ABSTRACT

Global System for Mobile Communication (GSM) is standard of digital mobile cellular communication technology which introduced since 1991. As a standard of communication technology, GSM has own security system that is used to secure the entire network from outside party. The aims of this are to protect subscriber identity, signaling and user data. But from several researches, it was found that there are weaknesses on the system that allow to be penetrated.

To overcome those weaknesses, this final paper simulates the combination of Elliptic Curve Cryptography (ECC) method with A3, A8, and A5 algorithms on GSM security system services; authentication, TMSI assignment, and ciphering. This combination is applied on registration, roaming, and basic call setup procedures. Parameters which analyzed are security scheme, processing time, data rate, and avalanche effect testing to get the endurance of ECC method when it is combined with the system.

The result of this final paper shows that ECC method only can be applied on authentication and subscriber identity fidelity services. ECC method cannot be combined with ciphering service because of the different mechanism with A5 algorithm. The implementation of ECC method on the system adds processing time and data rate transmission on several paths. The addition of time still can be tolerated because it is belonging to the allocation time of the procedures.

From avalanche effect testing on IMSI, TMSI, SRES, RAND, and Kc, it is showed that ECC method has a maximal grade for one bit cipher text changing. The conclusion of it is ECC method has a great endurance to protect the GSM security system parameters in the transmission path.