sharda University and SAG DRDO for making the conference a success. Finally, we would like to thank all the authors who submitted their work to INDOCRYPT 2018, and we also would like to

thank all the participants. Without their support and enthusiasm, the conference would not have succeeded.

December 2018

Debrup Chakraborty
Tetsu Iwata

INDOCRYPT 2018

The 19th International Conference on Cryptology in India

New Delhi, India
December 9–12, 2018

General Chairs

Anu Khosla	Scientific Analysis Group, DRDO, Delhi, India
Brishbhan Singh Panwar	Sharda University, India

Program Chairs

Debrup Chakraborty	Indian Statistical Institute, Kolkata, India
Tetsu Iwata	Nagoya University, Japan

Organizing Chairs

Indivar Gupta	Scientific Analysis Group, DRDO, Delhi, India
Shri Kant	Sharda University, India

Program Committee

Diego Aranha	University of Campinas, Brazil and Aarhus University, Denmark
Shi Bai	Florida Atlantic University, USA
Subhadeep Banik	EPFL, Switzerland
Lejla Batina	Radboud University, The Netherlands
Rishiraj Bhattacharyya	NISER, India
Christina Boura	University of Versailles and Inria, France
Debrup Chakraborty	Indian Statistical Institute, Kolkata, India
Sanjit Chatterjee	Indian Institute of Science, Bangalore, India
Geoffroy Couteau	Karlsruher Institut für Technologie, Germany
Pooya Farshim	CNRS and ENS, France
Shay Gueron	University of Haifa, Israel
Divya Gupta	Microsoft Research India, India
Indivar Gupta	SAG, DRDO, Delhi, India
Gottfried Herold	ENS de Lyon, France
Viet Tung Hoang	Florida State University, USA
Takanori Isobe	University of Hyogo, Japan
Tetsu Iwata	Nagoya University, Japan
Elena Kirshanova	ENS Lyon, France

Shanta Laishram	Indian Statistical Institute, Delhi, India
Patrick Longa	Microsoft Research, Redmond, USA
Atul Luykx	Visa Research, USA
Subhamoy Maitra	Indian Statistical Institute, Kolkata, India
Hemanta K. Maji	Purdue University, USA
Bart Mennink	Radboud University, The Netherlands
Kazuhiko Minematsu	NEC Corporation, Japan
Debdeep Mukhopadhyay	IIT Kharagpur, India
Mridul Nandi	Indian Statistical Institute, Kolkata, India
Khoa Nguyen	NTU, Singapore
Ryo Nishimaki	NTT, Japan
Raphael Phan	Multimedia University, Malaysia
Manoj Prabhakaran	Indian Institute of Technology, Bombay, India
Somindu C. Ramanna	Indian Institute of Technology, Kharagpur, India
Francisco Rodriguez-Henriquez	CINVESTAV-IPN, Mexico
Adeline Roux-Langlois	University of Rennes, CNRS, IRISA, France
Jacob Schuldt	AIST, Japan
Peter Schwabe	Radboud University, The Netherlands
Francois-Xavier Standaert	UCL, Belgium
Siwei Sun	Chinese Academy of Sciences, China
Atsushi Takayasu	University of Tokyo, Japan
Srinivas Vivek	IIIT Bangalore, India
Shota Yamada	AIST, Japan
Kazuki Yoneyama	Ibaraki University, Japan
Yu Yu	Shanghai Jiao Tong University, China
Vassilis Zikas	University of Edinburgh, UK

External Reviewers

Nuttapong Attrapadung
Arnab Bag
Balthazar Bauer
Sai Lakshmi Bhavana
Avik Chakraborti
Bishwajit Chakraborty
Joan Daemen
Prem Laxman Das
Martianus Frederic Ezerman
Chun Guo
Jian Guo
Muhammad Ishaq
Matthias Kannwischer
Louiza Khati
Manoj Kumar
Iraklis Leontiadis
Shun Li
Fuchun Lin
Fukang Liu
Alice Pellet–Mary
Ryutaroh Matsumoto
Nicky Mouha
Fabrice Mouhartem
Pierrick Méaux
Tapas Pandit
Christophe Petit
Shravan K. Parshuram Puria
Yogachandran Rahulamathavan

Joost Renes
Yusuke Sakai
Palash Sarkar
Akash Shah
Danping Shi
Bhupendra Singh
Ben Smith
Shifeng Sun
Sharwan Kumar Tiwari
Yiannis Tselekounis
Alexandre Wallet
Weijia Wang
Xiao Wang
Yuyu Wang
Yohei Watanabe
Weiqiang Wen
Masaya Yasuda
Thomas Zacharias
Bin Zhang
Juanyang Zhang

Abstracts of Invited Talks

On dec(k) Functions

Gilles Van Assche

STMicroelectronics, Diegem, Belgium

Cryptographic objects with input and output extension properties are very convenient in numerous situations. With the duplex construction, we defined a cryptographic object that can return a digest on a growing sequence of strings, with an incremental cost, i.e., without the need to process again the entire sequence [2]. Similarly, the Farfalle construction builds a keyed cryptographic function with an extendable input and able to return an output of arbitrary length [1]. It supports for sequences of strings as input and a specific incremental property, namely that computing $F(Y \circ X)$ costs only the processing of Y if $F(X)$ was previously computed. Clearly, duplex and Farfalle are not the only way to build functions with such properties, and the construction should be decoupled from the input-output signature.

For this purpose, we propose the name *dec function* for a function that takes a sequence of input strings and returns a digest of arbitrary length and that can be computed incrementally. Here, "dec" stands for *Doubly-Extendable Cryptographic*. Note that a dec function is a particular case of extendable-output function (XOF), as a XOF is not required to accept growing inputs at an incremental cost. Likewise, we propose the name *deck function*, with an additional "k" for *Keyed*, for a keyed function with the same incremental properties and whose output is a pseudorandom string of arbitrary length.

In this talk, I will explain the purpose of dec(k) functions, from transcript hashing to authenticated encryption, and how to implement them. On this last point, I will relate them to the duplex and full-state keyed duplex constructions, as well as to the Strobe protocol framework [2, 4, 5]. Then, I will explore the permutation-based Farfalle construction as a way to build an efficient deck function from permutation components [1]. Finally, I will detail the recent Xoodoo permutation, its cryptographic properties and the deck function Xoofff built on top of it [3].

References

1. Bertoni, G., Daemen, J., Hoffert, S., Peeters, M., Van Assche, G., Van Keer, R.: Farfalle: parallel permutation-based cryptography. IACR Trans. Symmetric Cryptol. **2017**(4), 1–38 (2017)
2. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: Duplexing the sponge: single-pass authenticated encryption and other applications. In: Miri, A., Vaudenay, S. (eds.) SAC 2011. LNCS, vol. 7118, pp. 320–337. Springer, Heidelberg (2012)
3. Daemen, J., Hoffert, S., Van Assche, G., Van Keer, R.: Xoodoo cookbook. IACR Cryptol. ePrint Arch. **2018**, 767 (2018)

4. Daemen, J., Mennink, B., Van Assche, G.: Full-state keyed duplex with built-in multi-user support. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017. LNCS, vol. 10625, pp. 606–637. Springer, Cham (2017)
5. Hamburg, M.: The STROBE protocol framework. IACR Cryptol. ePrint Archive **2017**, 3 (2017)

Public Key Encryption Secure Against Related Randomness Attacks

Takahiro Matsuda

National Institute of Advanced Industrial Science and Technology (AIST),
Tokyo, Japan
t-matsuda@aist.go.jp

Abstract. Most cryptographic primitives are designed under the assumption that perfect (uniform) randomness is available. Unfortunately, however, random number generators (RNGs) are notoriously hard to implement and test, and we have seen many examples of the failures of RNGs in practice. Motivated by the challenge of designing public key encryption secure under randomness failure, Paterson, Schuldt, and Sibborn (PKC 2014) introduced a security notion called *related randomness attack (RRA) security*. This notion captures security against adversaries that are allowed to control the randomness used in the encryption scheme, but still requires that messages encrypted under an honestly generated public key remain hidden, given that certain restrictions are placed on the adversaries' queries. RRA security is one of the promising security notions that allows us to hedge against randomness failures in the usage of public key encryption. In this talk, I will give a brief survey of the topic, in particular the formalizations, existing results, and techniques used for achieving RRA security.

How to Make a Single-Key Beyond Birthday Secure Nonce-Based MAC

Mridul Nandi

Indian Statistical Institute, Kolkata
mridul.nandi@gmail.com

Abstract. At CRYPTO 2016, Cogliati and Seurin [1] have proposed a highly secure nonce-based MAC called Encrypted Wegman-Carter with Davies-Meyer (EWCDM) construction, as $\mathsf{E}_{K_2}(\mathsf{E}_{K_1}(N) \oplus N \oplus \mathsf{H}_{K_h}(M))$ for a nonce N and a message M. This construction achieves roughly $2^{2n/3}$ bit MAC security with the assumption that E is a PRP secure n-bit block cipher and H is an almost xor universal n-bit hash function. Note that EWCDM requires three keys; two block cipher keys K_1 and K_2 and one hash key K_h. Thus, it is natural to ask that whether one can achieve the similar security in the case of using less number of keys. In fact, proving BBB security of single-keyed EDM ($\mathsf{E}_{K_1}(\mathsf{E}_{K_1}(N) \oplus N)$), is a highly complicated task as evident from [2] and it is not clear at all how to build on this result to prove the MAC security of EWCDM construction with $K_1 = K_2$. Moreover, Cogliati and Seurin, in their proof of single-keyed EDM [2], have also stated that

"For now, we have been unable to extend the current (already cumbersome) counting used for the proof of the single-permutation EDM construction to the more complicated case of single-key EWCDM."

In this talk, I will discuss a recent design - Decrypted Wegman-Carter with Davies-Meyer (DWCDM) construction - which is structurally very similar to its predecessor EWCDM except that the outer encryption call is replaced by decryption. The biggest advantage of DWCDM is that we can make a truly single key MAC: the two block cipher calls can use the same block cipher key $K = K_1 = K_2$. Moreover, we can derive the hash key as $K_h = \mathsf{E}_K(1)$, as long as $|K_h| = n$. Whether we use encryption or decryption in the outer layer makes a huge difference; using the decryption instead enables us to apply an extended version of the mirror theory by Patarin to the security analysis of the construction. DWCDM is secure beyond the birthday bound, roughly up to $2^{2n/3}$ MAC queries and 2^n verification queries against nonce-respecting adversaries when nonce is a $2n/3$ bits string. I will also describe how this construction can be further improved in two directions. We extend the nonce space to as large as the set of all $n-1$ bits. Moreover, the security bound can be extended against $2^{3n/4}$ MAC queries. The details of a part of this talk can be found in [3].

Keywords: EDM · EWCDM · Mirror theory · Extended mirror theory
H-Coefficient

References

1. Cogliati, B., Seurin, Y.: EWCDM: an efficient, beyond-birthday secure, nonce-misuse resistant MAC. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 121–149. Springer, Heidelberg (2016)
2. Cogliati, B., Seurin, Y.: Analysis of the single-permutation encrypted Davies-Meyer construction. Des. Codes Cryptography 2018 (2018, to appear)
3. Datta, N., Dutta, A., Nandi, M., Yasuda, K.: Encrypt or decrypt? To make a single-key beyond birthday secure nonce-based MAC. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. LNCS, vol. 10991, pp. 631–661. Springer, Cham (2018)

Contents