Faculty Candidate Talk

Department of Computer Science and Engineering
Indian Institute of Technology Kanpur

Side-Channel Analysis: Attacks and Constructions for Resilience

Bodhisatwa Mazumder
Postdoctoral Fellow
New York University at Abu Dhabi

Date: September 28, 2016
Time: 4:00 pm -- 5:30 pm
Venue: RM 101

Abstract: In today's world, side-channel attacks have become one of the most serious threats to standard cryptosystems in practice. Instead of targeting the mathematical structure, which is usually sound and robust, these attacks attempt to gain information about the secret key from the leakage from the physical implementation of the algorithm itself. Among these attacks, the power analysis and timing attacks have received significant attention as they are highly powerful and do not usually require the knowledge of implementation on the target device on which the attack is performed. The talk will first focus on characterization of crypto-primitives called block cipher S-boxes for power analysis resilience. In this part, the relation between cryptographic parameters of coordinate functions of S-boxes that define the power-analysis resilience, will be addressed. Based on such properties, a class of S-boxes will be proposed that have improved power-analysis resilience as compared to standard S-boxes such as AES Rijndael S-box along with a marginal tradeoff of classical cryptographic properties.

The next part of the talk will discuss constructions of rotation symmetric S-boxes (RSSBs) that have improved power analysis resilience along with good cryptographic properties like high nonlinearity, low global avalanche characteristics and high algebraic degree. The evaluation of security metric called guessing entropy on the proposed class of RSSBs show that as compared to Rijndael S-box, a side-channel adversary requires more computational effort to exploit the information leakage when these S-boxes are plugged in AES block cipher.

The final part of the talk will emphasize on timing attack vulnerabilities of cryptographic implementations that are based on nano-electromechanical systems (NEMS), which is regarded as one of the important emerging technologies. NEMS based devices have a significantly small power dissipation compared to CMOS technologies owing to zero leakage current and static power loss. However, despite its zero static leakage, NEMS relay technology suffer from large delay compared to CMOS technology. Binary Decision Diagram (BDD) based implementations of NEMS relay design targets minimizing the total delay. However, this implementation renders the timing delay of the output of a BDD input-dependent, which is a threat to security-critical applications, such as cryptographic ciphers. In this part, we analyze the impact of the input-dependent timing variation on the security of NEMS relay based block cipher implementations.

Biography: Bodhisatwa Mazumdar is presently a post-doctoral researcher in the Design-for-Excellence laboratory in New York University Abu Dhabi. He earned his PhD degree in Computer science and Engineering in 2015, and MS degree in Electronics and Electrical Communication Engineering in 2009, both from IIT Kharagpur. He obtained his B. Tech degree in Electronics and Instrumentation Engineering from University of Kalyani in 2004. His research interest lies in side-channel analysis of cryptographic primitives such as S-boxes, security vulnerability analysis, and emerging technologies in VLSI Design.