Research of Public Key Cryptography Hardware with Ternary Logic

Masaaki Shirase
School of Information Science,
Japan Advanced Institute of Science and Technology

January 10, 2006

Abstract

There are two main types of cryptography, RSA and ElGamal. RSA requires many multiplications modulo the public key N for encryption/description. ElGamal requires many multiplications modulo p for encryption/decryption, where p is characteristic of a finite field. This research focus on XTR that is a type of ElGamal. XTR enable that the size of public key is a third and calculation amount of encryption/decryption is reduced compared with traditional ElGamal. This research shows that the size of public key of XTR can become moreover half using a finite field of characteristic 3. One of the theme of this paper is a hardware of XTR over characteristic 3.

This paper proposes TG method for design of ternary logic gates. TG method is of the best ternary logic gates at the moment, which designs any function gates using one variable function gate by Olson method with T gate. Gates by TG method The merit of TG method and Olson method are producible in the processing technology of CMOS that doesn't flow the current when stability, that is, power consumption is a little. Simulation of the gate by TG method is performed using HSPICE because the gate is similar to CMOS. This paper designs the hardware of XTR over characteristic 3 using gates by TG method, then estimate its performance.

Next, This paper propose that large scale Wallace tree multiplier is designed by ternary logic gates. Construction of Wallace tree is very simple using symmetric ternary notation, hence design of Wallace tree becomes easy. Large scale multiplier designed by ternary logic is benefit for Encryption/decryption of ElGamal using a finite field of large characteristic and RSA, because they require multiplications of large integers. This paper shows that there are version of symmetric ternary notation of "Montgomery multiplication" and "Residue algorithm modulo pseudo Mersenne prime", which are algorithms for residue unless division and used well by ElGamal and RSA. This paper explains that multiplier, adder and hardwares of their algorithms by ternary logic gate by TG method.

Key Words: Ternary logic, Public key Cryptography, symmetric ternary notation, finite field of characteristic 3, TG method