AN RESULT ORIENTATION IN DIGITAL SIGNATURE TECHNOLOGY

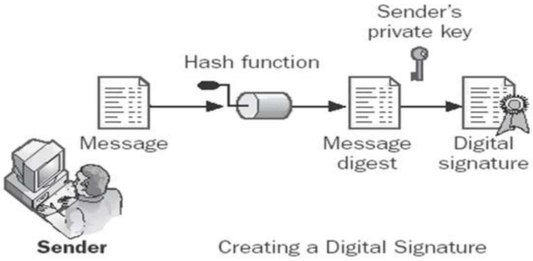
Parul[1], Anjali Namdev[2]
[1]PG Student, [2]Assistant Professor, CSE Department, S(PG)ITM Rewari, Haryana, India

I. INTRODUCTION

Generally, in order to authenticate and verify the validity of transactions, a handwritten signature with or without an official or personal seal is used for signing a document or a convention between two countries in political, military or diplomatic activities, signing a contract or an agreement between two common companies or persons in commercial activities, or depositing money in or withdrawing money from a bank or making bank transferring. As a result of the technical development and the demand of the information-based society, people want to sign documents, contracts or agreements remotely and quickly via the internet, thus digital signature was born in cryptology, especially on the basis of the fast development of public-key cryptology. As an important safety technique, digital signature plays a significant role in guaranteeing the integrality, privacy, and non-repudiation of data. With the technology of digital signature, people can realize contract or agreement signing, commodities purchase, bank transferring and information release and so on remotely within their doors, furthermore, the authorized persons can verify the authenticity and validity conveniently, thus to save time and resources effectively. Moreover, with the help of advanced technologies, the copying function which is impossible to be achieved in computation is realized.

Digital Signature

A digital signature verifies the authenticity of an electronic document or digital message. Digital signatures are commonly used to identify electronic entities for online transactions. A valid digital signature gives a user reason to believe that the message was created by a known legitimate sender, such that the sender cannot deny having sent the message and that the message was not altered in transit. A digital signature uniquely identifies the originator of digitally signed data and also ensures the integrity of the signed data against tampering or corruption. Digital signatures are commonly used for software distribution, Authenticate online entities, Verify the origin of digital data. Ensure the integrity of digital data against tampering, financial transactions, and in other cases where it is important to detect forgery attack. A digital signature procedure is shown in Figure



Authentication

A message source is authenticate by digital signature. A valid signature shows that the message was sent by that user, where user is the requester. Authenticity in digital signature means that the message or the user is valid.

Non-repudiation

Non-repudiation is an important feature of digital signature. By this property, an entity that has signed some information cannot at a later time deny having signed it.

Attacks on Digital Signature

This section describes attack on digital signature. Key-Only attack, Known message attack and Chosen-Message attack are some attacks on DS. If the attack is successful, the result is a forgery. We can have two types of forgery.

Forgery

In a cryptographic digital signature system, digital signature forgery is the ability to create a pair consisting of a message and a signature that is valid for message, and message has not been signed by the legitimate signer . Existential and Selective are the two types of forgery.

Existential Forgery

In an existential forgery the attacker is able to create a valid signature-message pair, but the attacker cannot use this pair really. This type of forgery is probable, but the attacker cannot benefit from it.

Selective Forgery

In the selective forgery, the attacker is able to forge signers signature on a message. The attacker gets benefit from this forge unlike existential forgery. The probability of such forge is low .

Basic Digital Signature

Basic digital signature is an extension of digital signature in which a message is signed by a signer without knowing the content of the message. Basic digital signature was first introduced by David Chaum in 1983. It allows a person to get a message signed by another party without revealing any information about the message to the other party].

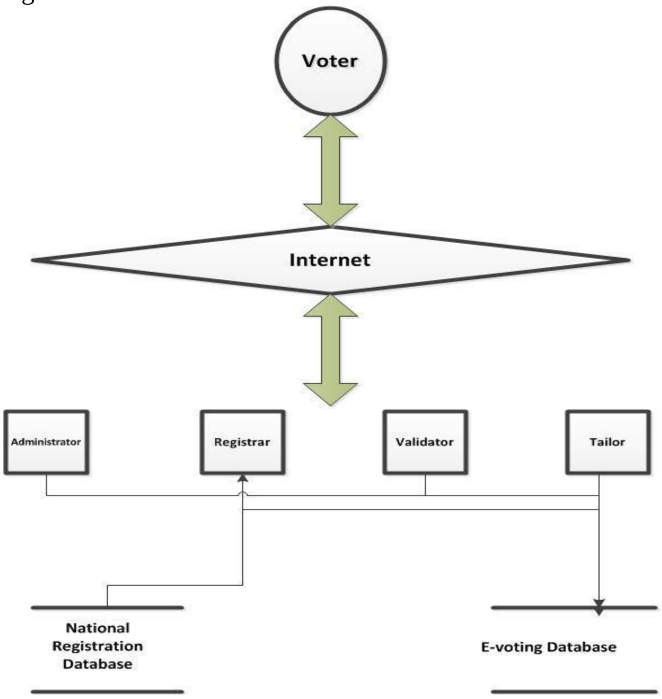
Sometimes we have a document that need to get signed without revealing the con-tents of the document to the signer. For example, a scientist, say Bob, might have discovered a very important theory that need to be signed by a public, say Alice, without allowing Alice to know the content of the document. Basic digital signature protocol for this purpose works as follows.

Scope of the Work

Our scheme can be applicable in real life scenario, where digital document need to be signed without disclosing its content. It is very useful for the application, where security is the prime necessity such as e-cash, e-voting, e-commerce. The proposed scheme has a wide range of scope in confidential transactions].

E-voting

Basic digital signature is the most popular cryptographic technique in EVS by providing Confidentiality of the voters vote. The signature is used to authenticate the voter without disclosing the content of a vote. The authority is not able to know whom a voter votes]. In E-Voting, a vote is blinded in order to achieve its Confidentiality. To ensure the secrecy of the voters vote, a voter casts a ballot, blinds a vote using a random number and sends it to the valuator. The valuator then signs the blinded vote after verifying the voter. After receiving the validated ballot, the voter un-blinds the ballot, to get the true signature, of the valuator for the vote see Figure



Electronic voting (also known as e-voting) is voting using electronic means to either aid or take care of the chores of casting and counting votes. Depending on the particular implementation, e-voting may encompass a range of Internet services, from basic to full-function online voting through common connectable household devices. Similarly, the degree of automation may vary from simple chores to a complete solution that includes voter registration & authentication, vote input, local or precinct tallying, vote data encryption and transmission to servers, vote consolidation and tabulation, and election administration. A worthy e-voting system must perform most of these tasks while complying with a set of standards established by regulatory bodies, and must also be capable to deal successfully with strong requirements associated with security, accuracy, integrity swiftness, privacy, auditability, accessibility, cost-effectiveness, scalability and ecological sustainability.

Electronic voting technology can include punched cards, optical scan voting systems and specialized voting kiosks (including self-contained direct-recording electronic voting systems, or DRE). It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet.

In general, two main types of e-Voting can be identified:

- e-voting which is physically supervised by representatives of governmental or independent electoral authorities (e.g. electronic voting machines located at polling stations);
- remote e-voting via the internet (also called i-voting) where the voter votes at home or without going to a polling station.

Many insecurities have been found in commercial voting machines, such as using a default administration password. Cases have also been reported of machines making unpredictable, inconsistent errors. Key issues with electronic voting are therefore the openness of a system to public examination from outside experts, the creation of an authenticatable paper record of votes cast and a chain of custody for records.

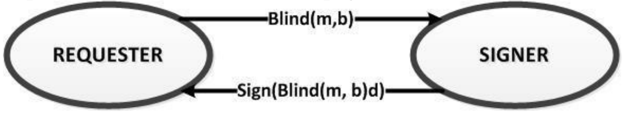
Electronic voting technology can speed the counting of ballots, reduce the cost of paying staff to count votes manually and can provide improved accessibility for disabled voters. However, there has been contention, especially in the United States, that electronic voting, especially DRE voting, could facilitate electoral fraud and may not be fully auditable. In addition, electronic voting has been criticized as unnecessary and expensive to introduce. Several countries have cancelled e-voting systems or decided against a large-scale rollout, notably the Netherlands and the United Kingdom

E-Cash

Setup Phase: The legitimate authority generates a public/private key pair for a signature scheme. This key pair is used for verification of the details of the scheme and the bank's other public keys. The public key is widely published]. The bank generates a public/private key pair for a public-key encryption scheme. The association which represents the top German financial interest groups. Usually paired with a Transaction account or Current Account, cards with an Electronic Cash logo are only handed out by proper credit institutions. An electronic card payment is generally made by the card owner entering their PIN (Personal Identification Number) at a so-called EFT-POS-terminal (Electronic-Funds-Transfer-Terminal). The name “EC” originally comes from the unified European checking system Eurocheque. Comparable debit card systems are Maestro and Visa Electron. Banks and credit institutions who issue these cards often pair EC debit cards with Maestro functionality

The public key is widely published in a certificate signed using the legitimate authority's private key. The legitimate authority generates a series of public/private key pairs for the basic digital signature scheme for each denomination of coin. These are widely published in certificates signed using the legitimate authority's private key

Withdrawal Phase: The user prepares a coin, which is blank. This contains information, in a predefined agreed format, for the identity of the bank, the de-nomination of the coin and a randomly chosen serial number. The user undertakes the basic digital signature protocol on the blank. The user also supply details of what denomination the coin should have and make payment for the coin. The private key is used to generate basic digital signature for denomination indicated by the user. The coin have a blank and the signature on the blank. Deposit-spend Phase: The user encrypts the coin (blank and the signature) using the bank's public encryption key. The merchant received the cipher text. The bank received the encrypted coin from the merchant. The bank decrypts it and recovers the coin. The bank now ensures that the signature verifies using the public key spec certificates i e by the denomination of the coin by the blank. If not, the bank rejects the coin and informs the merchant about this. Otherwise the bank checks to see if the serial number of the coin exists. If so, the bank rejects the coin and the merchant is informed about this. If the serial number isn't valid, then the serial number is added to the database and coin got accepted. The merchant receive payment for coin.



Bob creates a message and blinds it. Bob sends the blinded message to Alice

Alice signs the blinded message and send the signature on the blinded message

Bob unblinds the signature to obtain a signature on the original message.

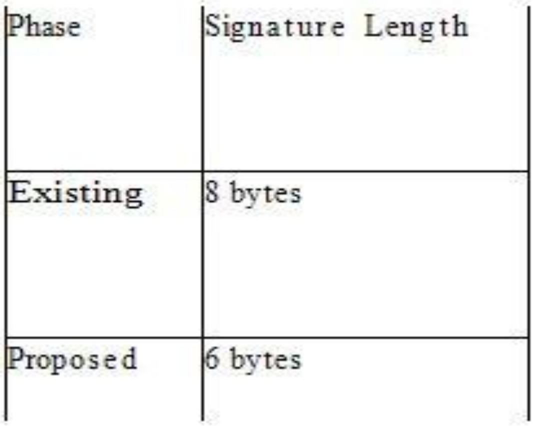
Basic security features of a standard basic digital signature are un-linkability, blindness and non-repudiation .Lets see a block diagram of basic digital signature protocol see Figure . It consist of two participants a requester and a signer where, requester wants signer to sign a message m .Requester blind the message m with some basic digital phase factor b. Signer sign the blind message, where d is signers private key. Requester un-blind the message and get the sign(m , d) which is signers signature on m.

The random oracle model is very efficient cryptographic solution for a large number of problems (digital encryption and signature, identification protocols etc.). However, security proofs in this model are not sound with respect to the standard model: there exist constructions of various cryptographic schemes provably secure in the random oracle model, but for which no instantiation of the random oracle yields a secure scheme in the standard model. As a consequence, a central line of research in modern cryptography is designing efficient schemes provably secure in the standard model. Basic digital signature(BS) was introduced by Chaum to protect the right of an individual's privacy. Since Chaum's first basic digital signature scheme was proposed, many basic digital signature schemes have been proposed, where have been proven secure in the random oracle and are secure in the standard model. Concurrency in the context of blind signatures was put forth by Juels et al. who presented the first security model for blind signatures that takes into account that the adversary may launch many concurrent sessions of the blind signing protocol. Concurrency is particularly important since in implementations of blind signatures in e-voting.

II. RESULT

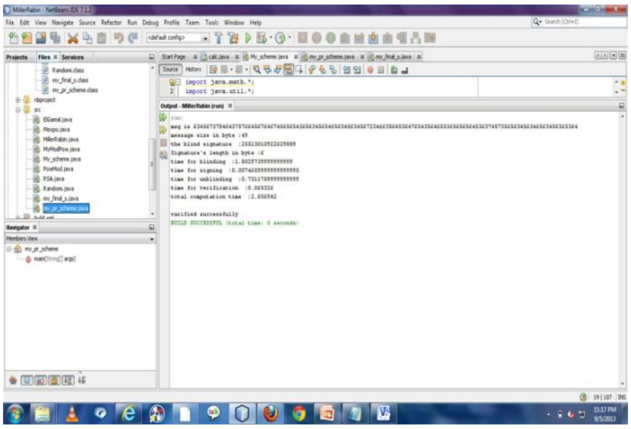
Phases	Existing scheme	Proposed Scheme
Basic digital phase	75.93ms	1.702 ms
Signing	0.422 ms	0.007 ms
Un-basic digital phase	0.083 ms	0.721 ms
Verification	0.161 ms	0.055 ms
Total computational time	72.557 ms	3.606 ms

Table : Comparison of Computational Overhead



Phase	Signature Length
Existing	8 bytes
Proposed	6 bytes

Copyright 2017.All rights reserved.



```
import java.math.*;
import java.util.*;
```

```
run:
msg is 4345673784643757664567646745656543656345654656345634567234663564536476543564655365656564536374573565634563465634563656364
message size in byte :45
the blind signature  :25513010922829889
Signature's length in byte :6
time for blinding  :1.8029739999999999
time for signing  :0.0074659999999999951
time for unblinding  :0.7311789999999999
time for verification  :0.065326
total computation time  :2.606942

verified successfully
BUILD SUCCESSFUL (total time: 0 seconds)
```

III. CONCLUSION

The proposed BS scheme is based upon the hard computation assumption such as DLP and IFP [Chapter 4]. The proposed scheme is implemented in Java. It is also analyzed and verified successfully]. Proposed scheme is compared with the existing scheme and found that the computation overhead and signature length is lesser for proposed scheme than the existing scheme. The proposed scheme can have wide range of application in areas such as e-cash, e-voting, e-commerce [Chapter 3]. It ensures to be more secure than existing scheme. The proposed scheme ensure, very ability, non-repudiation, identify ability.