*Dynamics of Continuous, Discrete and Impulsive Systems*
*Series* **A:** *Mathematical Analysis* **11 (2004)** 675-689


# FAST MODULAR MULTIPLICATION AND PARALLEL ALGORITHMS IN PUBLIC-KEY CRYPTOSYSTEMS

Ping Luo and Yiqi Dai

Department of Computer Science
Tsinghua University, Beijing 100084

**Abstract.** A modular multiplication is one of the most important operations in public-key cryptography like RSA cryptosystem. This paper is just devoted to a practical method and construction of speeding up such operation. Furthermore, the modular multiplication expansions are given and based on these expansions the fast modular multiplication and parallel algorithms are proposed.

**Keywords.** Cryptography, parallel algorithm, public-key cryptosystem, modular multiplication.

**AMS (MOS) subject classification:** 94A60, 68P25, 68Q22.

## 1 Introduction

It is well known that the invention of public key cryptograpy by Diffie and Hellman in 1976 [1] not only revolutionized the field of cryptography, but also had a profound effect on the direction of research in computational number theory. Thus, it has be earning particular attention of cryptography experts and mathematician. The first usable public key system, introduced in 1978 [17], was the RSA cryptosystem, which is based on the problem of factoring large integers. RSA soon became the best known and most widely used public key cryptosystem. So far this system still has been used in many applied fields.

To set up RSA cryptosystem, each user $A$ (Alice) picks two large primes $p$ and $q$ (secret) and computes their product $N = pq$ (public). The group used is $G = Z_N^\star$, the multiplicative group of units in the integers modulo $N$. It is well known that the order of group $G$ is $\phi(N) = (p-1)(q-1)$, where $\phi$ denotes the Euler function. Pick a random integer $e$ such that $gcd(e, \phi(N)) = 1$ and compute $d$ such that $de = 1(mod\,\phi(N))$. $e$ and $d$ are said to be public key and private key respectivily.

Let $M$ denote the set of all possible plaintext messages, $C$ the set of all possible ciphertext messages (encrypted messages) and $K$ the set of all possible keys. Let encryption and decryption functions

$$E_{k_1} : M \to C \text{ and } D_{k_2} : C \to M$$