【Grant-in-Aid for Scientific Research (S)】

Broad Section J

Title of Project : Resilience Enhancement of IoT Ecosystem by Cryptographic Technologies

Kazuo Sakiyama
(The University of Electro-Communications, Graduate School of Informatics and Engineering, Professor)

Research Project Number : 18H05289 Researcher Number : 80508838
Keyword : Information Security, Cryptography, Information Theory, Hardware Security, IC Engineering

【Purpose and Background of the Research】

The purpose of this research is to improve the resilience of the IoT (Internet of Things) systems by considering the circulation of the security state, transited by physical attacks on an IoT device, as the function of IoT ecosystem. Cryptographic devices in the IoT era face the threat of new physical attacks that appear one after another. Laser-based fault attacks are known to be one of the most serious physical attacks against cryptographic IC (Integrated Circuit). If the attacker's ability becomes even higher, we must assume the probing attack that directly reads out intermediate values in IC. In this research, we develop a leakage sensor in order to measure the security state of the key in the cryptographic device, and in each layer of the cryptographic primitive, algorithm, and protocol, we aim to improve the resilience that recovers the IoT system lithely to the normal state even if partial key leakage occurs.

【Research Methods】

We set two specific research topics. The first is the proper introduction of cryptographic technology into IoT systems with physical attack countermeasures in mind. We plan to build a leakage detection technology to check whether the cryptographic key is in a normal condition and leakage-resilient cryptography to withstand key leakage by physical attacks.

The second topic is about the key lifecycle and resilience enhancement of IoT ecosystem. Based on the position that key leakage is inevitable, we consider the expansion of leakage-resilient cryptography that resists physical attacks even if the key leakage is suspected and its collaboration with the key distillation technology that extracts a secure key from a partially-leaked key.

The core technology in this research is cryptography and leakage sensor. In 2019, we design the first leakage sensor applying the optical sensor and the electromagnetic wave sensor and perform the operation verification and the security evaluation. In 2021, we develop a cryptographic device embedded with a leakage sensor and conduct collaborative research on leakage-resilient cryptography, key distillation, and leakage detection technology.

【Expected Research Achievements and Scientific Significance】

We expect to create novel IoT devices with physical attack countermeasures by integrating sensor and cryptographic technology. Theoretical research leads advanced topic such as the construction of a security proof technique incorporating physical parameters and information distillation excluding leaked key information. By combining the results of practical research and theoretical research, we believe that the circulation of the security state of the cryptographic key is achievable as one aspect of the IoT ecosystem.

The leakage sensor developed in this research is a technology that bridges physical and mathematical aspects around detection of the probing attack and can be said to be a new concept enabling a collaboration between different research fields. Namely, this research project functions as a source of academic knowledge creation related to countermeasures against physical attacks.

【Publications Relevant to the Project】

・K. Matsuda, T. Fujii, N. Shoji, T. Sugawara, K. Sakiyama, Y. Hayashi, M. Nagata, N. Miura, “A 286F²/cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser Against Laser Fault Injection Attack,” ISSCC 2018: 352-354 (2018).

・K. Sakiyama, Y. Li, M. Iwamoto, and K. Ohta, “Information-Theoretic Approach to Optimal Differential Fault Analysis,” IEEE Trans. Inf. Forensic Secur., 7(1): 109-120, (2012).

【Term of Project】 FY2018-2022

【Budget Allocation】 149,500 Thousand Yen

【Homepage Address and Other Contact Information】

http://sakiyama-lab.jp/study