Cryptology ePrint Archive: Report 2011/557

An Improved Trace Driven Instruction Cache Timing Attack on RSA

Chen Cai-Sen, Wang Tao, Chen Xiao-Cen and Zhou Ping

Abstract: The previous I-cache timing attacks on RSA which exploit the instruction path of a cipher were mostly proof-of-concept, and it is harder to put them into practice than D-cache timing attacks. We propose a new trace driven timing attack model based on spying on the whole I-cache. An improved analysis algorithm of the exponent using the characteristic of the size of the window is advanced, which could further reduce the search space of the bits of the key than the former and provide an error detection mechanism to detect some erroneous decisions of the operation sequence. We implemented an attack on RSA of OpenSSL under a practical environment, proving that the feasibility and effectiveness of I-Cache timing attack could be improved.

Category / Keywords: public-key cryptography / Instruction cache-timing attacks, side channel attack, RSA cryptographic algorithm, Trace-driven.

Date: received 9 Oct 2011

Contact author: caisenchen at 163 com