ABSTRACT

Cryptography is the practice and study of hiding information. In modern times, cryptography is considered as a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. Cryptography is defined as the study of mathematical techniques related to aspects of information security. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce.

A digital signature is reminiscent of an ordinary signature. They have the characteristic that they are easy for a user to produce, but difficult for anyone else to forge. Digital signatures can also be permanently tied to the content of the message being signed. They cannot then be detached from one document to another and if any attempt is made then it will be detectable. The common reasons for applying a digital signature to communications are to ensure Authentication and to achieve Data integrity. That is if a message is digitally signed, any change in the message will invalidate the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions.

In secure network communication, algorithms are designed to resist plaintext attacks and their security is based on the difficulty of deducing the

secret key from the public key and difficulty of deducing the plaintext from the ciphertext. Public-key algorithms are most often based on the computational complexity of mathematically "hard" problems, often from number theory and abstract algebra. For example, the security of (Rivest Shamir Adleman) RSA algorithm is related to the hardness of integer factorization problem, while Diffie-Hellman and DSA are related to the hardness of Discrete Logarithm Problem (DLP). Most of the public-key algorithms involve operations such as modular multiplication and exponentiation because of the difficulty of the underlying problem. On the other hand, usages of these operations are much more computationally expensive than the techniques used in most of the symmetric key algorithms, especially with typical key sizes.

Elliptic Curve Cryptosystems (ECC) was proposed by Neal Koblitz and Victor Miller in 1985. The security of ECC is based on the discrete logarithm problem over the points on an elliptic curve. The hardness of elliptic curve cryptosystem is related to the elliptic curve discrete logarithm problem (ECDLP). The time required to crack the DLP grows “subexponentially” with the length of the key whereas the time required to crack the ECDLP grows “fully exponentially”.

The main objective of this research is to develop digital signature schemes based on various mathematical hard problems to obtain efficient and robust signature generation for intrinsic authentication applications like electronic voting, Health Care Insurance Claims, Contract Signing and Proprietary certificates. All the digital signature models is implemented using Java programming language and performance evaluation had been made. The

proposed digital signature schemes are theoretically developed and numerically justified.

A new type of digital signature scheme named as Proxy Blind Distributed Signature Scheme which is based on Discrete Log Problem (DLP) is proposed in Chapter 2. The signing delegation is distributed into a group of persons with a threshold version. This technique will overcome the problem of unavailability of the system in a proxy signature scheme. Furthermore, this distributed concept will increase the robustness of the signature scheme.

Another new type of digital signature scheme named as Identity Based Proxy Blind Distributed Signature Scheme is proposed in Chapter 3. The identity of a person plays a vital role in the verification process of a signed electronic document or message. In many real time applications like Automated Health Insurance Policies, the claims for the insurance holder need the identity of the person when the digitally signed bill was verified. Secondly by distributing the signing power to the group of servers will make the signing process more trusted while compared to delegation of signing power to a single person.

Chapter 4 addresses the Verifiable Encryption of Elliptic Curve Digital Signature. The protocol presented is an Adjudicated protocol, that is, the Trusted Third Party (TTP) takes part in the protocol only when there is a dispute. This scheme provides the solution to the *Fair Exchange Problem* that occurs in the Internet. This scheme can be used to build efficient fair exchanges and certified e-mail protocols. Chapter 5 concerns with the digital certificate based authentication scheme. A new simple scheme for theft-

protected proprietary certificate problem is presented by introducing a mobile phone as an additional requirement for the proprietor. Also this chapter presents the proprietary certification process using Elliptic Curve Discrete Log Problem (ECDLP) instead of Discrete Log Problem (DLP) for defining the relation R. Chapter 6 concerns about some applications of the proposed digital signature schemes in a polling station based automated electronic voting scheme and Health care insurance service management system.

The important features of the proposed schemes are highlighted. The major contribution of this research work is summarized and the possible directions for future work are also indicated.