# Emerging Attacks and Solutions for Secure Hardware in the Internet of Things

Chip Hong Chang, *Fellow, IEEE*, Marten van Dijk, Ulrich Rührmair, and Mark M. Tehranipoor , *Fellow, IEEE*

IT could well be argued that the emerging internet of things (IoT), together with the two long-standing trends of pervasive and ubiquitous computing, constitutes one of the most massive civil endeavors in the history of mankind. While it promises outstandingly positive usability and convenience effects, its implications for security and privacy are less clear. The vision of billions of low-cost, lightweight, and highly interconnected endpoints certainly rises a host of pressing issues to both cryptographers and system designers. Ideally, these should be resolved prior to a large-scale deployment of the IoT, and before its underlying infrastructure and standards have been established.

This special issue is devoted to proactive and foresightful research on *"Emerging Attacks and Solutions for Secure Hardware in the Internet of Things."* It so aims at contributing solid hardware foundations for a secure and privacy-preserving future IoT. Overall, the special issue received 27 high-quality submissions, 14 of which had to be accepted. Each article went through a rigorous peer review process, in addition to several follow-up rounds with the authors. A summary of the accepted articles (in arbitrary order) is given below.

In *"A Highly Efficient Side Channel Attack with Profiling through Relevance-Learning on Physical Leakage Information,"* a team of researchers from Singapore developed a novel and efficient method for side channel attacks, that advantageously applies machine learning methods on the measured data. It exhibits significant performance advantages over certain existing methods.

In the article *"A Secure Exception Mode for Fault-Attack-Resistant Processing,"* researchers from Virginia Tech proposed a generic technique to detect and react to fault attacks on embedded software. Their countermeasure combines a micro-architecture extension in hardware with a secure trap in software, leading to a secure exception mode to handle fault attacks.

The work on *"A Silicon PUF based Entropy Pump"* by scientists from the University of Maryland proposes a novel and innovative use for PUFs: They demonstrate that the internal, manufacturing variation based entropy of PUFs can be used to boost the (often all too low) entropy of passwords. This increases password strength and makes fraudulent logins more difficult.

The authors of *"Atlas: Application Confidentiality in Compromised Embedded Systems,"* which come from Leuven and Erlangen, propose and study a new hardware method for guaranteeing security and isolation even if the operating system of an embedded system has been compromised. Their method leads to minimal cycle overheads, at the cost of a reduced maximum frequency.

In their work *"Building PUF-Based Authentication and Key Exchange Protocol for IoT without Explicit CRPs in Verifier Database,"* a team of researchers from Kharagpur, Kolkata and Bangalore develops a new technique by which PUF-responses do not need to be stored in the clear at the verifier in identification protocols. This evades a main attack point in vulnerable verifiers in typical IoT-settings.

In *"Building a Trustworthy Execution Environment to Defeat Exploits from both Cyber Space and Physical Space for ARM,"* authors from Pennsylvania, Georgia, Washington and Boston deal with the problem of secure execution and comprised operating systems. They provide a comprehensively protected execution environment for unmodified application running on ARM-based IoT devices.

The publication *"Ciphertext-only Fault Analysis on the LED Lightweight Cryptosystem in the Internet of Things"* deals with the security of lightweight ciphers in the IoT. Its authors from Shanghai discuss a certain fault injection attack on the LED cipher that improves attack efficiency. Their techniques and analyses provide novel insights also for the security of other lightweight ciphers.

The article *"Decay-Based DRAM PUFs in Commodity Devices"* by colleagues from Yale, Darmstadt and Eindhoven describes the use of DRAM cells in commodity devices as PUFs. Among other things, their work shows how to establish secret keys in IoT-hardware that does not carry non-volatile memory, but merely DRAMs. This allows convenient individualization and identification of such hardware.


- *C. H. Chang is with the NTU Singapore 639798, Singapore. E-mail: echchang@ntu.edu.sg.*
- *M. van Dijk is with the University of Connecticut, Storrs-Mansfield, CT 06269. E-mail: marten.van_dijk@uconn.edu.*
- *U. Rührmair is with the LMU München, München 80333, Germany. E-mail: ruehrmair@ilo.de.*
- *M. M. Tehranipoor is with the University of Florida, Gainesville, FL 32611-6200. E-mail: tehranipoor@ece.ufl.edu.*


*For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.*
*Digital Object Identifier no. 10.1109/TDSC.2019.2901048*

The authors of *"Detecting Fault Injection Attacks Based on Compressed Sensing and Integer Linear Programming,"* all coming from Shenzhen, investigate fault injection attacks, one of the main potential physical attack forms against IoT endpoints. They suggest a new fault injection detection method that is not based on physical sensors, but mainly on inexpensive software methods.

In *"GaitLock: Protect Virtual and Augmented Reality Headsets Using Gait,"* an international team from Harbin, Coventry, Shenzhen, Sydney and Boston deals with the possibility of identifying users by their gait, i.e., by walking a few steps. In this process, they introduce a new gait recognition model. Their contribution allows user identification beyond classical retina or fingerprint scans in the IoT.

By publishing *"HAL— The Missing Piece of the Puzzle for Hardware Reverse Engineering, Trojan Detection and Insertion,"* researchers from Amherst and Bochum discuss the pressing problem of Trojan detection and insertion. They deal with methods to detect and also to insert Trojans based on netlists and other information.

In the work *"High Rate Robust Codes with Low Implementation Complexity,"* authors from Bar Ilan University deal with robust codes, which can detect any errors with non-zero probability. This allows them to effectively notice any fault injection attacks, for example against IoT hardware. The article presents new constructions for close to optimum, low complexity, high rate codes.

By developing *"Memory-Efficient Implementation of Elliptic Curve Cryptography for the Internet-of-Things,"* an international team from Nanjing, Luxembourg, Busan, Salerno and San Antonio deals with particularly efficient cryptographic implementations of elliptic curve algorithms. They can substantially enhance speed and memory requirements, both key factors in IoT-settings.

In *"Noisy Vibrational Pairing of IoT Devices,"* the authors from Birmingham, Alabama study a novel method for exchanging keys and identifying IoT-devices that are in close physical proximity to each other. They show how to mask a vibrational channel by use of standard speakers in the device, securing it against acoustic eavesdroppers.

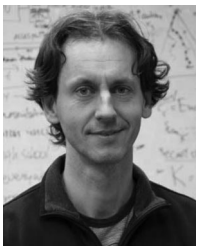
The above works indeed make various substantial contributions to their respective fields. The following list, which subsumes some of the long-standing questions and research targets in the area, may guide and inspire follow-up activities:

- How can billions of secret keys in vulnerable, inexpensive devices be effectively protected against physical and malware attacks?
- How can we realize tamper-protection in small, highly mobile, and lightweight IoT-endpoints?
- How can the non-malicious and unaltered behavior of unknown hardware and communication partners be proven remotely?
- How can potentially malicious manufacturers be detected, and/or their impact on IoT-security be minimized?
- How can long-term security and confidentiality be established with computationally and battery constrained hardware?
- How can secure physical data storage for large data volumes be established in typical IoT-devices?
- How can we preserve user privacy in pervasive, ubiquitous IoT-scenarios?

We hope that this volume can deliver new insights, and inspire coming research activities, on the long and thorny road to a secure and privacy-preserving future IoT.

*Guest Editors*
Chip-Hong Chang
Marten van Dijk
Ulrich Rührmair
Mark M. Tehranipoor

**Chip Hong Chang** received the BEng Hons degree from the National University of Singapore, in 1989, and the M Eng and PhD degrees from Nanyang Technological University (NTU) of Singapore, in 1993 and 1998, respectively. He served as a technical consultant in industry prior to joining the School of Electrical and Electronic Engineering (EEE) of NTU, in 1999, where he is currently an associate professor. He held joint appointments with the university as assistant chair of Alumni of the School of EEE from 2008 to 2014, deputy director of the Center for High Performance Embedded Systems from 2000 to 2011, and program director of the Center for Integrated Circuits and Systems from 2003 to 2009. He has coedited four books, published ten book chapters, around 100 international journal papers (more than two-thirds are IEEE) and more than 170 refereed international conference papers (mostly in IEEE), and delivered more than 30 colloquia. His current research interests include hardware security and trustable computing, low-power and fault-tolerant computing, residue number systems, and application-specific digital signal processing algorithms and architectures. He serves as the associate editor of *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, since 2011, *IEEE Access*, since 2013, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, and *IEEE Transactions on Information Forensic and Security*, since January 2016, *IEEE Transactions on Circuits and Systems-I*, from 2010 to 2013, *Integration, the VLSI Journal*, from 2013 to 2015, *Springer Journal of Hardware and System Security*, since June 2016 and *Microelectronics Journal*, since May 2014. He was the editorial advisory board member of *Open Electrical and Electronic Engineering Journal*, from 2007 to 2013 and *Journal of Electrical and Computer Engineering*, from 2008 to 2014, as well as the guest editor of special issues for *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Circuits and Systems-I*, *Journal of Circuits, Systems and Computers and Journal of Electrical and Computer Engineering*. He has served key appointments in organizing committee and technical program committee for more than 60 international conferences (mostly IEEE). He is a fellow of the IEEE and the Institution of Engineering and Technology (IET), and the 2018-2019 distinguished lecturer of *IEEE Circuits and Systems Society*.



**Marten van Dijk** received the MS degree in mathematics, and 2nd MS degree in computer science, and the PhD degree in mathematics, from Eindhoven the University of Technology. He has more than 20 years research experience in system security both in academia and industry. He is now the Charles H. Knapp associate professor in the ECE Department at UConn. He worked for two and a half years at RSA Laboratories in cybersecurity. He has published more than 100 papers in applied cryptography and hardware security and is quoted more than 8,000 times on Google scholar. Prior to RSA Laboratories, he was a research scientist at MIT CSAIL working together with Prof. Srini Devadas, with an emphasis on processor architectures that offer strong security guarantees. Most notably, this collaboration led to the introduction of the first circuit realizations of Physical Unclonable Functions (PUFs) which received the A. Richard Newton Technical Impact Award in Electronic Design Automation in 2015 (and the ACSAC'02 outstanding student paper award); it led to the design of Aegis, the first single-chip secure processor that verifies integrity and freshness of external memory which was selected for inclusion in "25 years of International Conference on Supercomputing" in 2014; and gave rise to a simple and efficient Oblivious RAM which received a best student paper award at CCS 2013. The IRIS authenticated file system with proofs of retrievability received the NYU-Poly AT&T Best Applied Security Paper Award, 3rd place, 2012. His work on fully homomorphic encryption over the integers was nominated (1 out of 3) for best paper award at Eurocrypt 2010. Prior to working in system security he was a research scientist at the digital signal processing group at Philips Research where he became the lead inventor of the error correcting codes used in Blu-ray disc.

**Ulrich Rührmair** received his MSc degree in Mathematics and the Foundations of Computer Science from the University of Oxford. He holds two PhD degress: A PhD in computer science from TU Berlin, and a PhD in electrical engineering from TU Munich. He has founded and led the physical cryptography project at TU Munich for several years, and headed a working group on Physical Cryptography and Security at the Horst Görtz Institute for IT-Security at the University of Bochum. Ulrich has written more than 50 publications on physical unclonable functions, hardware security, applied cryptography, and related topics, and given numerous invited talks, including presentations at Yale, Harvard, MIT, and ETH Zürich. He furthermore served as keynote speaker at SOFSEM 2011 and IEEE IVSW 2016. He has been called to the program committees (PCs) of the two top security conferences IEEE S&P ("Oakland") and ACM CCS, and to the two leading hardware security conferences HOST and CHES, multiple times, and has acted as reviewer for manifold top tier journals, including *Nature Communications*, *Nature Nanotechnology*, *IEEE T-IFS*, etc. In 2014, he organized a special session on "How secure are PUFs really? On the reach and limits of current PUF attacks" at DATE in Dresden. He is the founder and steering committee member of the ASHES workshop at ACM CCS.

**Mark M. Tehranipoor** is currently the Intel Charles E. Young Preeminence Endowed professor in cybersecurity at the University of Florida. His current research projects include hardware security and trust, supply chain security, VLSI design, test and reliability. He has published more 400 journal articles and refereed conference papers and has given about 200 invited talks and keynote addresses. He has published 11 books and more than 20 book chapters. He is a recipient of several best paper awards as well as the 2008 IEEE Computer Society (CS) Meritorious Service Award, the 2012 IEEE CS Outstanding Contribution, the 2009 NSF CAREER Award, and the 2014 MURI award. He serves on the program committee of more than a dozen of leading conferences and workshops. He served as program chair of the 2007 IEEE Defect-Based Testing (DBT) workshop, program chair of the 2008 IEEE Defect and Data Driven Testing (D3T) workshop, co-program chair of the 2008 International Symposium on Defect and Fault Tolerance in VLSI Systems (DFTS), general chair for D3T-2009 and DFTS-2009, and vice-general chair for NATW-2011. He co-founded the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) and served as HOST-2008 and HOST-2009 general chair. He is currently serving as an associate editor for *Journal of Electronic Testing Theory and Applications*, *Journal of Low Power Electronics*, *IEEE Xplore: IEEE Transactions on Very Large Scale Integration* and *ACM Transactions on Design Automation of Electronic Systems*. Prior to joining UF, he served as the founding director for CHASE and CSI centers at the University of Connecticut. He is currently serving as co-director for Florida Institute for Cybersecurity Research (FICS). He is a fellow of the IEEE, a golden core member of IEEE, and member of ACM and ACM SIGDA.