Design and analysis of Rabin-p Key Encapsulation Mechanism for CyberSecurity Malaysia MySEAL initiative

ABSTRACT

The modular square root problem has a special property of the having computational equivalent to a well-known hard mathematical problem namely integer factorization problem. The proposed Rabin-p Key Encapsulation Mechanism is built upon the said problem as its source of security, aiming for efficient and practical modular square root-based cryptosystem of which accompanied with the following properties; 1) improves the performance without plaintext padding mechanisms or sending extra bits during encryption and decryption processes, 2) the plaintext is uniquely decrypted without decryption failure, 3) improve decryption efficiency by using only one modular exponentiation, 4) a decryption key using only a single prime number, 5) sufficiently large plaintext space, 6) appropriate plaintext-ciphertext expansion ratio, 7) implementable on software and hardware with ease, and 8) achieves IND-CPA security

Keyword: Rabin-p cryptosystem; Key encapsulation; AKBA MySEAL; CyberSecurity Malaysia