Efficient Scalable Hardware Architecture For Montgomery Inverse Computation In GF(P)

Gutub, A.A.A. Tenca, A.F.; Dept. of Comput. Eng., King Fahd Univ. of Pet. & Miner., Dhahran, Saudi Arabia;

Signal Processing Systems, 2003. SIPS 2003. IEEE Workshop on;Publication Date: 27-29 Aug. 2003;ISBN: 0-7803-7795-8

King Fahd University of Petroleum & Minerals

http://www.kfupm.edu.sa

Summary

The Montgomery inversion is a fundamental computation in several cryptographic applications. We propose a scalable hardware architecture to compute the Montgomery modular inverse in GF(p). We suggest a new correction phase for a previously proposed almost Montgomery inverse algorithm to calculate the inversion in hardware. The intended architecture is scalable, which means that a fixed-area module can handle operands of any size. The word-size, which the module operates, can be selected based on the area and performance requirements. The upper limit on the operand precision is dictated only by the available memory to store the operands and internal results. The scalable module is in principle capable of performing infinite-precision Montgomery inverse computation of an integer, modulo a, prime number. This scalable hardware is compared with a previously proposed fixed (fully parallel) design showing very attractive results.