A proposed CCA-secure encryption on an ElGamal variant

ABSTRACT

This paper proposes a variant of the ElGamal public key cryptosystem which is secure against chosen ciphertext attack. Our proof of security is based on the intractability of the Gap Hashed Diffie-Hellman assumption in the standard model. The proposed scheme is practical to encrypt short messages such as credit card information, PIN code etc. This scheme also preserves the computational performance of the hash ElGamal encryption scheme (i.e. its simplistic algebraic construction, less exponentiation cost).

Keyword: Chosen ciphertext security; ElGamal encryption scheme; Gap hashed Diffie-Hellman problem