ABSTRACT

SECURING ELLIPTIC CURVE BASED EL-GAMAL AGAINST POLLARD RHO ATTACK USING DIFFIE-HELLMAN KEY EXCHANGE

Tafta Zani

Supervisor : Ir. Ari Moesriami Barmawi, M.Sc., Ph.D.

Co-Supervisor : Maman Abdurrahman, S.T., M.T.

El-Gamal cryptosystem is one of many widely used public key cryptosystems especially for exchanging session key or encypting and decrypting small size message during secure communication. El-Gamal cryptosystem makes use of computational difficulty of solving discrete logarithm problem (DLP). A more advance technique is to use different form of DLP known as Elliptic Curve Discrete Logarithm Problem (ECDLP).

For breaking ECDLP, Pollard Rho method is currently the fastest attack. Pollard Rho cryptanalysis uses a random walk through the cyclic subgroup to find a collision and then using values at the collision point to create an equation to reveal the private key. In this study a hybrid of Elliptic Curve Diffie-Hellman Key Exchange (ECDHKE) and Elliptic Curve based El-Gamal (ECEG) is proposed as an attempt to make harder for Pollard Rho to gain information from the public key.

From the study it is concluded that the proposed method increases the strength of the cryptosystem by 100% when the Pollard Rho Attack success probability is 50%, but the strength decreases as the attack success probability increases. It is also known that the feasibility for implementing the proposed method for small message size is low. One disadvantage regarding public key variation is for each different communication party a new base point for ECEG is created, thus communicating parties must keep a list of pair containing the public key with the corresponding communication party.

Keywords: Security, Public Key Cryptography, Elliptic Curve Discrete Logarithm Problem, Elliptic Curve based El-Gamal, Elliptic Curve based Diffie-Hellman Key Exchange, Pollard Rho Attack