Cryptology ePrint Archive: Report 2011/161

Efficient Hardware Implementations of BRW Polynomials and Tweakable Enciphering Schemes

Debrup Chakraborty and Cuauhtemoc Mancillas-Lopez and Francisco Rodriguez-Henriquez and Palash Sarkar

Abstract: A new class of polynomials was introduced by Bernstein (Bernstein 2007) which were later named by Sarkar as Bernstein-Rabin-Winograd (BRW) polynomials (Sarkar 2009). For the purpose of authentication, BRW polynomials offer considerable computational advantage over usual polynomials: $(m-1)$ multiplications for usual polynomial hashing versus $\lfloor\frac{m}{2}\rfloor$ multiplications and $\lceil\log_2 m\rceil$ squarings for BRW hashing, where m is the number of message blocks to be authenticated. In this paper, we develop an efficient pipelined hardware architecture for computing BRW polynomials. The BRW polynomials have a nice recursive structure which is amenable to parallelization. While exploring efficient ways to exploit the inherent parallelism in BRW polynomials we discover some interesting combinatorial structural properties of such polynomials. These are used to design an algorithm to decide the order of the multiplications which minimizes pipeline delays. Using the nice structural properties of the BRW polynomials we present a hardware architecture for efficient computation of BRW polynomials. Finally we provide implementations of tweakable enciphering schemes proposed in Sarkar 2009 which uses BRW polynomials. This leads to the fastest known implementation of disk encryption systems.

Category / Keywords: implementation / Pipelined architecture, tweakable enciphering schemes, Karatsuba multiplier, disc encryption, polynomial evaluation

Date: received 31 Mar 2011

Contact author: debrup at cs cinvestav mx