A Study on Information Security Attack based Side-Channel Attacks

Young-Jin Kang*, Ndibanje Bruce*, SuHyun Park**, HoonJae Lee**

**Dept. Ubiquitous It, Dongseo University, Busan, Rep. of KOREA*

***Div. Of Information and Communication Engineering, Busan, Rep. of KOREA*

rkddudwls55@gmail.com, ndibabruce@gmail.com, {subak, hjlee}@dongseo.ac.kr

***Abstract*—Electronics devices are always targeted with different kind of attacks due to their activities related to data processing, data storages and data transactions. In each case, the attacker performs the attacker according to what he needs from the device. In this paper, we present various attacks types on electronics devices in particularly on crypto-module devices where we focus on side channel attacks in its form of attacks such as power analysis attack, electromagnetic attack and fault injection attack. Finally, we develop a series of countermeasures against the side-channels attacks on crypto-module devices where the result shows that they are resilient and achieve better efficient.**

***(Pt9)Keyword*—Side-Channel Attacks, Physical Attacks, Hardware-based Countermeasure, Software-based Countermeasure, Hardware Device**

Young-Jin Kang

2013: BS at Dongseo University, Republic of Korea
2015: MS at Dongseo University, Republic of Korea
2015 ~ current: doctor´s course Dongseo University, Republic of Korea
Research Interests: Wireless Sensor Networks, Cryptography and Network Security, Side Channel Analysis

Ndibanje Bruce

2004: BS at Ngozi University, Republic of Burundi
2013: MS at Dongseo University, Republic of Korea
2016: Ph.D at Dongseo University, Republic of Korea
Research Interest: Information Security, Wireless Sensor Networks, Cryptography and Network Security, Side Channel Analysis

SuHyun Park

1986: BS at Pusan National University, Republic of Korea
1988: MS at Pusan National University, Republic of Korea
1999: Ph.D at Pusan National University, Republic of Korea
1996 ~ current: Professor of Dongseo University, Republic of Korea
Research Interests: Maritime IT, Artificial Intelligence, Intelligent System

HoonJae Lee

1985: BS at Kyungpook National University, Republic of Korea
1987: MS at Kyungpook National University, Republic of Korea
1998: Ph.D at Kyungpook National University, Republic of Korea
2002 ~ current: Professor of Dongseo University, Republic of Korea
Research Interests: Password Theory, Network Security, Side-Channel Attack, Information Communication/Information Network