Hardware Security: A 21st Century Perspective

Debdeep Mukhopadhyay, Rajat Subhra Chakraborty, and Chester Rebeiro
Dept. of Computer Science and Engineering
Indian Institute of Technology Kharagpur
Kharagpur, India – 721302

{debdeep, rschakraborty, chester}@cse.iitkgp.ernet.in

With the ever-increasing proliferation of e-business practices, great volumes of business transaction and data transmission are routinely carried out in an encrypted form in devices ranging in scale from personal smartcards to business servers. These algorithms are often computationally intensive and most implementations of these algorithms leak information that can be exploited by an adversary to gather information about the secret encryption key. Side-by-side, economic reasons dictate the widespread participation of external agents in modern design and manufacture of integrated circuits (ICs), which decreases the control that the IC design houses used to traditionally have over their own designs. This issue raises the question of ensuring *Trust* in an integrated circuit, and whether the entire design and manufacturing flow can be certified to be piracy-free. This tutorial explores these pertinent threats in the domain of hardware security and discusses solutions for them from different perspectives such as algorithm and circuit design, CAD, circuit testing, etc.

Designs of both symmetric and asymmetric key cryptographic algorithms are the heart of almost all security applications. The first part of the tutorial surveys hardware implementations of these security primitives. This includes efficient (in terms of latency, throughout, area, power) and real-time hardware implementation of non-linear Boolean functions and complex arithmetic building blocks (often for large operands) for symmetric and asymmetric key cryptographic algorithms, under resource-constrained platforms. In particular, the tutorial would focus on the hardware implementation challenges and solutions for the "Advanced Encryption Standard" (AES) and "Elliptic Curve Cryptography" (ECC) algorithms.

The tutorial would then investigate attacks which exploit information leaked from hardware implementations of cryptographic algorithms. These attacks are extremely potent and a threat to most cryptographic systems in use today. *Simple power analysis* and *differential power analysis* derive the secret key by analyzing the circuit current transient; *fault attacks* are based on the controlled induction of a fault and then analysis of faulty cipher-text produced from a VLSI implementation of the cryptographic algorithm; *cache timing attacks* are based on the correlation of the secret key of the cryptographic algorithm with the cache-timing characteristics of an embedded implementation. The tutorial would review the threat from these attacks, as well as algorithmic, circuit and system level protection methods against these threats.

The next part of the tutorial investigates the threat of hardware intellectual property (IP) piracy. Hardware IPs are pre-verified, ready-to-use circuit building blocks used in complex modern SoCs. The business of providing and using IPs has become a standard practice, especially among "fabless" semiconductor companies. With the greater

acceptance of FPGAs as a deployment platform rather than a prototyping-only platform, this business model is only going to increase in popularity in near future. However, recent trends of hardware IP piracy by illegal copying and cloning have become a cause of great concern to the IP vendors, resulting in loss of millions of dollars in revenue. In this tutorial we would explore the threat of hardware IP piracy, and design and platform-specific techniques for hardware IP protection. Another threat is the piracy in Integrated circuits (IC). This is similar to the threat of hardware IP piracy, only in this case ICs are illegally copied and cloned in remote fabrication facilities. Sometimes, the ICs can be reverse-engineered and then copied. The tutorial would explore the threat posed by IC piracy and design techniques to prevent them.

The final part of the tutorial delves into hardware Trojans. These are malicious circuitry which can be triggered in-field post-deployment and affect normal circuit operation, potentially with catastrophic consequences in critical application areas and public infrastructure. Such malicious circuitry can also be inserted by CAD automation tools obtained from untrusted third party vendors. Several unexplained military mishaps around the world in recent years are suspected to be the result of undetected hardware Trojans in the electronic systems. This tutorial would explore the operating modes and models of hardware Trojans, and design and testing techniques to prevent/detect them. In addition, it would investigate novel Trojan designs arising out of the malicious nexus between multiple parties associated with the design and manufacturing flow, which can evades all known detection techniques.

Biographical Sketch:

Dr. Debdeep Mukhopadhyay is presently working as an Assistant Professor in the Computer Science and Engineering department of Indian Institute of Technology (IIT) Kharagpur. Prior to this he worked as an Assistant Professor in the Computer Science department of IIT Madras. He obtained his BTech degree in Electrical Engineering , MS and PhD in Computer Science, IIT Kharagpur. He has been the author of more than 60 international conference and journal papers in Cryptography, Security and VLSI and has co-authored a text book on Cryptography and Network Security. He has collaborated with several organizations, like ISRO, DIT, ITI, CAIR-DRDO, Broadcom USA and NTT-Labs Japan. He has been the recipient of the *Indian Semiconductor Association (ISA) TechnoInventor Award* for best PhD Thesis in 2008, and has been selected for the *Indian National Science Academy Young Scientist Award 2010 and Indian National Academy of Engineers (INAE) Young Engineer Award 2010.* His research interests include VLSI of Cryptographic algorithms and Side Channel Analysis.

Dr. Rajat Subhra Chakraborty is an Assistant Professor in the Computer Science and Engineering Department of IIT Kharagpur. He received his Ph.D. degree in Computer Engineering from Case Western Reserve University (2010) and a B.E. (Hons.) degree in Electronics and Telecommunication Engineering from Jadavpur University (2005). He has held engineering and internship positions at National Semiconductor (India) and AMD (California). He has about 25 publications in international journals and conferences of repute. He has received multiple student travel awards from IEEE and ACM, and a graduate student award for academic excellence from Case Western Reserve University. He is the holder of one provisional U.S. patent. His research interest includes hardware security, including design methodology for hardware IP/IC protection, hardware Trojan detection/prevention, and prevention of attacks on hardware implementation of cryptographic algorithms.

Mr. Chester Rebeiro is a PhD scholar in the Department of Computer Science and Engineering, *IIT Kharagpur*. He has a Bachelor's degree in Instrumentation and Electronics from *Bangalore University* (1998) and an MS degree in Computer Science from *IIT Madras (2009).* From 1999 to 2009, he was a member technical staff in *C-DAC,* Bangalore. While at C-DAC, he has handled courses on ARM SoC at the *Advanced Computing Training School* and has also conducted training on Computer architecture and Cryptography for the *Research and Analysis Wing*. He has over 15 publications in reputed international conferences and journals. His research interests include side-channel attacks and high performance implementations of cryptographic and cryptanalytic algorithms.