1. Hardware Trojans in wireless cryptographic ICs: Silicon demonstration & detection method evaluation

Accession number: 13999815

Authors: Yu Liu (1); Yier Jin (2); Makris, Y. (1)
Author affiliation: (1) Dept. of Electr. Eng., Univ. of Texas at Dallas, Dallas, TX, United States; (2) Dept. of Electr. Eng. & Comput. Sci., Univ. of Central Florida, Orlando, FL, United States

Source: 2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)
Publication date: 2013
Pages: 399-404
Language: English
ISBN-13: 978-1-4799-1071-7
Document type: Conference article (CA)
Conference name: 2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)
Conference date: 18-21 Nov. 2013
Conference location: San Jose, CA, USA
Sponsor: IEEE Counc. Electron. Design Autom.
Publisher: IEEE
Place of publication: Piscataway, NJ, USA
Material Identity Number: YXB4-1900-035

Abstract: We present a silicon implementation of a hardware Trojan, which is capable of leaking the secret key of a wireless cryptographic integrated circuit (IC) consisting of an Advanced Encryption Standard (AES) core and an Ultra-Wide-Band (UWB) transmitter. With its impact carefully hidden in the transmission specification margins allowed for process variations, this hardware Trojan cannot be detected by production testing methods of either the digital or the analog part of the IC and does not violate the transmission protocol or any system-level specifications. Nevertheless, the informed adversary, who knows what to look for in the transmission power waveform, is capable of retrieving the 128-bit AES key, which is leaked with every 128-bit ciphertext block sent by the UWB transmitter. Using silicon measurements from 40 chips fabricated in TSMC's 0.35µm technology, we also assess the effectiveness of a side channel-based statistical analysis method in detecting this hardware Trojan.

Number of references: 14
Inspec controlled terms: cryptography - invasive software - microprocessor chips - radio transmitters - radiofrequency integrated circuits - statistical analysis - ultra wideband communication
Uncontrolled terms: hardware trojans - wireless cryptographic IC - wireless cryptographic integrated circuit - silicon demonstration method evaluation - silicon detection method evaluation - secret key - advanced encryption standard core - ultra-wide-band transmitter - UWB transmitter - transmission specification margins - process variations - transmission power waveform - 128-bit AES key - TSMC 0.35µm technology - side channel-based statistical analysis method - silicon measurements - 128- bit ciphertext block
Inspec classification codes: B1350H Microwave integrated circuits - B2570 Semiconductor integrated circuits - B6250 Radio links and equipment - B6120D Cryptography - B1265F Microprocessors and microcomputers - B0240Z Other topics in statistics
Treatment: Practical (PRA); Theoretical or Mathematical (THR)
Discipline: Electrical/Electronic engineering (B)
DOI: 10.1109/ICCAD.2013.6691149
IPC Code: G06F15/76 - H01L27/00 - H04B1/02 - H04B7/00 - H04L9/00 - H04W - H04W84/18 - H04B1/7163
Database: Inspec

Data Provider: Engineering Village