SPA on Rabin variant with public key $N=p2q$

ABSTRACT

Variants of the Rabin cryptosystem are built to overcome the decryption failure problem encountered by the cryptosystem. In this paper, we perform a theoretical simple power analysis on one of the variants that operates its decryption procedure via modular multiplication where the moduli $N1=pq$ is kept secret while the moduli $N=p2q$ is public. The attack utilizes Legendre's theorem of continued fraction to successfully retrieve the secret key of the cryptosystem. An example of the attack is also included in this paper.

Keyword: Simple power analysis; Rabin variant cryptosystem; Modular multiplication