Lecture Notes in Computer Science 10662

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

Editorial Board

David Hutchison
Lancaster University, Lancaster, UK
Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA
Josef Kittler
University of Surrey, Guildford, UK
Jon M. Kleinberg
Cornell University, Ithaca, NY, USA
Friedemann Mattern
ETH Zurich, Zurich, Switzerland
John C. Mitchell
Stanford University, Stanford, CA, USA
Moni Naor
Weizmann Institute of Science, Rehovot, Israel
C. Pandu Rangan
Indian Institute of Technology, Madras, India
Bernhard Steffen
TU Dortmund University, Dortmund, Germany
Demetri Terzopoulos
University of California, Los Angeles, CA, USA
Doug Tygar
University of California, Berkeley, CA, USA
Gerhard Weikum
Max Planck Institute for Informatics, Saarbrücken, Germany

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

Sk Subidh Ali · Jean-Luc Danger
Thomas Eisenbarth (Eds.)

Security, Privacy, and Applied Cryptography Engineering

7th International Conference, SPACE 2017
Goa, India, December 13–17, 2017
Proceedings

Springer

Editors
Sk Subidh Ali
Indian Institute of Technology
Tirupati, Andhra Pradesh
India

Thomas Eisenbarth
University of Lübeck
Lübeck
Germany

Jean-Luc Danger
Institut Mines-Télécom
Paris
France

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-71500-1 ISBN 978-3-319-71501-8 (eBook)
https://doi.org/10.1007/978-3-319-71501-8

Library of Congress Control Number: 2017959611

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2017
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

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

Preface

This volume contains the papers accepted for presentation at the 7th International Conference on Security, Privacy, and Applied Cryptography Engineering 2017 (SPACE 2017), held during December 13–17, 2017, at the Don Bosco College of Engineering, Goa, India. This annual event is devoted to various aspects of security, privacy, applied cryptography, and cryptographic engineering. This is indeed a very challenging field, requiring expertise from diverse domains, ranging from mathematics to solid-state circuit design.

This year we received 49 submissions from about eight different countries, out of which, after an extensive review process, 13 papers were accepted for presentation at the conference, and one shorter paper was accepted for short presentation. The submissions were evaluated based on their significance, novelty, technical quality, and relevance to the SPACE conference. The submissions were reviewed in a double-blind mode by at least three members of the 36-member Program Committee (one more if at least one of the authors was member of the Program Committee). The Program Committee was aided by 50 additional reviewers. The Program Committee meetings were held electronically, with intensive discussions.

The program also included seven invited talks and four tutorials on several aspects of applied cryptology, delivered by world-renowned researchers: Asaf Ashkenazi, Shivam Bhasin, Jean-Luc Danger, Thomas Eisenbarth, Harry Halpin, Mike Hamburg, Gary Kenworthy, Victor Lomne, Axel Poschmann, Karim Tobich, Ingrid Verbauwhede, and Yuval Yaron. We sincerely thank the invited speakers for accepting our invitations in spite of their busy schedules. Like its previous editions, SPACE 2017 was organized in co-operation with the International Association for Cryptologic Research (IACR). We are thankful to Don Bosco College of Engineering for being the gracious host of SPACE 2017.

There is a long list of volunteers who invested their time and energy to put together the conference, and who deserve accolades for their efforts. We are grateful to all the members of the Program Committee and the additional reviewers for all their hard work in the evaluation of the submitted papers. We thank Cool Press Ltd., owner of the EasyChair conference management system, for allowing us to use it for SPACE 2017, which was a great help. We thank our publisher Springer for agreeing to continue to publish the SPACE proceedings as a volume in *the Lecture Notes in Computer Science* (LNCS) series. We are grateful to the local Organizing Committee, especially to the organizing chair, Roseline Fernandes, who invested a lot effort for the conference to run smoothly. We are further very grateful to Vishal Saraswat, program chair of SPACE 2016, for his guidance and active support toward organizing SPACE 2017. Special thanks to our general chairs, Rev. Fr. Kinley D'Cruz, Neena Panandikar, and Sandeep Shukla, for their support and encouragement. Our sincere gratitude to Debdeep Mukhopadhyay, Veezhinathan Kamakoti, and Sanjay Burman for being

constantly involved in SPACE since its very inception and responsible for SPACE reaching its current status.

Last, but certainly not least, our sincere thanks go to all the authors who submitted papers to SPACE 2017, and to all the attendees. The conference is made possible by you, and it is dedicated to you. We sincerely hope you find the proceedings stimulating and inspiring.

October 2017

Sk Subidh Ali
Jean-Luc Danger
Thomas Eisenbarth

Organization

Honorary General Chair

Rev. Fr. Kinley D'Cruz	DBCE, India

General Co-chairs

Neena Panandikar	DBCE, India
Sandeep Shukla	IIT Kanpur, India

Program Co-chairs

Sk Subidh Ali	IIT Tirupati, India
Jean-Luc Danger	Institut Mines-Telecom, France
Thomas Eisenbarth	Worcester Polytechnic Institute, USA

Organizing Chair

Roseline Fernandes	DBCE, India

Steering Committee

Sanjay Burman	CAIR-DRDO, India
Veezhinathan Kamakoti	IIT Madras, India
Debdeep Mukhopadhyay	IIT Kharagpur, India

Program Committee

Sk Subidh Ali (Co-chair)	IIT Tirupati, India
Reza Azarderakhsh	Florida Atlantic University, USA
Lejla Batina	Radboud University Nijmegen, The Netherlands
Guido Marco Bertoni	STMicroelectronics, Italy
Shivam Bhasin	NTU, Singapore
Swarup Bhunia	University of Florida, USA
Lilian Bossuet	University St. Etienne, France
Claude Carlet	University of Paris, France
Rajat Subhra Chakraborty	IIT Kharagpur, India
Pandu Rangan Chandrasekaran	Indian Institute of Technology Chennai, India
Anupam Chattopadhyay	NTU, Singapore
Dipanwita Roy Chowdhury	IIT Kharagpur, India
Jean-Luc Danger (Co-chair)	Institut Mines-Telecom, France

Thomas Eisenbarth (Co-chair)	Worcester Polytechnic Institute, USA
Junfeng Fan	Open Security Research, China
Sylvain Guilley	GET/ENST, CNRS/LTCI, France
Tim Guneysu	Universität Bremen, Germany
Indivar Gupta	DRDO, Delhi, India
Naofumi Homma	Tohoku University, Japan
Subhamoy Maitra	Indian Statistical Institute, India
Bodhi Satwa Majumdar	IIT Indore, India
Stefan Mangard	TU Graz, Austria
Mitsuru Matsui	Mitsubishi, Japan
Philippe Maurine	LIRMM Montpellier, France
Debdeep Mukhopadhyay	IIT Kharagpur, India
Svetla Nikova	KU Leuven, Belgium
Thomas Poeppelmann	Infineon Technologies, Germany
Emmanuel Prouff	ANSSI, France
Bimal Roy	Indian Statistical Institute, India
Kazuo Sakiyama	UEC Tokyo, Japan
Somitra Sanadhya	IIT Ropar, India
Vishal Saraswat	Indian Statistical Institute, India
Francois-Xavier Standaert	UCL Crypto Group, Belgium
Mostafa Taha	Western University, Canada
Ming Tang	Wuhan University, China
Carolyn Whitnall	Bristol, UK
Yuval Yarom	University of Adelaide, Australia
Amr Youssuf	Concordia University, Canada
Yongbin Zhou	CAS Beijing, China

Additional Reviewers

Alexandre Berzati	Bernhard Jungk
Sarani Bhattacharya	Brian Koziel
Urbi Chatterjee	Manoj Kumar
Wei Cheng	Yogesh Kumar
Guillaume Dabosville	Hui Ma
Joan Daemen	Marco Martinoli
Nilanjan Datta	Pedro Maat Massolino
Dhananjoy Dey	Sihem Mesnager
S.V. Dilip Kumar	Yasin Muhammad
Lorenzo Grassi	Zakaria Najm
Daniel Gruss	Sikhar Patranabis
Nupur Gupta	Shuang Qiu
Amir Jalali	Francesco Regazzoni
Dirmanto Jap	Guenael Renault

Aniket Roy
Debapriya Basu Roy
Rajat Sadhukhan
Peter Schwabe
Michael Schwarz
Raphael Spreitzer
Diangarti Bhalang Tariang
Srinivas Vivek
Tim Wood
Yan Yan

Organizing Institute

Don Bosco College of Engineering, Goa, India

Invited Talks/Tutorials

On the (in)Security of ChaCha20 Against Physical Attacks

Shivam Bhasin

Temasek Labortaries, Nanyang Technological University Singapore
sbhasin@ntu.edu.sg

The stream cipher ChaCha20 and the Poly1305 authentication are adopted in several products including Google Chrome [1], or OpenSSL [2] etc. For instance, Google Chome often uses ChaCha20 for secure communication when the underlying platform lacks hardware support for AES. The two algorithms have potential to be adopted across multiple domains in the future. The ChaCha20-Poly1305 cipher suite is advertised as being easier to implement in a side-channel resistant way [3], especially compared to ciphers based on substitution permutation networks. However, the side-channel security claim is only limited to timing based leakage. In this talk, we investigate the security of ChaCha20 against two commonly known physical attacks: *side-channel attacks* and *fault attacks*.

The first part focuses on power [4] or electromagnetic [5] based side-channels. The development of the omnipresent Internet of Things (IoT), or the connected car increases the amount of embedded appliances, which can be attacked using these side-channels. Hence, it is important to understand the security of deployed cryptographic algorithms not only against attacks on the timing side-channels but a wider attack suite. We analyze the stream cipher ChaCha20 [3, 6] and show how the secret key can be completely extracted. While first attack recovers the key from initial round of ChaCha20, another attack demonstrates key retrieval exploiting the final addition.

The second part will look into active attacks realised using fault injection [7]. Often stream ciphers are believed to be harder to attack against fault injection attacks owing to the complexity of the required offline analysis. We propose four differential fault analysis (DFA) attacks on ChaCha20 running on a low cost microcontroller, using the instruction skip and instruction replacement fault models. The attacks target the keystream generation module at the decryption site, and entirely avoid nonce misuse. We practically demonstrate our proposed attacks using a laser fault injection setup.

The talk is based on recent joint works. The part on side-channel attack is based on recent work with Bernhard Jungk from NTU, Singapore [8]. Fault attacks was investigated with co-authors from IIT Kharagpur, India and NTU, Singapore [9].

References

1. Bursztein, E.: Speeding up and strengthening HTTPS connections for Chrome on Android (2014). https://security.googleblog.com/2014/04/speeding-up-and-strengthening-https.html
2. Staruch, M.: Support for ChaCha20-Poly1305 (2015). https://github.com/openssl/openssl/issues/304
3. Nir, Y., Langley, A.: ChaCha20 and Poly1305 for IETF Protocols. IETF RFC 7539 (2015)
4. Kocher P., Jaffe J., Jun B.: Differential power analysis. In: Wiener, M. (eds.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_25
5. Agrawal, D., Archambeault, B., Rao, J.R., Rohatgi, P.: The EM side—channel(s). In: Kaliski, B.S., Koç, K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 29–45. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-36400-5_4
6. Bernstein, D.J.: ChaCha, a variant of Salsa20. In: Workshop Record of SASC - The State of the Art of Stream Ciphers (2008)
7. Barenghi, A., Breveglieri, L., Koren, I., Naccache, D.: Fault injection attacks on cryptographic devices: theory, practice, and countermeasures. Proc. IEEE **100**, 3056–3076 (2012)
8. Jungk, B., Bhasin, S.: Don't fall into a trap: physical side-channel analysis of chacha20-poly1305. In: 2017 Design, Automation and Test in Europe Conference and Exhibition (DATE). IEEE, pp. 1110–1115 (2017)
9. Kumar, S.D., Patranabis, S., Breier, J., Mukhopadhyay, D., Bhasin, S., Chattopadhyay, A., Baksi, A.: A practical fault attack on arx-like ciphers with a case study on chacha20. In: 2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). IEEE (2017)

How to Digitally Construct and Validate TRNG and PUF Primitives Which Are Based on Physical Phenomenon? (Tutorial)

Jean-Luc Danger

Telecom ParisTech, University Paris-Saclay, Scientific Advisor at Secure-IC
September 23, 2017

Abstract. In digital devices, the cryptographic functions are dependant on peripheral primitives, like the True Random Number Generation (TRNG) and Physically Unclonable Function (PUF) which generates a random number and an identifier respectively. The source of these primitives is not defined by a digital algorithm but comes from physical phenomenon, notably the noise. Consequently a conversion is necessary to output a digital random number or identifier. Indeed, these two types of primitives exploit the noise, but at different stage. At the manufacturing stage, the variance of the manufacturing process creates mismatches between transistors. These slight differences are fixed once the chip is fabricated, they should be transformed by the PUF to a digital variable when an identifer is called by the application. When the chip is in used, the environmental noise is extracted by the TRNG to generate a digital random number. In case of PUF, we can say that the entropy is "static", whereas the entropy for the TRNG is "dynamic". The dynamic entropy is a major problem for the PUF which is natively not steady because of the environmental noise. The TRNG is very sensitive to an external noise, which can be malevolently generated by an attacker, and can bias the TRNG output. Consequently, it is necessary to add to the primitives an evaluation or correction block to detect or enhance their behavior. This means that some tests and metrics have to be be specified to define what is a good identifier and a good random number.

We will see in this tutorial, the different constructions of PUF and TRNG, but also the methods to validate their quality to ensure a minimum level of trust.

Cache Attacks: From Cloud to Mobile

Thomas Eisenbarth

University of Lübeck and Worcester Polytechnic Institute
thomas.eisenbarth@uni-luebeck.de

Abstract. The microarchitecture of modern CPUs features many optimizations that result in data-dependent runtime behavior. Data-dependent execution behavior can result in information leakage, enabling malicious co-located processes to overcome logical isolation boundaries of hypervisors and operating systems. For instance, cache attacks that exploit access time variations when retrieving data from the cache or the memory are a powerful tool to extract critical information such as cryptographic keys from co-located processes.

This tutorial introduces several methods of how to exploit cache-based side channels. Modern attacks and their behavior in various application scenarios, from cloud to mobile and embedded processors will be discussed. It will be shown of the introduced techniques can be applied to extract sensitive information from a co-located processes or VMs across cores and even across processor boundaries and how such attacks can be prevented.

May the Fourth Be With You: A Microarchitectural Side Channel Attack on Several Real-World Applications of Curve25519

Daniel Genkin[1,2] Luke Valenta[1], and Yuval Yarom[3,4]

[1] University of Pennsylvania
{danielg3,lukevg}@cis.upenn.edu
[2] University of Maryland
[3] University of Adelaide
yval@cs.adelaide.edu.au
[4] Data 61, CSIRO

In recent years, applications increasingly adopt security primitives designed with better countermeasures against side channel attacks. A concrete example is Libgcrypt's implementation of ECDH encryption with Curve25519. The implementation employs the Montgomery ladder scalar-by-point multiplication, uses the unified, branchless Montgomery double-and-add formula and implements a constant-time argument swap within the ladder. However, Libgcrypt's field arithmetic operations are not implemented in a constant-time side-channel-resistant fashion.

Based on the secure design of Curve25519, users of the curve are advised that there is no need to perform validation of input points. In this work we demonstrate that when this recommendation is followed, the mathematical structure of Curve25519 facilitates the exploitation of side-channel weaknesses.

We demonstrate the effect of this vulnerability on three software applications—encrypted git, email and messaging—that use Libgcrypt. In each case, we show how to craft malicious OpenPGP files that use the Curve25519 point of order 4 as a chosen ciphertext to the ECDH encryption scheme. We find that the resulting interactions of the point at infinity, order-2, and order-4 elements in the Montgomery ladder scalar-by-point multiplication routine create side channel leakage that allows us to recover the private key in as few as 11 attempts to access such malicious files.

Parameter Choices for LWE

Mike Hamburg

Rambus, USA

Abstract. All widely-deployed public-key encryption algorithms are threatened by the possibility of a quantum computer that can run Shor's algorithm. The most popular approach for future, "post-quantum" encryption is the "learning with errors" (LWE) problem, and its variants Ring-LWE, Module-LWE, Integer-Module-LWE, etc. Compared to elliptic curves, LWE systems are tricky to parameterize. The relationship between the parameters and the security they provide is complex, and there is also the threat of attacks based on decryption failures.

In this talk, I will cover how to choose parameters for LWE systems. I will focus especially on how to estimate failure probabilities, and the difficulty of attacks based on decryption failure.

IoT Insecurity – Innovation and Incentives in Industry

Axel Y. Poschmann

DarkMatter, Abu Dhabi, United Arab Emirates

Abstract. Why is the Internet of Things going to be a security and privacy nightmare (it is already, but we have only seen the beginning)? What does it have to do with disruptive innovation, incentives in industry, time-to-market trade-offs, and quantifiability? This talk—a collection of thoughts and observations, really—walks along these questions to conclude with a set of promising research directions.

Hardware Enabled Cryptography: Physically Unclonable Functions and Random Numbers as Roots of Trust

Ingrid Verbauwhede

KU Leuven – COSIC
Ingrid.verbauwhede@esat.kuleuven.be

Abstract. Intelligent things, medical devices, vehicles and factories, are all part of so-called cyber-physical systems. These systems will only be secure if we can build devices that can perform the mathematically demanding cryptographic protocols and algorithms in an efficient way in an embedded context. Unfortunately, many of devices operate under extremely limited power, energy and area constraints. At the same time, we request that the implementations are also secure against a wide range of physical attacks and that keys or other sensitive material are stored securely. Often forgotten but of utmost important are the sources of randomness to support the cryptographic protocols and algorithms. This will be the focus of this presentation. We will therefore focus on two roots of trust: Physically Unclonable Functions and True Random Number generators. We will discuss design principles and how to make them suit embedded devices. We will explain how they can fit in FPGA or ASIC. We will also discuss possible attacks and test strategies. We will include myths and realities and discuss future trends for PUF and TRNGs.

Acknowledgements. This research summarizes the work of several PhD students, who are gratefully acknowledged. The research is funded in part by the Research Council KU Leuven: C16/15/058, and the Horizon 2020 research and innovation programs under grant agreement No 644052 HECTOR and Cathedral ERC Advanced Grant 695305.

Efficient Side Channel Testing of Cryptographic Devices Using TVLA (Tutorial)

Gary Kenworthy

Rambus Cryptography Research
gkenworthy@rambus.com

Abstract. Power and EM side channels are very powerful attack vectors for cryptographic devices. Protecting against these attacks is an important design consideration for any cryptographic implementation, and validating the effectiveness of countermeasures is critical to verify their effectiveness. Whereas an attacker has potentially unlimited time and resources to mount an attack, the validation against such attacks must be done in an efficient and cost effective way. Test Vector Leakage Assessment (TVLA) is a methodology that can "level the field" and provide an objective, quantified assessment of leakage and the protection afforded by the design. In this tutorial, we will first review the risks of simple power analysis (SPA) and differential power analysis (DPA) and their EM counterparts (SEMA and DEMA). The concepts behind TVLA will be presented, with case studies and demonstrations correlating the TVLA measurements with actual attacks. TVLA measurements will be demonstrated on protected and unprotected hardware cores. Limitations and cautions of using TVLA will also be discussed.

Contents