World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:03, 2015

New Practical and Non-Malleable Elgamal Encryption for E-Voting Protoco

Authors : Karima Djebaili, Lamine Melkemi

Abstract : Elgamal encryption is a fundamental public-key encryption in cryptography, which is based on the difficulty of discrete logarithm problem and the Diffie-Hellman problem. Supposing the Diffie–Hellman problem is computationally infeasible then Elgamal is secure under a chosen plaintext attack, where security indicates it is difficult for the attacker, given the ciphertext, to restore the whole of the plaintext. However, although it is secure against chosen plaintext attack, Elgamal is absolutely malleable i.e. is not secure against an adaptive chosen ciphertext attack, where the attacker can recover the plaintext. We present a extension on Elgamal encryption which result in non-malleability against adaptive chosen plaintext attack using concatenation and a cryptographic hash function, our evidence utilizes the device of plaintext aware. The algorithm proposed can be used in cryptography voting protocol given its level security. Our protocol protects the confidentiality of voters because each voter encrypts their choice before casting their vote, offers public verifiability using a signing algorithm, the final result is correctly computed using homomorphic property, and works even in the presence of an adversary due to the propriety of non-malleability. Moreover, the protocol prevents some parties colluding to fix the vote results.

Keywords : Elgamal encryption, non-malleability, plaintext aware, e-voting
Conference Title : ICACNS 2015 : International Conference on Applied Cryptography and Network Security
Conference Location : Madrid, Spain
Conference Dates : March 26-27, 2015