THE IMPROVEMENT ON DIGITAL SIGNATURE STANDARD

PANOMPORN SUVANNAPATTANA

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
(COMPUTER SCIENCE)

IN

FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
1996

ชื่อวิทยานิพนธ์ การปรับปรุงอัลกอริทึมมาตรฐานของลายเซ็นดิจิตอล

ผู้วิจัย พนมพร สุวรรณปัฐนะ

ปริญญา วิทยาศาสตรมหาบัณฑิต (คอมพิวเตอร์)

คณะกรรมการควบคุมวิทยานิพนธ์

ดำรัส วงศ์สว่าง Ph.D.

ศุภชัย ตั้งวงศ์ศานต์ Ph.D.

วันที่สำเร็จการศึกษา 10 เมษายน พ.ศ. 2539

บทคัดย่อ

ความปลอดภัยในการติดต่อสื่อสารด้วยระบบคอมพิวเตอร์เป็นสิ่งที่มีความสำคัญเป็นอย่างยิ่งต่อการสื่อสารในปัจจุบัน ความปลอดภัยดังกล่าวประกอบด้วยการรักษาข้อมูลของแต่ละบุคคลมิให้มีการเปิดเผยโดยผู้ที่ไม่มีสิทธิ การป้องกันมิให้ผู้หนึ่งผู้ใดทำการปลอมแปลงหรือ แสดงเป็นตัวแทนของผู้ส่งนั้น ๆ ได้ ซึ่งในระบบที่เราใช้กันตามปกติจะใช้ลายเซ็นที่เขียนด้วยมือเป็นการยืนยันถึงความเป็นของแท้ของเอกสารนั้นๆ

ลายเซ็นดิจิตอลเป็นการเข้ารหัสข้อมูลประเภทหนึ่งซึ่งมิได้มีวัตถุประสงค์เพื่อปกปิดข้อมูล แต่เพื่อใช้ในการ Authentication โดยจะมีการใช้กุญแจทำการเข้ารหัสข้อมูลเพื่อป้องกันการปลอมแปลงและเพื่อบ่งบอกการเป็นเจ้าของข้อมูลที่แท้จริง

ในปัจจุบันได้มีมาตรฐานของประเทศสหรัฐอเมริกากำหนดวิธีการในการสร้างลายเซ็นดิจิตอลและการตรวจสอบลายเซ็นดิจิตอล ซึ่งประกอบไปด้วยการประยุกต์ใช้ Modular and inverse computation และ Discrete logarithm ซึ่งจะมีความซับซ้อนในการคำนวณ ร่วมกับความยากในการทำ Prime factorization ของตัวเลขขนาดใหญ่ขนาด 512-1024 bits-binary เพื่อเป็นเครื่องประกันความปลอดภัยของข้อมูลหรือลายเซ็นต่อการถูกแก้ไขหรือปลอมแปลง ซึ่งทำให้การใช้งานมีความซับซ้อนยุ่งยากและเสียเวลามากขึ้นตามไปด้วย

งานวิทยานิพนธ์นี้จึงมีความคิดที่จะปรับปรุงหรือเปลี่ยนแปลงวิธีการดังกล่าวให้มีความง่ายในการใช้งาน โดยพัฒนาการสร้างลายเซ็นซึ่งไม่จำเป็นต้องมีการคำนวณ Modular inversion แต่ยังคงประสิทธิภาพในเรื่องของความแข็งแรงทนทานต่อการแก้ไขหรือปลอมแปลงเท่ากับประสิทธิภาพของลายเซ็นมาตรฐานที่มีอยู่

Thesis Title	The Improvement on Digital Signature Standard
Name	Panomporn Suvannapattana
Degree	Master of Science (Computer Science)
Thesis Supervisory Committee	
	Damras Wongsawang, Ph.D.
	Supachai Tangwongsan, Ph.D.
Date of Graduation	10 April B.E. 2539 (1996)

ABSTRACT

The Digital Signature is one of the cryptographic methods used for authentication. The two keys, public key and private key, are used for cipherment the original data. Currently, there is the standard document on the license of US government for the standard algorithm on the digital signature for signing and verifying processes. The algorithm consists of the modular and inverse modular computation that are very complex to implement. The difficulty of computation of discrete logarithm and the prime factorization of a large number are their strength enduring the attacking or forging the signature or the data.

The Digital Signature is used to detect unauthorized modifications of data and to authenticate the identification of the signatory. In addition to the recipient of signed data can use a digital signature in proving to a third party that the signature is really generated by the signatory. The Digital Signature Standard has two main algorithms, the Secure Hash Algorithm (SHA-1) and the Digital Signature Standard (DSS).

SHA-1 is required for use with the Digital Signature Algorithm (DSA) as specified in DSS. The SHA-1 is used by both the transmitter and intended receiver of a message in computing and verifying a digital signature. The SHA-1 lets the condensed message 160-bit long with the original message not longer than 2^{64} bits . The SHA-1 can be also used in others propose, for instance showing integrity of the data. It is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest.

The DSS is used to generate the signature and to verify the signature. There is much complexity in computation with the prime number, modular and modular inverse computation in the form of bits operation. This thesis proposes the idea to improve this standard algorithm to be ease of implementation in computation complexity, by eliminating the inverse modular computation and some modular equation. The DSS exploits the difficulties in computation of the discrete logarithm to prevent the user from being attacked and forged the data on the signature by eavesdropper/wiretapping. The new algorithm proposed by the author can meet this objective. Then the signer and verifier can perform the digital signature more efficiently. This thesis describes such an improvement both theoretically and experimentally.