UGC JOURNAL NUMBER 44557

**International Journal of Allied Practice, Research and Review**

**Website: www.ijaprr.com (ISSN 2350-1294)**

# Comparison between Various Signature Schemes

**Sarvesh Tanwar and Anil Kumar**
**[1]Departement of Computer Science & Engineering, Mody University of Science & Technology, Laxmangarh, Sikar, Rajasthan, India**
**[2]Department of Computer Science & Engineering, Mody University of Science & Technology, Laxmangarh, Sikar, Rajasthan, India**

**Abstract - Digital signature guarantees that the document was not modified in route and no one else can read the document. Signatures are bind in digital certificate. Certification authorities (CAs) are responsible for generation, issuing, verification and revocation of certificates. They can be independent third parties or organizations running their own certificate issuing server software. Trust in certificate is achieved by adopting Public Key Infrastructure (PKI) to rely on CAs to establish a valid certificate chains to form certificate paths. A CA is a single point of failure in PKI system. A compromised CA break the entire infrastructure. In this paper we do comparison between the Digital Signature schemes. As digital signature is the heart of the public key infrastructure.**

**Keywords - *Digital Signature, Certificate, Certification authority, PKI***

## I. Digital Signature

The most important cryptographic operation in PKI is the digital signature. Digital signature serves to verify that signer of the document has created and signed that document and that document has not been tampered with [8]. It is used for non-repudiation, authentication and data integrity, generated using public key cryptography. If two parties are exchanging some digital document, it may be important to protect that data so that the recipient knows that the document has not been altered since it was sent and that document received was indeed created by the sender.

Digital signatures guarantees the following information security properties [4][5]:-

**Authenticity:**

The importance of authentication, verifying the identity of users and machines becomes crucial when an organization opens its doors to the Internet. Strong authentication mechanisms ensure that persons and machines are the entities they claim to be.

**Integrity:** PKI provides integrity through digital signatures, which can be used to prove that data has not been tampered or altered within transit.

**Non-repudiation:** Non-repudiation provides a proof-of-participation in an action or transaction by establishing that a user's private key was used to digitally sign an electronic business transaction [9]. PKI can be used to provide non-repudiation through digital signatures. This proves that a specific user perform the particular task at a given time.

**Credibility:** Receiver can verify the received signature is indeed a legitimate signer has signed that.

**Enforceability:** Digital signature generation process is a trained reflex which is not subject to conscious muscular control. That's why it's hard to forge. Only sender can generate and sign his own signature as he knows his private key.

**Non-reusable:** Digital Signature is a function of the file and cannot be converted into another file [5].Digital signature is not reusable. Other persons cannot cut and paste the signature to other documents [7].

**Unalterable:** The signed documents are unalterable. The signature, on a document guarantee the origin and integrity of the document that bears signature [7].

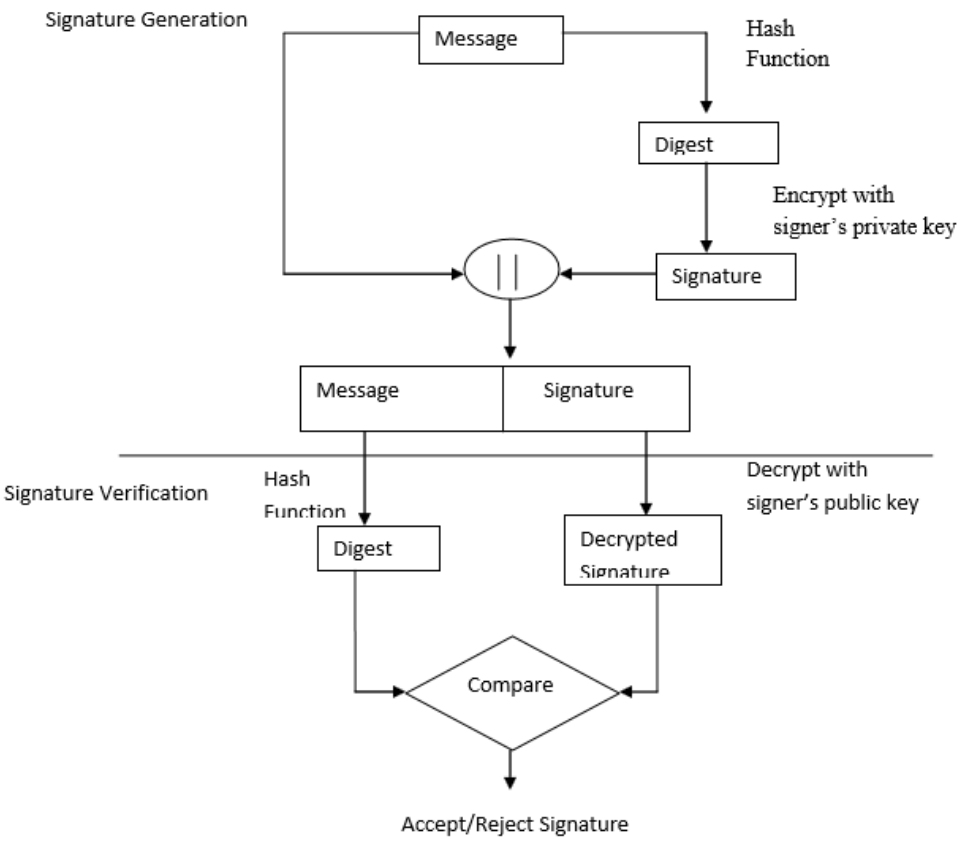


**Figure 1: Generation and Verification of Digital Signature**

The rest of the paper is organized in the following sections: Literature review is explained in section 2. Section 3 explained various signature schemes such as blind signature, batch and multiple signatures. Section 4 describes the comparison between various signature schemes following by conclusion in section 5.

## II. Literature review

Section 2 describes various schemes proposed by researchers.

**Negi, Arvind, et. al [4].** Proposed digital signature algorithm which is based on factoring the product of two large prime numbers and discrete algorithms problem. This technique used multiple public key exponents which in turn provide multiple public and private key. The proposed scheme also improved the security by using multiple integers($e_1$,$e_2$…$e_n$) to primary integer number and increasing difficulty of decryption key. The limitation of this scheme is that it do not allow to store digital signature certificates.

**Nia et. al. [3]** compared different types of digital signature schemes based on security level, efficiency and complexity. He explained different type of digital signature schemes and procedures such as batch scheme, forward secure scheme, blind scheme and proxy scheme.

**Tianhuanget. al**. focused on DSA digital signature technology in ecommerce security issues and proposed algorithm for the improvement of DSA. They simulate signatures to solve ecommerce security issues. They said digital signature technology needs further improvement and efforts to improve security of it.

**Wang et. al [2]** proposed concept of multiple signature. They said a single compromised CA break the entire PKI infrastructure and compromised CA can issue bogus certificate for any domains without the consent of the domain owners. Bogus certificate have been used in MITM attacks. They proposed multiple signature approach on a server's certificate as the probability of breaking multiple CAs in a short period of time is reduced significantly. They modify the current X.509 V3 certificate to impose multiple signatures.

**Subramanya et al. [6]** explained the digital signature generation and verification process. They compared conventional and digital signature characteristics. They explained two basic categories of digital signature: direct and arbitrated. The direct digital signature involved two parties- sender and the receiver. There is trusted third party in a Arbitrated signature scheme. Every signed message from sender to receiver go through arbiter. They only compare the existing methods but do not propose any new method.

## III. Various Digital signature Schemes

In the last decade, organizations have been trying to move from a paper-intensive environment to a paper-free environment where the security of information is one of the primary issues and any vulnerability in this regards can have devastating effects. Security means the protection of the information from any sort of unauthorized access or manipulation through eavesdropping or mathematical or probabilistic algorithms and other methods. The most important security services are confidentiality, integrity, authentication, and non-repudiation. When designing a communication system, the security services of this system must be defined. These security services can be achieved using digital signatures. There are various forms of signatures such as batch signature, blind signature and multiple signatures.

### 3.1 Batch Signature Scheme

Batch authentication can be used to improve the performance of broadcast authentication [10]. Packets are authenticated in batch which uses batch signature to authenticate the batch. Batch signature supports the authentication of any number of packets simultaneously with one signature verification, to address the efficiency and packet loss problems in general environments. When receiver does not verify each and every packet, by doing this it reduces the verification computation, it verifies the received packets in batch. In Batch Signature sender signs each packet and transmit it to multiple receivers. The receiver must assure that packets are sends by the intended sender and sender can't deny for the signature by verifying corresponding signatures.

**Signing Process**

```
Byte b[] hash_to_computer=temp_msg.getBytes();
MD md= new MD();
BigInteger hash=md.cal_md(hash_to_computer);
BigInteger s=BigInteger.One;
S=((r.multiply(k)).subtract(hash.multiply(x))).mod(q)
```

**Veryfying Process**

```
Mul_r=mul_r.multiply(t1);
For(i=0;i<bfsize;i++)
{
T1=r[i].modInverse(q);
T2=hash[i];
T4=t2.multiply(t1);
U1=u1.add(t4);
T3=s[i];
T5=t3.multiply(t1);
U2=u2.add(t5);
}
V=((g.modPow(u2,p).multiply(y.modPow(u1,p))).mod(p)).mod(q
); If(v==mul_r)
```

### 3.2 Blind Scheme

For achieving anonymity many cryptographic encryptions has to be done, one best solution is to use blind signature.
Blind signature is defined as the signer signs the message without knowing what he is actually signs.

By using partial blind signature schemes customer should be anonymous to merchant. The blind signature scheme not only retains the properties of traditional digital signatures but also supports the properties:

1. The message content is blind to the signer
2. The message may not be traced by the signer after the signature is revealed.

Many other characteristics also provided by their protocol like merchant, bank and customer cannot deny that they do not send this message by using digital signature approach. Their protocol could be easily implemented with XML and other SSL security channel.

In our protocol anonymity is obtained by applying blind signature concept. Basically blind signature is used to get sign the message by signer without actually knowing what he is signing. Customer also gets blinded sign on actual e-cash coin so that bank will not get to link e-cash to customer.

For achieving anonymity many cryptographic encryptions has to be done, one best solution is to use blind signature.
Blind signature is defined as the signer signs the message without knowing what he is actually signs.

**Blind Signature Generation**

$$BigInteger\ b\ =\ ((r.modPow(e,n)).multiply(m)).mod(n);$$
$$BigIntegerbs\ =\ b.modPow(d,n);$$

**Blind Signature Verification**

$$BigInteger\ check\ =\ s.modPow(e,n);$$
$$System.out.println(m.equals(check));$$

### 3.3 Multiple Signatures

In 1983 Itakura and Nakamura introduced the concept of multiple signatures [7]. Multiple signatures allow multiple signers to sign and authenticate a message using a single compact signature [R. Duran]. In multiple signature n random secret keys $k_1$, $k_2$, $k_n$ and public key t is generated such that:

$$(k_1 + k_2 + .. k_n) * t = 1\ mod\ \emptyset(n)$$

- Each signor takes the message M and signs it by

$$S_i = M^{k_i}\ mod\ n$$

- N signed are then multiplied by CA/PKG to form Signature S

$$S = S_1 * S_2 * S_n\ mod\ n$$

- This Signature S is sent to the recipient. The recipient can verify the signature using t

$$S^t\ mod\ n = (S_1 * S_2 * .. * S_n)^t mod\ n$$
$$= M^{[k_1+k_2+..k_n]*t}\ \ mod\ n$$
$$= M$$

- Original message can be verified by any member by using the public key t.

#### 3.3.1 Types of Multiple Signatures [11]

**1. Sequential Multiple Signature**

In this scheme, the first signer signs the contents and the second signer signs on the content and the first signer's signature. The form is considered signed when all signers sign the form and last signature is appended on it. It can be distinguished as follows:-

- Independent sequential Multiple Signature

In this scheme sequence of signing is not important; the signer only signs the content.

- Dependent Sequential Multiple Signature

In this scheme sequence is important. The last signer signs on the content and signature of the form.

$$S_1 = C^{pr}\ mod\ n$$

$$S_2 = S_1^{ps}\ mod\ n$$

### 2. Parallel Multiple Signature

In this scheme, the signer signs on the content of the form but not on the signature of other signers

## IV. Comparison

Digital signature schemes are compared in terms of security, verification, efficiency and difficulty level.

### 4.1 Security

- Batch signatures are strong but in several conditions can make mistake to verify signature [3].

- Blind signature's security depends on blindness and enforceability. It can be good as well as harmful if attacker signs the message. Because attacker's identity cannot be verified.

- Multiple signatures are very strong as message is signed by multiple signers. If any of the signer is compromised he is not able to issue the certificate.

### 4.2 Efficiency

As shown in the table 1 all the three schemes are efficient. Efficiency of the algorithms depends on the security of network, verification process and applications of the schemes. In case of e-cash blind signatures are efficient where anonymity is required.

### 4.3 Verification

Verification shows how receiver verifies the signature. Multiple signature verification increase overhead.

Complexity of signature verification is O ($L^S$) where L is path length and S is number of signature.

### 4.4 Difficulty

Difficulty is one of the parameter for implementation by the programmer of these signatures. Programmers choose platform and technique according to their programming skills [3].

**Table 1: Comparison between digital signature schemes**

| Bases | Batch | Blind | Multiple Signature |
|---|---|---|---|
| **Security** | Middle | Strong | Very Strong |
| **Efficiency** | Average | Very efficient | Very Efficient |
| **Verification** | Middle | Good | Good |
| **Difficulty** | Low | Middle | Average |

## V. Conclusion

Finally we come to the conclusion that multiple Signatures approach is more secure than the single CA signature. If any of the CA is compromised whether its database or key will not be able to issue certificate to any server as multiple signatures are required. This resolved the single point of failure in PKI.

## VI. References

**[1.] De la Hoz, Enrique, et al. "Detecting and defeating advanced man-in-the-middle attacks against TLS."** ***2014 6th International Conference On Cyber Conflict (CyCon 2014)*****. 2014.**

**[2.] Wang, Xinli, Yan Bai, and Lihui Hu. "Certification with Multiple Signatures."** ***Proceedings of the 4th Annual ACM Conference on Research in Information Technology*****. ACM, 2015.**

**[3.] Nia, Mehran Alidoost, Ali Sajedi, and AryoJamshidpey. "An Introduction to Digital Signature Schemes."** ***arXiv preprint arXiv:1404.2820*** **(2014).**

**[4.] Negi, Arvind, et al. "New Method for Obtaining Digital Signature Certificate using Proposed RSA Algorithm."** ***International Journal of Computer Applications*** **121.23 (2015).**

**[5.] Tianhuang, Chen, and Xu Xiaoguang. "Digital signature in the application of e-commerce security."** ***E-Health Networking, Digital Ecosystems and Technologies (EDT), 2010 International Conference on*****. Vol. 1. IEEE, 2010.**

**[6.] Subramanya, S. R., and Byung K. Yi. "Digital signatures."** ***Potentials, IEEE*** **25.2 (2006): 5-8.**

**[7.] Zhou, Jianying, and Robert Deng. "On the validity of digital signatures."** ***ACM SIGCOMM Computer Communication Review*** **30.2 (2000): 29-34.**

**[8.] Henry, David. "Who's got the key?."** ***Proceedings of the 27th annual ACM SIGUCCS conference on User services: Mile high expectations*****. ACM, 1999, pp-101-110.**

**[9.] Wang, Xinli, Yan Bai, and Lihui Hu. "Domain based certification and revocation." Proceedings of the 2015 International Conference on Security and Management, SAM. Vol. 15. 2015.**

**[10.] Rajarajan, K., T. M. Thiyagu, and S. Chandrasekar. "Multicast Authentication Based on Batch DSA." International Journal of Engineering Research and Technology. Vol. 2. No. 4 (April-2013). ESRSA Publications, 2013.**

**[11.] Moussa, ChaficMarounRouhana. "Digital Signature and Multiple Signature: Different Cases for Different Purposes." GSEC Practical Assignment, Version 1** (2003).