World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:09, 2015

Round Addition DFA on Lightweight Block Ciphers with On-The-Fly Key Schedule

Authors : Hideki Yoshikawa, Masahiro Kaminaga, Arimitsu Shikoda, Toshinori Suzuki

Abstract : Round addition differential fault analysis (DFA) using operation bypassing for lightweight block ciphers with on-the-fly key schedule is presented. For 64-bit KLEIN and 64-bit LED, it is shown that only a pair of correct ciphertext and faulty ciphertext can derive the secret master key. For PRESENT, one correct ciphertext and two faulty ciphertexts are required to reconstruct the secret key.

Keywords : differential fault analysis (DFA), round addition, block cipher, on-the-fly key schedule
Conference Title : ICACPS 2015 : International Conference on Applied Cryptography and Provable Security
Conference Location : Dubai, United Arab Emirates
Conference Dates : September 13-15, 2015