Performing side channel attack on a commercial AES-256 device

Ohto Myllynen, Mika Kaustinen, Tero Jokela, Lauri Koskinen
Department of Future Technologies
University of Turku
Turku, Finland

In cryptography, a side-channel attack is any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms. For example, electromagnetic leaks can provide an extra source of information, which can be exploited to break the system. Side-channel attacks pose a serious threat to the security of cryptographic devices. In consequence, implementations have to be evaluated for their resistivity against such attacks and the incorporation of different countermeasures has to be considered.

We performed electromagnetic side channel attack on a commercial AES-256 USB-encryption module in ECB mode. First the module, proprietary software and USB -traffic were analyzed using electromagnetic probe to find supposed encryptions. Before actual attack, oscilloscope, electromagnetic probe with low-noise amplified and isolated power supply were used together with computer to record typically 10000 plaintexts encryptions. The plaintexts, encrypted plaintexts i.e. ciphertexts, and recorded oscilloscope traces of the electromagnetic probe were then used in actual attack. Correlation Power Analysis (CPA) method was used in the attack. Attack was performed in Matlab software. The power consumption (and thus the EM emission) of the device was modelled using hamming distance metric. Thus, finding correlation between modeled power consumption and measured traces allows us to extract the AES round keys one byte at a time. For AES-256 two last (rounds 13 and 14) round keys are needed to complete the key schedule. Finding the two round key therefore allows us to calculate back the full secret key of the module.

For successful attack several measurements were required to find right measurement setup for oscilloscope and electromagnetic head position. In our attack 30 out of the 32 round key bytes were found using side channel attack and the two remaining were found using brute force. The complexity of using brute force increases exponentially with the number of unknown bytes. Therefore finding more bytes by brute force becomes computationally extensive.

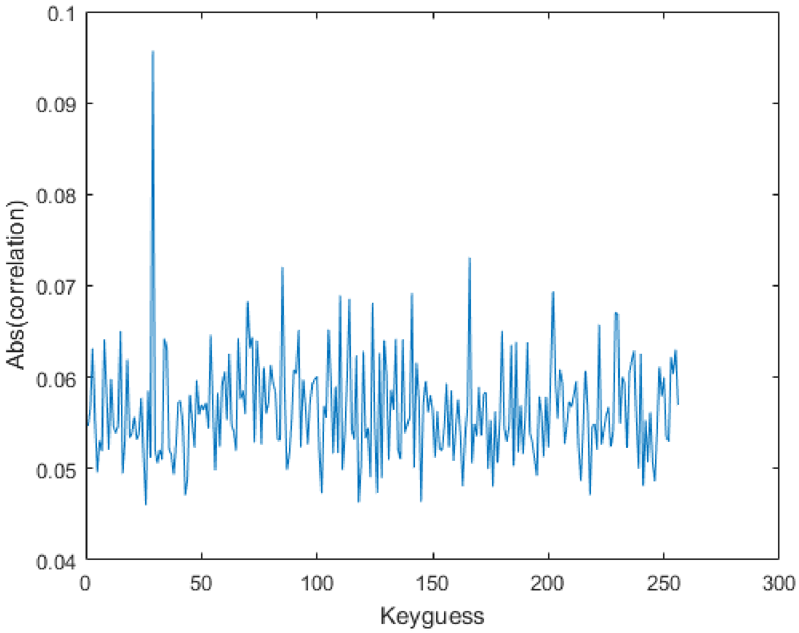

Figure: Correlation of different byte values of round key byte