Cryptology ePrint Archive: Report 2011/030

Fast Elliptic Curve Cryptography Using Optimal Double-Base Chains

Vorapong Suppakitpaisarn and Masato Edahiro and Hiroshi Imai

Abstract: In this work, we propose an algorithm to produce the double-base chains that optimize the time used for computing an elliptic curve cryptosystem. The double-base chains is the representation that combining the binary and ternary representation. By this method, we can reduce the Hamming weight of the expansion, and reduce the time for computing the scalar point multiplication (Q = rS), that is the bottleneck operation of the elliptic curve cryptosystem. This representation is very redundant, i.e. we can present a number by many expansions. Then, we can select the way that makes the operation fastest. However, the previous works on double-bases chain have used a greedy algorithm, and their solutions are not optimized. We propose the algorithm based on the dynamic programming scheme that outputs the optimized the double-bases chain. The experiments show that we have reduced the time for computing the scalar multiplication by 3.88-3.95%, the multi-scalar multiplication by 2.55-4.37%, and the multi-scalar multiplication on the larger digit set by 3.5-12%.

Category / Keywords: implementation / Elliptic Cruve Cryptography, Minimal Weight Conversion, Digit Set Expansion, Double-Base Chains

Date: received 17 Jan 2011

Contact author: mr_t_dtone at is s u-tokyo ac jp