Theory of Implementation Security Workshop (TIs 2016)

Begül Bilgin
KU Leuven and iMinds
Kasteelpark Arenberg 10
3001 Leuven, Belgium

Svetla Nikova
KU Leuven and iMinds
Kasteelpark Arenberg 10
3001 Leuven, Belgium

Vincent Rijmen
KU Leuven and iMinds
Kasteelpark Arenberg 10
3001 Leuven, Belgium

ABSTRACT

The Internet of Things (IoT) enables a network of communication between people-to-people, people-to-things and things-to-things. The security of these communications against all possible attacks is a significant part of todays security and privacy. Due to the design nature of IoT systems, IoT devices are easily accessible by attackers which increases the importance of their security against physical attacks. This workshop is dedicated to research on the design of cryptographic algorithms and implementations secure against physical attacks.

CCS Concepts

•**Security and privacy → Side-channel analysis and countermeasures;** *Cryptography; Embedded systems security;*

Keywords

Cryptography, Embedded Security, Hardware security, Side-channel attacks and countermeasures, TIs, Threshold Implementations

1. BACKGROUND AND MOTIVATION

An IoT system using cryptographically secure protocols correctly is still vulnerable to attacks if its underlying implementations are not secure. Namely, an attacker can easily access the nodes in the IoT due to its nature and use side-channel information such as execution time, instantaneous power consumption or electromagnetic radiation of the device during a cryptographic operation to reveal the sensitive information [2, 3]. Moreover, an active attacker can also use information of a faulty output caused by clock glitching, under/over powering or over heating/cooling during execution [1]. All of these attacks, which date back to 90s, are simple to apply and require relatively cheap equipment. Hence, they are undeniable threats to today's IoT.

Several countermeasures against SCA and fault analysis have been suggested in literature covering a wide spectrum from ad-hoc to provable secure, from lightweight to high-resource demanding, from generic to specific to a certain architecture. However, the task to find a provably secure countermeasure against all kinds of physical attacks applicable to all algorithms on multiple devices is still challenging.

2. SCOPE AND OBJECTIVES

In this workshop, we focus on physical attacks and their countermeasures. Considering the limitations of an IoT device, we emphasize on efficiency and applicability.

The workshop topics include (but are not limited to) the following:

- Physical attacks and countermeasures
- Efficient and secure implementations of cryptographic algorithms
- Designs of cryptographic algorithms with physical attack resistance

A special topic of interest is:

- Advances in theory and practice of Threshold Implementations

Threshold Implementation (TI) is proposed as a countermeasure against side-channel attacks in 2006 [4]. This masking based method attracted a lot of attention due to its efficiency and generality in recent years. It has been extended to higher orders. In order to celebrate the 10$^{\text{th}}$ anniversary of TI design, this workshop encourages novel results on TI.

3. INVITED SPEAKERS

There are 2 invited speakers at the workshop: Prof. Nigel Smart (University of Bristol, US) and Dr. Mike Hutter (Cryptography Research - Rambus, USA). The titles and abstracts of their talks are listed below.

"**Masking and MPC: When Crypto Theory Meets Crypto Practice**", Nigel Smart.

Abstract: I will explain the linkage between threshold implementation masking schemes and multi-party computation. The basic principles that need to be taken from multi-party computation will be presented, as well as some basic protocols. The different natures of the resources and threat models between the two different applications of secret sharing will also be covered.

CCS'16 October 24-28, 2016, Vienna, Austria

ACM ISBN 978-1-4503-4139-4/16/10.
DOI: http://dx.doi.org/10.1145/2976749.2990488

"**Threshold Implementations in Industry: A Case Study on SHA-256**", Mike Hutter.

Abstract: Implementing efficient countermeasures against side-channel attacks is a challenge since two decades. Especially in hardware, many masking countermeasure implementations failed due to first-order leakages caused by glitches or other effects such as early evaluation and unbalanced routing. The Threshold Implementation (TI) scheme was proposed a decade ago and it provides provable security even in the presence of such effects. In this talk, I will discuss different state of the art secure logic styles and TIs from an industry perspective. As a case study, we will consider SHA-256 which is especially interesting to mask due to its ARX-based design. I will present various techniques for efficient mask conversion that can be applied to SHA-256 and discuss solutions for higher-order security.

4. PROGRAM COMMITTEE

- Joan Daemen (Radboud University Nijmegen, the Netherlands and STMicroelectronics, Belgium)
- Junfeng Fan (Open Security Research, China)
- Benedikt Gierlichs (KU Leuven, Belgium)
- Marcel Medwed (NXP, Austria)
- Amir Moradi (Ruhr-University Bochum, Germany)
- Elisabeth Oswald (University of Bristol, UK)
- Emmanuel Prouff (ANSSI, France)
- Christian Rechberger (DTU, Denmark and TU Graz, Austria)
- Matthieu Rivain (CryptoExperts, France)
- Kazuo Sakiyama (The University of Electro-Communications, Japan)
- Jörn-Marc Schmidt (Secunet, Germany)
- Francois Xavier Standaert (Universite Catholique de Louvain, Belgium)
- Elena Trichina (Cryptography Research, France)

5. PC CO-CHAIRS

Begül Bilgin is a postdoctoral researcher at the COSIC research group in ESAT, KU Leuven and postdoctoral fellow at the Flemish Research Foundation (FWO). Her main research interests are countermeasures against physical attacks and designs and hardware implementations of lightweight symmetric-key algorithms. Her Ph.D. is on Threshold Implementations. She organized a day dedicated to Threshold Implementations (TI day) in 2015 and co-organised the IPICS academic summer school in 2016.

Svetla Nikova is a research expert in the research group COSIC of KU Leuven, Belgium. Prior to that she was assistant professor in University of Twente, NL. She is a coauthor of more than 80 research papers in international journals and conferences. Among others she has co-invented together with Vincent Rijmen the side-channel resistance method called Threshold Implementations. She has been involved in a number of projects (EU, Flemish, NL) Most recently she is also co-PI of a research project about Threshold Implementations funded by NIST. Svetla Nikova is a Member of the MC of the ICT COST Action IC1306 Cryptography for Secure Digital Interaction and was a member of the Board of Directors of IACR (2014-2015). She is a member of the steering committee of CARDIS, and she was a Program Chair of EuroPKI 2011 and WAIFI 2016 and General Chair of PROOFS 2012 and Eurocrypt 2015. She is serving in a number of PCs - Eurocrypt 2016, Asiacrypt 2016, FSE , SAC etc.

Vincent Rijmen is a full professor at the University of Leuven (KU Leuven), Belgium. Together with Joan Daemen, he designed the Advanced Encryption Standard (AES). He has co-authored more than 100 research papers in international journals and conferences, and a book on the design of the AES. He has been program co-chair of the conferences Indocrypt 2010, Selected Areas in Cryptography (SAC) 2009, Central European Conference on Cryptography and Coding (CECC) 2008, RFIDSec 2007, Fast Software Encryption (FSE) 2006. He has been PC member of many international conferences in the field of cryptography. He is currently editor of the Journal of Cryptology and the journal "Designs, Codes & Cryptography".

6. REFERENCES

[1] D. Boneh, R. A. DeMillo, and R. J. Lipton. *On the Importance of Checking Cryptographic Protocols for Faults*, pages 37–51. Springer Berlin Heidelberg, Berlin, Heidelberg, 1997.

[2] P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In N. Koblitz, editor, *Advances in Cryptology CRYPTO 96*, volume 1109 of *LNCS*, pages 104–113. Springer Berlin Heidelberg, 1996.

[3] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In M. Wiener, editor, *Advances in Cryptology CRYPTO 99*, volume 1666 of *LNCS*, pages 388–397. Springer Berlin Heidelberg, 1999.

[4] S. Nikova, C. Rechberger, and V. Rijmen. Threshold implementations against side-channel attacks and glitches. In P. Ning, S. Qing, and N. Li, editors, *Information and Communications Security*, volume 4307 of *LNCS*, pages 529–545. Springer Berlin Heidelberg, 2006.