ANALYSIS OF NUMBER THEORETIC TRANSFORMS BASED CRYPTOSYSTEM, GROUP SIGNATURES, e-VOTING AND A FACTORIZATION ALGORITHM

ABSTRACT

of the thesis

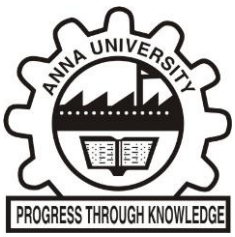
Submitted by

C. PORKODI

in fulfillment for the award of the degree

of

DOCTOR OF PHILOSOPHY



FACULTY OF SCIENCE AND HUMANITIES

ANNA UNIVERSITY CHENNAI

CHENNAI - 600 025

DECEMBER 2009

ABSTRACT

Information security is essential for today's world, because of the proliferation of computers and their ability to constitute the networks in the fields of energy, medicine, space, military, banking, transportation, etc. Messages exchanged over worldwide publicly accessible computer networks must be kept confidential and protected against manipulation. Cryptography provides solution to these problems.

Cryptography is the science of secret writing. It involves the study and applications of the principles and techniques, which are used to secure the data flow between computers, to digitize speech, and to encrypt facsimile messages. One of the major contributions of modern cryptography is the development of advanced protocols providing high-level cryptographic services, such as, secured user identification, voting schemes, and digital cash. The objective of the thesis is to analyze the cryptographic algorithms in, end to end communication and group oriented communications satisfying the security aspects and the cryptographic protocols in electronic voting.

There are numerous approaches to provide the cryptographic goals, confidentiality, authentication, data integrity and non-repudiation ranging from physical protection to mathematical algorithms. Cryptosystems are used to disguise the messages, before sending them in to the insecure communication channel. In **chapter 2,** a new public key cryptosystem based

on number theoretic transforms is developed. The key agreement is done using Diffie Hellman protocol. The security of the proposed cryptosystem is based on the computational hard problems integer factorization, discrete logarithm and Diffie Hellman problem. The proposed system has the advantage of high speed encryption and decryption rates, since it involves only two exponentiations. The proposed cryptosystem is applicable for end to end as well as group oriented communication. Numerical illustration is presented for the proposed cryptosystem.

In today's business scenario, messages are frequently addressed by a group of people and the responsibility of signing is to be shared among the group members. In such communication, the concept of threshold signatures and group signature schemes are introduced. In the overwhelming literature contributions, the secret and public keys are constructed based on a secret polynomial and the polynomial reconstruction problem is involved in generating the partial signatures. One of the focuses of this dissertation is to develop the group signature schemes without such complicated polynomial reconstruction problem.

In **chapter 3,** four group oriented signature schemes are developed based on primitive roots, elliptic curves, symmetric functions and Chinese remainder theorem. A section of group members sign a message with the assistance of a trusted authority. The trusted authority is responsible for constructing and transmitting private and public keys to the group members. He/she generates the group signature on behalf of the group, using the partial signatures of the group members and sends the signature along with the

message to the receiver. The proposed schemes are based on the computational hard problems integer factorization, discrete logarithm and elliptic curve discrete logarithm; and hence, they provide the same level of security as the existing schemes, but the partial signature generation and verification are complex free than the existing schemes. Hence, execution time is minimized. All proposed signature schemes are illustrated numerically.

Cryptographic protocols provide an environment for secure electronic elections over the internet, which is a speedy, economical, convenient voting process and appreciates many voters to vote from anywhere resulting in a great impact on the contemporary democratic societies. In **chapter 4,** single authority two way electronic voting scheme, multi authority two way electronic voting scheme and multi authority multi way voting scheme based on elliptic curves are developed. The two phases of electronic voting namely, voting phase and counting phase are analyzed. As the elliptic curve cryptosystem provide equivalent level of security with smaller keys compared to the cryptosystems based on modular exponentiation, the proposed voting schemes are efficient in cost wise and time wise. The designed voting schemes satisfy the basic requirements like privacy, universal verifiability and robustness of the electronic elections. The developed voting schemes are illustrated numerically.

The factorisation of large integers is a significant mathematical problem with practical applications to public-key cryptography. The security of the popular RSA, DSA hardware implementation depends on the

computational hard integer factorization problem. Factorization of large composite numbers is considered to be a part of cryptanalysis, since the progress in factoring tends to weaken the existing efficient public key cryptosystem. In **chapter 5,** a special purpose factorization algorithm based on recursion is developed. The proposed algorithm needs only very small memory space to hold the successive values as any computation analyst expects. It is a deterministic one and has less running time complexity compared to the existing popular algorithms: Lenstra's method and Quadratic sieve. The proposed algorithm is compared with the factorization techniques: Lenstra's method and Quadratic sieve theoretically and numerically.

Finally, in **chapter 6,** the major contribution of this research work is summarized and the possible directions for future work are also indicated.