Cryptology ePrint Archive: Report 2011/710

Cryptanalysis of the Full AES Using GPU-Like Special-Purpose Hardware

Alex Biryukov and Johann Gro{\ss}sch{\"a}dl

Abstract: The block cipher Rijndael has undergone more than ten years of extensive cryptanalysis since its submission as a candidate for the Advanced Encryption Standard (AES) in April 1998. To date, most of the publicly-known cryptanalytic results are based on reduced-round variants of the AES (respectively Rijndael) algorithm. Among the few exceptions that target the full AES are the Related-Key Cryptanalysis (RKC) introduced at ASIACRYPT 2009 and attacks exploiting Time-Memory-Key (TMK) trade-offs such as demonstrated at SAC 2005. However, all these attacks are generally considered infeasible in practice due to their high complexity (i.e. $2^{99.5}$ AES operations for RKC, 2^{80} for TMK). In this paper, we evaluate the cost of cryptanalytic attacks on the full AES when using special-purpose hardware in the form of multi-core AES processors that are designed in a similar way as modern Graphics Processing Units (GPUs) such as the NVIDIA GT200b. Using today's VLSI technology would allow for the implementation of a GPU-like processor reaching a throughput of up to 10^{12} AES operations per second. An organization able to spend one trillion US\$ for designing and building a supercomputer based on such processors could theoretically break the full AES in a time frame of as little as one year when using RKC, or in merely one month when performing a TMK attack. We also analyze different time-cost trade-offs and assess the implications of progress in VLSI technology under the assumption that Moore's law will continue to hold for the next ten years. These assessments raise some concerns about the long-term security of the AES.

Category / Keywords: secret-key cryptography / AES, Cryptanalysis, Cryptanalytic Hardware

Date: received 30 Dec 2011

Contact author: johann groszschaedl at uni lu