CORR 2001-61

Efficient Modular Operation for A Class of Moduli

Huapeng Wu, M. Anwar Hasan*, Ian F. Blake*

Abstract In this paper, we propose an efficient method to compute modular operation $X \pmod{N}$, where $X < N^2$. When the modulus N is in the form of $2^n + A$, where $-2^{n/2} \leq A \leq 2^{n/2}$, formulas which can significantly simplify modular operation are obtained. We show that the complexity in calculating modular operation depends on the hamming weight in the non-adjacent form (NAF) of the modulus. When a modulus is a sum of three positive or negative powers of 2, the modular operation is equivalent to performing not more than six addition operations with the operands of about the same as or less than modulus.

Keywords Modular arithmetic, integer ring, elliptic curve cryptosystem, RSA cryptosystem.