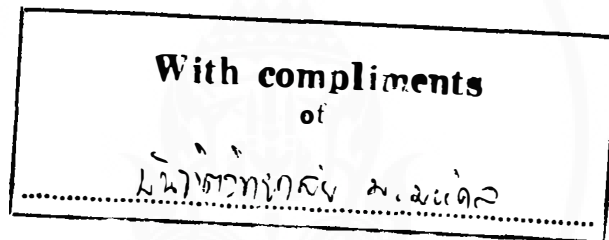




- 5 SEP 1996

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

Copyright by Mahidol University

TH
P1961
1996

36065

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.