# A STUDY ON CRYPTOGRAPHY FOR INTRINSIC AUTHENTICATION APPLICATIONS

Joshi Shraddha V.
M.E.(CSE) Department of Computer Science & Engineering
VidyaVikasPrathisthan Institute Of Engineering and technology, Solapur, India

Prof. Deshmukh S.P
Associate Professor in Department of Computer Science & Engineering
VidyaVikasPrathisthan Institute of Engineering and technology, Solapur, India.

## 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. 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. 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.

## INTRODUCTION

### ENCRYPTION AND SECRECY

The fundamental and classical task of cryptography is to provide confidentiality by encryption methods. The message to be transmitted can be some text, numerical data, an executable program or any other kind of information which is called the plaintext. Alice encrypts the plain text m and obtains the cipher text c. The cipher text c is transmitted to Bob. He then turns the cipher text back into the plaintext by decryption. To decrypt, Bob need some secret information. However, the encryption should guarantee secrecy and prevent anyone from deriving any information about the plaintext from the observed cipher text without the knowledge of the key. Providing confidentiality is not the only objective of cryptography. Cryptography is also used to provide solutions for other problems like Data Integrity: the receiver of a message should be able to check whether the message was modified during transmission, either accidentally or deliberately. No one should be able to substitute a false message for the original message, or parts of it. Encryption and decryption algorithms, cryptographic hash function are the basic building blocks for solving problems involving secrecy, authentication or data integrity. In many cases a single building block is not sufficient to solve the given problem, hence different primitives must be Combined. A series of steps must be executed to accomplish a given task. Such a well-defined series of steps is called a cryptographic protocol.

## RELATED WORK

### PROXY BLIND DISTRIBUTED DIGITAL SIGNATURE SCHEME

Digital signature scheme named as Proxy Blind Distributed Signature Scheme which is based on Discrete Log Problem (DLP). The need for Proxy Blind Distributed Digital Scheme arises whenever a person delegate his signing authority to the intended person, there is no guarantee that the proxy signer will be in the position to do the work (signing process). The proxy signing system may be engaged with some other work or the system may be corrupted due to some malicious programs at that time. In this case, if the system is modeled with proxy signature scheme, then the original signer cannot achieve his goal. Hence 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.

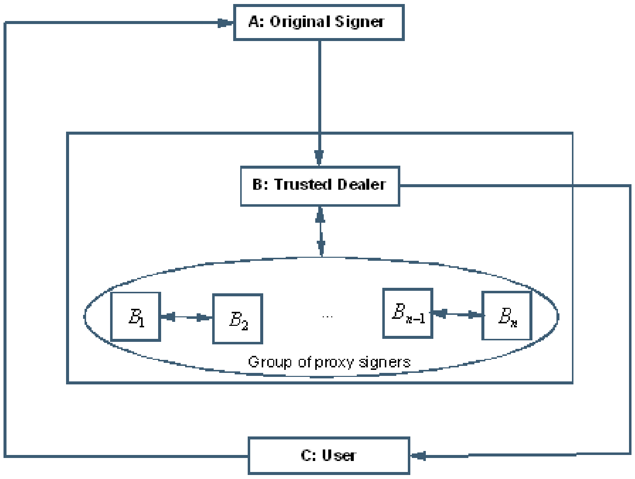

**Fig:- Proxy Blind Distributed Signature Scheme**

The participating entities in the digital signature scheme are the original signer A, a trusted dealer B, a group of proxy signer (servers) B1, B2…Bn and the user C. The user C request the original signer to blindly sign the given message m which in turn direct the signing process to the group of proxy servers. The group of proxy servers will generate a shared secret key and blindly sign the message m on behalf of A. The user C will verify the validity of the signature using the verification process.

## IDENTITY BASED

### PROXY BLIND DISTRIBUTED DIGITAL SIGNATURE SCHEME

In this system each user has a public key based on her or his identity, such as an email address. A central trusted authority assigns a corresponding private key to each user. In most public key systems, when Alice wants to send a message to Bob, she looks up Bob's public key. However, she needs some way to being sure that this key actually belongs to Bob, rather than someone such as Eve who is masquerading as Bob. In the present system, the authentication happens in the initial communication between Bob and the trusted authority. After that, Bob is the only one who has the information necessary to decrypt message that are encrypted using his public identity. In cryptography, if auxiliary information is included in the process then it allows the users to verify their shares as consistent. Verifiable secret sharing ensures that even if the dealer is malicious there is a well-defined secret that the users can later reconstruct. In a contract signing problem, there are two or more parties who are trying to agree on a contract. Each party will digitally sign the contract to signal their agreement. A variant of the contract signing problem is the return receipt problem or certified mail problem.

## WORKING

In an electronic voting scheme, the vote managing center commission a vote branch to act as a proxy signer. A voter can cast his/her vote in the vote branch. Since the vote branch does not know anything about the voting message during voting, the proxy blind signature scheme can be used in it. To achieve anonymity, blind signature scheme are normally used by e-voting schemes. Since a single vote manage center cannot blindly sign the vote messages from various branches, it can delegate its signing power to the proxy servers. Moreover, to achieve robustness the proxy delegation is distributed to the group of servers and a threshold number of servers lesser than the group members can generate the signature. Hence the proxy blind distributed signature scheme can be used to this electronic voting scenario.

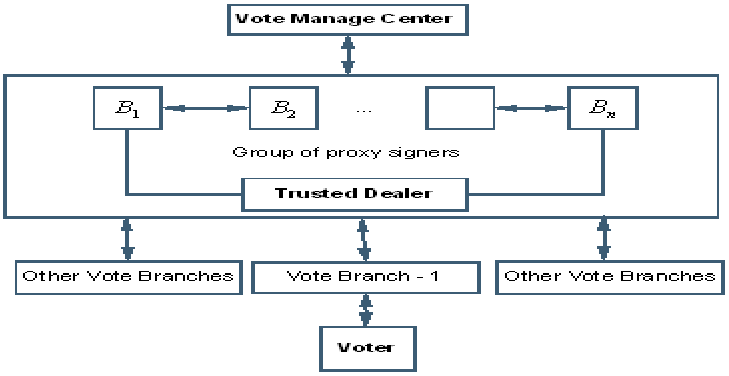

**Fig: - Proxy Blind Distributed Signature Scheme Use In Polling Station Based Internet Voting Scheme**

## APPLICATION TO HEALTH CARE INSURANCE SERVICE MANAGEMENT SYSTEM

A health insurance claim is a bill for health care services that the health care provider turns in to the insurance company for payment. Information security plays a vital role in the Health Care Insurance claim module due to the following fraudulent activities. There is a possibility for a person who does not have a valid insurance card to use someone's card. A dishonest hospital may give a forged receipt to an insurance card holder stating that medical treatment was given to that person who has not undergone any treatment. In these two fraudulent activities, the first one lacks the Identity of the Insurance card holder and the second lacks decentralization of signing power.

## CONCLUSION

Web technologies have revolutionized the delivery of information and services, providing commercial and noncommercial functions through the web demanding high level of authentication. This research work is concerned with a study on cryptography and provides new idea to build digital signature schemes and digital certification process for solving some of the existing problems in authentications. Signatures alone will not solve some specific problems like contract problem, certified electronic mail, etc. instead; the right approach is to use cryptographic tools to build protocols. That is explicitly specified processes are required for solving such problems.

## REFERENCES

[1].Adi Shamir (1979), '*How to share a secret*', *Communications of the ACM, Vol. 22 p612-613.*

[2] Adi Shamir (1984), '*Identity-Based Cryptosystems and Signature Schemes*', *Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science, pp. 47-53.*

[3] Asokan N., Shoup V. and Waidner M. (1998), '*Asynchronous protocols for optimistic fair exchange*', *In Proceedings of the IEEE Symposium on Research in Security and Privacy, 86-99.*

[4] Asokan N., Shoup V. and Waidner M. (2000), '*Optimistic fair exchange of digital signatures*', *IEEE Journal on Selected Area in Communications, pp. 45-56.*

[5] Avi Rubin (2004), '*Security consideration of remote e-voting over internet Technical Report*

[6] Bao F., Deng R.H. and Mao W. (1998), '*Efficient and Practical Fair Exchange Protocols with Off-line TTP*', *In IEEE Symposium on Security and Privacy, pp. 124-132.*

[7] Bellare M. and Michali S. (1988), '*How to sign given any trapdoor function*', *Proceeding of 20th STOC-ACM, pp. 32-42.*

[8] Ben-Or M., Goldreich O., Micali S. and Rivest R. (1990), ‘*A fair protocol for signing contracts’, IEEE Transactions on Information Theory, Vol. 36, No. 1, pp. 40-46.*

[9] Biehl I., Buchmann J.A., Meyer B., Thiel C. and Thiel C. (1994), ‘*Tools for proving zero knowledge’, Advances in Cryptology - EuroCrypt-94, pp. 356-365.*