World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:03, 2015

Tamper Resistance Evaluation Tests with Noise Resources

Authors : Masaya Yoshikawa, Toshiya Asai, Ryoma Matsuhisa, Yusuke Nozaki, Kensaku Asahi

Abstract : Recently, side-channel attacks, which estimate secret keys using side-channel information such as power consumption and compromising emanations of cryptography circuits embedded in hardware, have become a serious problem. In particular, electromagnetic analysis attacks against cryptographic circuits between information processing and electromagnetic fields, which are related to secret keys in cryptography circuits, are the most threatening side-channel attacks. Therefore, it is important to evaluate tamper resistance against electromagnetic analysis attacks for cryptography circuits. The present study performs basic examination of the tamper resistance of cryptography circuits using electromagnetic analysis attacks with noise resources.

Keywords : tamper resistance, cryptographic circuit, hardware security evaluation, noise resources
Conference Title : ICCETA 2015 : International Conference on Computer Engineering : Theory and Application
Conference Location : Singapore, Singapore
Conference Dates : March 29-30, 2015