Tutorial T7

Physically Unclonable Function: a Promising Security Primitive for Internet of Things

Debdeep Mukhopadhyay, Indian Institute of Technology Kharagpur, India
Rajat Subhra Chakraborty, Indian Institute of Technology Kharagpur, India
Phuong Ha Nguyen, Indian Institute of Technology Kharagpur, India
Durga Prasad Sahoo, Indian Institute of Technology Kharagpur, India

Abstract

Internet of Things (IoT) is a network of large number of uniquely identifiable intercommunicating "smart" devices that promise to transform our lives. Lightweight authentication protocols for resource {constrained smart devices should be secure against "physical attacks" such as *Side-Channel Attack. Physically Unclonable Functions (PUFs)* are a class of novel hardware security primitives that promise a paradigm shift in many security applications and protocols. In essence, a PUF circuit is a partially disordered system that has an instance{speci_c input{output behavior that cannot be replicated by man- ufacturing (hence \physically unclonable"). The unique features of PUFs avoid explicit key storage, and thus make them immune against many of the existing physical attacks which aim to divulge the secret key of cryptographic algorithms. However, the concept of PUF is not a panacea in the domain of security, and they are still vulnerable to several forms of intelligent attacks, using a combina- tion of concepts borrowed from side-channel analysis and machine learning. In this tutorial, we would explore design challenges, operating principles, attacks and defence strategies for PUF circuits. The tutorial would cover the follow-
ing topics: *Fundamentals of PUF, Lightweight PUF Designs, Security Analysis of PUFs* and *PUF-based Authentication Protocols.*

Keywords: Cryptography, design for security, hard- ware security primitive, machine learning, physical attacks, physically unclonable functions, side-channel analysis.

Speaker Biographies

Debdeep Mukhopadhyay received the B.Tech. degree from the Department of Electrical Engineering, IIT Kharagpur, Kharagpur, India, and the M.S. and Ph.D. degrees in computer science and engineering from IIT Kharagpur. He was an Assistant Professor with the Department of Computer Science and Engineering, IIT Madras, Chennai, India, and is currently an Associate Professor with the Department of Computer Science and Engineering, IIT Kharagpur. His research interests include cryptography, VLSI of cryptographic algorithms, and side channel analysis. He is the recipient of the Indian Semiconductor Association TechnoInventor Award for best Ph.D. thesis in 2010, the Indian National Science Academy Young Scientist Award in 2010, the Indian National Academy of

1063-9667/15 $31.00 © 2015 IEEE
DOI 10.1109/VLSID.2015.115

Engineers Young Engineer Award in 2010, the Associate of Indian Academy of Science in 2011, the Outstanding Young Faculty Fellowship in 2011, and the IUSSTF Fellowship in 2012.

Rajat Subhra Chakraborty is an Assistant Professor in the Computer Science and Engineering Department of IIT Kharagpur since 2010. He has a Ph.D. in Computer Engineering from Case Western Reserve University (USA) and a B.E. (Hons.) in Electronics and Telecommunication Engineering from Jadavpur University (India) in 2005. His professional experience includes a stint as CAD Software Engineer at National Semiconductor, and a graduate internship at AMD Headquarters at Santa Clara (California). His research interests include Hardware Security; including design methodology for hardware IP/IC protection; Hardware Trojan detection and prevention through design and testing, attacks on hardware implementation of cryptographic algorithms, and reversible watermarking for digital content protection. He has close to 50 publications in international journals and conferences of repute. He has delivered keynote talks and tutorials at several international conferences and workshops, and has rendered his service as a reviewer and program committee member for multiple international conferences and journals. He is the co-author of four book chapters, one published book: \Reversible Digital Watermarking: Theory and Practice" (Morgan Claypool, USA), and one forthcoming book: \Hardware Security" (CRC Press, USA). He is one of the recipients of the “IBM Faculty Award” for 2012, and a “Royal Academy of Engineering (U.K.) Fellowship” in 2014. He holds 1 U.S. patent, and 2 more international patents and 3 Indian patents have been _led based on his research work. Dr. Chakraborty is a member of IEEE.

Phuong Ha Nguyen is a Research Fellow in the Computer Science and Engineering Department of IIT Kharagpur since 2014. He has a Ph.D. in Cryptography from Nanyang Technological University (Singapore) in 2013 and a Specialist (Hons.) in Computer Science from Moscow State University (Russia) in 2008. He was a Research Associate at Temasek Lab@ NTU (Singapore) from August-2012 to August-2013. His research interests include cryptanalysis, crypto system design, side channel attacks and physically unclonable functions. He has 7 publications in international journals and conferences of repute. He has rendered his service as a reviewer for multiple international conferences and journals. He holds 1 U.S. patent and 1 submitted patent based on his research work.

Durga Prasad Sahoo is a Ph.D. Research Fellow in the Computer Science and Engineering Department of IIT Kharagpur since 2012. He received B.Sc., M.Sc., and M.Tech. from University of Calcutta in 2007, 2009, and 2011, respectively. His research interests include Physically Unclonable Function (PUF), and Secured Embedded System Design.