Invited Talk
Department of Computer Science and Engineering
Indian Institute of Technology Kanpur

Fault Tolerant Implementation of Cryptosystems: From Attacks to Defences

Speaker
Prof. Debdeeb Mukhopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
URL: http://cse.iitkgp.ac.in/~debdeep/

Venue: RM 101
Time: 11:00 - 12:30

Abstract

In today's world security requirements of various information disciplines, e.g., networking, telecommunications, database systems, and mobile applications, have caused applied cryptography to gain immense importance. In order to satisfy the high throughput requirements of such applications, the cryptographic systems are implemented either as cryptographic accelerators (ASIC and FPGA implementations), or as cryptographic libraries (optimized software routines). The complex hardware and software implementations are raising concerns regarding their security and reliability.

In this talk, we first present Differential Fault Analysis (DFA) on AES which can be used to obtain the key using a single fault induction. Subsequently, we extend these attacks to multiple byte faults, using a new fault model based on the diagonals of the AES state matrix. The work shows that the cipher can be attacked if one, two or three diagonals are affected needing 2, 2 or 4 faulty cipher-texts respectively to uniquely obtain the key. In order to thwart such powerful attacks, fault tolerance is introduced in block ciphers through either detection or infective schemes. However, there is a gap!; While conventional fault tolerance offers large amount of reliability under the assumption that all faults are equally likely, an attacker is equipped with a biased fault injection mechanism, which can threaten most existing fault tolerant architectures. We demonstrate that bias in the fault injections can be used to break popular detection schemes, which rely on redundancy using a technique known as the Differential Fault Intensity Analysis (DFIA) that combines principles of differential power analysis with fault attacks. We formalize the notion of bias of a fault model using the variance of the fault distribution. We also investigate infective countermeasures against fault attacks where there is no explicit comparison step unlike the detection schemes. However, even such schemes can be countered via stronger attack models like instruction skip. Finally, we present a fault tolerant implementation of the infective countermeasure using Idempotent Instructions, which reduces the threat of such skips

significantly. Overall, we claim to increase significantly the security margin against several known fault models.

Bio

Dr. Debdeep Mukhopadhyay is currently an Associate Professor at the Department of Computer Science and Engineering, Indian Institute of Technology at Kharagpur, India. At IIT Kharagpur he initiated the Secured Embedded Architecture Laboratory (SEAL), with a focus on Embedded Security and Side Channel Attacks (http://cse.iitkgp.ac.in/resgrp/seal/). Prior to this he worked as a visiting Associate Professor of NYU-Shanghai. He had also served as an Assistant Professor at IIT Madras, India and as a Visiting Researcher at NYU Polytechnic School of Engineering under the Indo-US STF Fellowship. He holds a PhD, an MS, and a B. Tech from IIT Kharagpur, India. Dr. Mukhopadhyay's research interests are Cryptography, Hardware Security, and VLSI. His books include Cryptography and Network Security (Mc Graw Hills), Hardware Security: Design, Threats, and Safeguards (CRC Press), and Timing Channels in Cryptography (Springer). He has written more than 100 papers in peer-reviewed conferences and journals and has collaborated with several Indian and Foreign Organizations. Dr. Mukhopadhyay is the recipient of the prestigious *Young Scientist award* from the Indian National Science Academy, the *Young Engineer award* from the Indian National Academy of Engineers, and is a Young Associate of the Indian Academy of Science. He was also awarded the Outstanding Young Faculty fellowship in 2011 from IIT Kharagpur, and the Techno-Inventor Best PhD award by the Indian Semiconductor Association. He has recently incubated a start-up on Hardware Security, ESP Pvt Ltd at IIT Kharagpur (http://esp-research.com/).