Rabin-RZ: a new efficient method to overcome Rabin cryptosystem decryption failure problem

ABSTRACT

We propose a new efficient method to overcome the 4 to 1 decryption failure for the Rabin cryptosystem by reducing the phase space of plaintext from M Ůℤ to M Ů22n-2, 22n-1 ⊂ ℤpq, where pq is a product of 2 strong primes and pq Ů22n, 22n+2. Instead of utilizing the pubic modulus N = pq, we use N = p2q. Upon decrypting by using the private modulus d = pq via the Chinese Remainder Theorem, we prove that there exist only one plaintext from the 4 roots obtained that will reside within the interval 22n, 22n+2. As a result, the decryption failure is overcome and this technique also enhances the decryption process for the Rabin cryptosystem. Furthermore, we make analytical comparison with other methods designed in previous literature to overcome the Rabin cryptosystem problem.

Keyword: Integer factorization problem; Rabin cryptosystem; Rabin-Williams cryptosystem; Square root modulo