Graduate School of Science and Technology Master's Thesis Abstract

Laboratory name (Supervisor)	Information Security Engineering (Yuichi Hayashi （Professor))		
Student ID	1911314	Submission date	2021 / 1 / 22
Name	HONG SEONGEON		
Thesis title	Evaluation of Efficiency of Fault Injection Analysis against Cryptographic Module under Controlling Temperature 温度制御下にある暗号モジュールに対する故障注入解析の効率評価		

Abstract

The fault injection attack intentionally induces a computational fault during the cryptographic calculation to obtain faulty cipher texts exploited to extract the secret key using differential fault analysis. The faults can be induced by setup time violation of integrated circuits. It occurs by heating ICs to slow down the speed of CMOS leading to delay in critical path. This phenomenon leads to setup time violation or early latching of data. In this paper, the vulnerability caused by controlling temperature on hardware security is studied. The proposed method of this paper is to improve efficiency of fault injection attack by making the target device vulnerable by controlling temperature. The proposed method makes it easier to inject faults. In order to investigate the effects of temperature on fault occurrence of encryption operation, the temperature was altered from 20 ºC to 40 ºC by 5 ºC changes. From the result of the experiment, it is observed that as temperature becomes higher, the occurrence of faults significantly increases. In theory, the probability of having 1byte fault in each round is the same. It means increased number of faulty outputs also provides increased chance of having 1byte fault in 8th or 9th round of AES encryption. This vulnerability reduces the difficulty of inducing faults into the target device. The result of the experiment can be threatening to hardware security since it is confirmed that fault can be injected efficiently by controlling the temperature. The means of heating is known to be not expensive. Therefore, attackers who can heat the target device are expected to obtain an increased amount of faulty outputs by fault injection attack.
Therefore, the vulnerability in cryptographic modules by controlling the temperature is threatening to hardware security. However, the experiment was conducted only on SASEBO-G, generality is not assured. Although only one device is tested, the FPGA is widely implemented in many cryptographic devices and they still can be heated. Therefore, the result of this paper is enough to provide awareness of threats.