Fast decryption method for a Rabin primitive-based cryptosystem

ABSTRACT

The Chinese Remainder Theorem (CRT) is an algorithm for solving linear congruence system into a unique representation and has been a useful tool in applications of cryptography. For real-world practicality, Garnerôs algorithm is efficient to speed up the CRT computation. Recently, a cryptosystem based on the Rabin primitive was designed which utilizing the CRT for its decryption routine. It seems that its current decryption algorithm is significantly slower than its encryption process. Hence faster decryption algorithms are sought-after. In this paper we design a fast and efficient algorithm for the decryption of the new cryptosystem based on the Rabin primitive. We then review and analyze the usefulness of the Garnerôs algorithm in our proposed method. Our results indicate that the asymptotic complexity of the proposed algorithm indeed reduced the computational cost of the decryption process. We also provide the empirical results on the running time using the single-precision multiplications measurement. The results prove that our design reduces the cost of the current algorithm by approximately 33.8%.

Keyword: Chinese remainder theorem; Garnerôs algorithm; Asymptotic complexity