บทคัดย่อ

วิทยานิพนธ์นี้ เสนอวิธีการเข้ารหัสข้อมูลแบบ ElGamal Elliptic Curve ขนาด 176 บิต ซึ่งเป็นการนำวิธีการเข้ารหัสข้อมูลแบบ ElGamal และระบบคณิตศาสตร์แบบ Elliptic Curve มาใช้งานร่วมกันเพื่อจำลองแบบสมาร์ทการ์ดที่พัฒนาบน FPGA เนื่องจากระบบคณิตศาสตร์แบบ Elliptic Curve นี้ ทำให้สามารถลดขนาดของ Public-Key โดยที่ระดับความปลอดภัยอยู่ในระดับที่สามารถใช้งานได้ เมื่อเทียบกับวิธีการของ RSA และ EDL ทั้งยังทำให้ขนาดของข้อมูลที่เข้ารหัสแล้วมีขนาดเป็น2 เท่า เมื่อเทียบกับวิธีการเข้ารหัสข้อมูลแบบ ElGamal Discrete Logarithm จึงทำให้ความจุข้อมูลบนสามาร์ทการ์ดเพิ่มมากขึ้น

This thesis proposes the implementation of a smart card with data encryption / decryption aspects. Data stored in the memory(flash ROM) is primarily encrypted/decrypted with and on-chip encrypter/decrypter. Encryption and decryption schemes are based on ElGamal Elliptic Curve Cryptography with the block length of 176 bits. This method is proved to be superior compared to RSA and ElGamal Discrete Algorithm in term of key size. The prototype was implemented using FPGA. The preliminary investigation confirmed that the designed is fully function as planed.