An Enhanced Digital Signature Scheme

Seetha. R
School of Information Technology and Engineering, Vellore Institute of Technology,
Vellore, Tamilnadu, India.
Orcid Id: 0000-0003-1954-0982

Abstract

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message and intended to solve the problem of tampering and impersonation in digital transactions. Basically a digital signature is a public key cryptographic technique. Using the concept of public key cryptography and discrete logarithmic problem this paper proposes a digital signature scheme preserving the properties of digital signature algorithm.

Keywords: Digital Signature, Private Key, Public key, Authenticity, Integrity.

INTRODUCTION

In the current digital world, various documents are signed digitally in place of traditional pen-and-ink signatures. Digital signature uses asymmetric cryptography and provides validation and security to messages transmitted over an insecure medium. Because a digital signature is just a string of 0's and 1's, it differs from an analog signature (ink signature) in two important ways: (1) No matter how complicated an analog signature is, a forger intent on committing fraud will eventually be able to duplicate it. A digital signature, on the other hand, should by definition be inimitable. (2) A person's analog signature is constant; it is the same on all documents signed by that person. By contrast, digital signatures must be different for every message. A digital signature scheme has three phases, namely, key generation phase, Signing phase and Verifying phase. In key generation phase, a pair of private, public key is generated. In signing phase, the signature is generated using private key and other parameters and thus the signature generated is used for signing the document to be sent. In verifying phase, the receiver validates the signature and accepts or rejects it accordingly. Basically a digital signature is depicted as given in Figure 1.

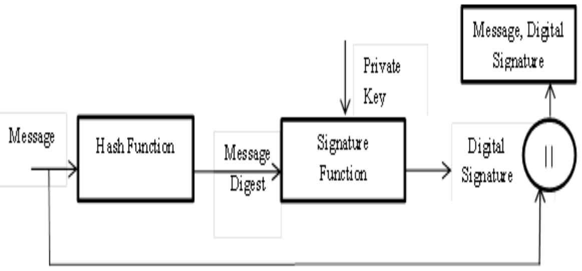

Figure 1: Digital Signature Scheme

Digital signature schemes are usually classified into one of two categories: true signatures or arbitrated signatures. In a true signature scheme, signed messages produced by the sender S are transmitted directly to the receiver R, who verifiestheir validity and authenticity. A dispute arises if S denies R's claim that a signed message in R's possession was actually sent by S. In such case, a judge may be called in to decide who is at fault. In an arbitrated signature scheme, on the other hand, all signed messages are transmitted from S to R via an arbitrator A, who serves as a witness. The presence of A reduces (almost eliminates) the occurrence of disputes.

A valid digital signature must provide authenticity, unforgeability, non-reusability, non-repudiation and integrity. Authenticity which states that the signature belongs to the originator, unforge -ability means that only the signer has generated the signature, non-reusability means the signature cannot be reused, non-repudiation means the signer cannot deny the signature and integrity is ensuring the content transmitted is same as the content received.

Apart from using hash function that generates a message digest for digitally signing the message, there are three more algorithms that are used for digital signature generation under the DSS standard.

- DSA (Digital Signature Algorithm)
- RSA (Rivest Shamir Adleman)
- ECDSA (Elliptic Curve Digital Signature Algorithm)

The RSA Signature scheme

The RSA signature scheme [1] is a deterministic digital signature scheme which provides message recovery. For the RSA public-key encryption scheme the message space M and the cipher text C are $Zn= \{0, 1, 2, ... , n-1\}$.

Key-Generation:

In RSA public key cryptosystems each user

1. Generates two large distinct random primes p and q.

2. Computes $n = pq$ and $\Phi = (p-1)(q-1)$.

3. Selects a random integer $e, 1 < e < \Phi$, such that $\gcd(e,\Phi) = 1$

4. Computes the unique integer $d, 1 < d < \Phi$, such that $ed \equiv 1 \bmod \Phi$.

Now the public key of Alice is (n,e) and the private key is d.

Signature Generation:

To sign a message m Є M, Alice

1. identifies m with a number ~ m in Zn through a map R : M → Zn.
2. computes the signature s = ~ md mod n.

Verification:

To verify the signature of Alice, Bob

1. chooses the public key (e,n) of Alice.
2. computes ~ m = se mod n.
3. Verifies that ~ m Є M' where M' denotes the set of images of R. If it does not hold rejects the signature else recovers the message as m = R-1 (~ m).

The DSA Signature scheme:

The DSA [2] makes use of the following parameters:

1. p = a prime modulus, where $2L-1 < p < 2L$ for $512 <= L <= 1024$ and L a multiple of 64

2. q = a prime divisor of $p - 1$, where $2159 < q < 2160$

3. $g = h(p-1)/q \bmod p$, where h is any integer with $1 < h < p - 1$ such that $h(p-1)/q \bmod p > 1$ (g has order q mod p)

4. x = a randomly or pseudo randomly generated integer with $0 < x < q$

5. $y = gx \bmod p$ 6. k = a randomly or pseudo randomly generated integer with $0 < k < q$ The integers p, q, and g can be public and can be common to a group of users. A user's private and public keys are x and y, respectively. They are normally fixed for a period of time. Parameters x and k are used for signature generation only, and must be kept secret. Parameter k must be regenerated for each signature.

Signature Generation:

The signature of a message M is the pair of numbers r and s computed according to the equations below: $r = (gk \bmod p) \bmod q$ and $s = (k\text{-}1(\text{SHA-1}(M) + xr)) \bmod q$. In the above, k-1 is the multiplicative inverse of k, mod q; i.e., $(k\text{-}1\ k) \bmod q = 1$ and $0 < k\text{-}1 < q$. The value of SHA- 1(M) is a 160-bit string output by the Secure Hash Algorithm specified in FIPS 180-1. For use in computing s, this string must be converted to an integer. If either r = 0 or s = 0, a new value of k should be generated and the signature should be recalculated. The signature is transmitted along with the message to the verifier.

Verification:

Prior to verifying the signature in a signed message, p, q and g plus the sender's public key and identity are made available to the verifier in an authenticated manner. Let M¢, r¢, and s¢ be the received versions of M, r, and s, respectively, and let y be the public key of the signatory. To verify the signature, the verifier first checks to see that 0 < r¢ < q and 0 < s¢ < q; if either condition is violated the signature shall be rejected. If these two conditions are satisfied, the verifier computes w = (s¢)-1 mod q u1 = ((SHA-1(M¢))w) mod q u2 = ((r¢)w) mod q v = (((g)u1 (y)u2) mod p) mod q. If v = r¢, then the signature is verified and the verifier can have high confidence that the received message was sent by the party holding the secret key x corresponding to y. For a proof that v = r¢ when M¢ = M, r¢ = r, and s¢ = s. If v does not equal r¢, then the message may have been modified, the message may have been incorrectly signed by the signatory, or the message may have been signed by an impostor. The message should be considered invalid. C.

The ElGamal Signature scheme

The ElGamal signature scheme [3] is a signature scheme.It requires a hash function h : {0,1}* →Zp, where p is large prime. In this scheme, system parameters are : p - a large prime number g - a generator of Z* p h- a secure collision free one-way hash function xA- a random integer in (1, p-1), it works as secret key of Alice. yA- where, yA= gxA mod p, works as the public key of Alice.

Signature Generation:

To sign a binary message m of arbitrary length, the user Alice selects a random integer k Є (1,p-1) such that gcd(k,p-1) = 1. Alice computes r = gk mod p and k-1 mod p-1. He further computes s = k-1 [h(m) - xAr] mod p - 1. " Alice's signature for the message m is (r,s,m).

Verification:

To verify the signature (r, s, m) Bob Checks that 1< r < (p-1) to accept a valid commitment of r, computes v1= yAr r s mod p. Computes h(m) and v2= gh(m) mod p. The signature is valid if and only if v1= v2.

Classes of Digital Signature

To protect the integrity of the signature, the keys are created, conducted, and saved in a secure manner, and often requires the services of a reliable Certificate Authority (CA). There are four classes of digital signature:

Class 0: This type of certificate is provided for demonstration purpose.

Class 1: Class 1 certificate is meant for private subscriber. The main purpose is to confirm that the user name and e-mail address form no duplication within the certifying authorities database.

Class 2: Class 2 certificate is meant for both business as well as private subscriber. The main purpose of this certificate is to assure that the information provided by the subscriber will not conflict with the information in well-known consumer database.

Class 3: Class 3 certificate will be issued to the individuals as well as organizations. The Class 3 certificates are high assurance certificate which is intended for e-commerce applications. Therefore, it is issued to an individual only on their physical appearance before the certifying authorities.

Advantages of digital signature

- Digital Signature enhances the speed of processing a business document as it eliminates, the need for sending paper documents by postal services and getting it signed by all partners.
- A digital signature is transmitted over a network and thus it is cost effective.
- Use of digital signatures and electronic documents alter the risks of documents being decoded, read, removed, or altered during transmission.
- A signatory cannot deny his/her digitally generated signature.
- With the help of time-stamping digital signatures will get the correct time when the documents is signed.

Limitations of digital signature

- Like any other electronic media digital signatures are also valid for a limited period of time.
- For effective use of digital signature it is necessary for both sender and receiver to buy authorized certificates.
- Commandments regarding computer-generated and technology-based issues are weak or even non-existent in some countries. Exchange in such jurisdictions becomes very risky for those who use digitally signed electronic documents.
- Deployment of digital signature scheme must be platform independent.
- The generation process and verification process of digital signature needs substantial quantity of time. So, for regular exchange of communication the speed of communication may decrease.
- If a user changes his private key after every fixed break of period, then the record of all these changes must be reserved. If an argument arises over a previously sent message then the old key pair needs to be referred. Thus loading of all the preceding keys is another overhead.

Existing Schemes

The basic idea of digital signature was first brought by Whitfield Diffie and Martin Hellman in 1976. Ronald Rivest, Adi Shamir, and Len Adleman [1] produced digital signature scheme based on RSA algorithm. T. ElGamal [3] gave a practically implemented digital signature algorithm based on discrete logarithm. A. Fiat, A. Shamir [4] came out with practical solutions that describe simple identification and signature schemes which enable any user to prove his identity and the authenticity of his messages to any other user without shared or public keys. C. Popescu [5] gave an identification scheme based on the elliptic curve discrete logarithm problem. Johnson and et al. [6] proposed an Elliptic Curve Digital Signature Algorithm on considering the strengths of sub exponential time algorithms. Iuon-Chang and Chin-Chen [7] stated security enhancement scheme for digital signature with fault tolerance in RSA.

D. Poulakis [8] narrated a variant of Digital Signature Algorithm based on a factorization problem and two discrete logarithm problems. Qin and Zhou [9] proposed a concurrent digital signature based on Diffie Hellman computations. Zhang and Mao [10] presented a RSA-based construction of certificate less signature scheme in the paper and showed that the security of the scheme is closely related to the RSA problem and the discrete logarithm problem. Minni et al. [11] stated an enhanced RSA algorithm where distribution of n was eliminated from the key so that factors p and q cannot be determined. M. Thangavel et al. [12] produced a modified and an enhanced scheme based on RSA public-key cryptosystem using four large prime numbers thus increasing the complexity than traditional RSA which uses only two large prime numbers. Aswathi and Ebin [13] proposed a modified Elliptic Curve and RSA cryptosystem by incorporating a newly designed Montgomery multiplier algorithm.

Pointcheval et al. [14] provides some security arguments for digital signature as well as for blind signature. The realistic parameters can be justified even if they are not optimal. Sandro et al. [15] provides information about XML signature. XML signatures are type of digital signatures generally helps in XML Transactions. It also defines a particular schema for the storage of XML data’s result based on digital signature operations. Nguyen et al. [16] proposed functionality extension of the Digital Signature Standards. The protocol used here is based on Belarusian DS standards which are flexible and provide a possibility of natural extension of their functionality. Zhang et al. [17] proposed an improved digital signature algorithm based on elliptic curve cryptography. Jian-zhi et al. [18] proposed a design of Hyper Elliptic Curve Digital Signature which combines the features of DSA and HEC algorithms. The algorithm provides high security to check data integrity.

Can et al. [19] proposed a new conic curve digital signature scheme which uses two private keys and provides a high security by upgrading the difficulty of private keys from stealing. Hai-peng et al. [20] proposed an algorithm based on Hash Round Function and self-certified Public Key System that worked on Digital signature. Jarusombat et al. [21] proposed a digital signature technique on mobile devices based on location. This technique uses GPS technology and works on those device that have low computational capability and low battery time period and also applies geo-encryption and mobility model in process of digital signature generation. Harn [22] proposed three threshold digital signature schemes which are totally based on difficulty to solve the discrete log problems. In this the signature's group can be produced when the number of participating member is greater than or same as threshold value. Campbell [23] provides a review on supporting digital signatures in mobile environments. According to the reviews Digital Signature Systems uses the end user's private key to generate a digital signature which has the characteristics of integrity and non-repudiation. W. Romney et al. [24] proposed a digital signature signing engine to protect the integrity of digital assets. This signing engine helps in provoking technologically challenging issues in digital assets. Blind signature scheme is a kind of digital signature with significant application in anonymous electronic voting and electronic payment. Hamid [25] proposed a new blind signature scheme based on hardness of discrete logarithm problem and inherits the efficiency of elliptic curve cryptosystem (ECDLP). The elliptic curved based variant of the proposed system provides a lower computational overhead. Such scheme is unforgeable, blind and untraceable. Hence they are appropriate to be employed in protocols such as untraceable e-payment or e-voting.

Some Applications of Digital Signatures [26]

The literature survey shows that digital signature have already been implemented in various electronic sector environment like the key agreement protocol (e.g. Common shared group key for group communication), contract signing protocol, chip level programming, fault tolerance technique, web based assessment system, identity based authentication and object oriented software engineering.

Key agreement protocol establishes a secure method between two entities who wants to agree on keying information secretly over a distributed medium where the security threat of passive and active attack is more. Similar techniques can be applied during transactions in e-Governance, e-Shopping, e-Voting, e-Learning, e-banking using the elliptic curve version of standard digital signature schemes.

Contract signing protocol is a method which allows the mutually suspicious parties to overcome distrust of each other and helps to interact electronically with minimal risk. This technique initiates Service Level Agreement which specifies the quality of services that has to be maintained between the communicating parties and provides provision for penalty if breach of contract is revealed. This technique can be implemented more efficiently using object oriented modelling during the financial transactions between the business entities and its consumers during online bill payment of goods, online payment of examination fees, online tax payment systems, etc.

Fault tolerance technique defines a method to achieve dependable software which makes it possible to provide service even in the presence of faults. This state can be achieved either by error processing or by fault treatment. Error processing aims to remove errors from the software either by error recovery or by error compensation. Fault treatment aims to prevent the activation of faults and so action is taken before the errors creeps in. Such technique can be used to develop more sophisticated software which will prove to be less susceptible to hardware or software interrupts during its practical implementation.

Web based assessment system provides new tools to the education research community which combines the ability of multiple-choice diagnostic tests to handle large numbers of subjects with some of the greater flexibility and additional information that other methods offer. This process helps to spread education more easily by circulating audio and video study materials using ICT. Elliptic curve cryptography can be smoothly embedded in this method to distribute these online study materials to the students from its actual sender thereby confirming its originality and integrity.

An authenticated key establishment protocol is called identity-based, if users use their identity based asymmetric key pair, instead of a traditional public/private key pair, in the protocol for authentication and determination of the established key. This system can be more cheaply implemented uisng ECDSA, ECRSA, EC ElGamal digital signature algorithms in the identity based smart card applications in various sectors like banking, education, insurance, employment, etc in the developing nations like INDIA.

Object oriented software engineering is the industry standard cost effective and faster methodology to develop a software application. This technique reduces the development time and overheads to produce more flexible and easily maintainable software systems.

Thus irrespective of the domain specific application of digital signatures, the primary focus is always over the implementation of authentication and integrity of data. Apart from non-repudiation, integrity, other parameters like cost efficiency, time efficiency, imposing industry standards, flexibility in generating digital signatures also need to be considered for improving the efficieny of digital signature algorithm.

Proposed Digital Signature Scheme

Understanding the strength and inheriting the properties of discrete logarithmic problem this paper proposes a digital signature algorithm.

The proposed Digital Signature Scheme uses four known values and some properties of discrete logarithm. The proposed Digital Signature algorithm is as follows. In the key generation phase a public key is generated using two secret values x_1 and x_2. To generate the public key, two large distinct prime numbers say, p and q are chosen. Then two secret values $x_1 < (p\text{-}1)$ and $x_2 < q$ are chosen. The public key Y is computed which is defined as $Y= (x_1^p+x_2^q) \bmod ϕ(n)$. ϕ(n) is defines as the product of (p-1) and (q-1).

In the signature generation phase a pair of signature is generated. Two numbers say r_1 and r_2 are chosen randomly such that $r_1 < (p\text{-}1)$ and $r_2 < q$. Using these values K is computed. K is defined as $K= (r_1^p+r_2^q) \bmod ϕ(n)$. Using K, value of M_1 is computed which is defined as H(m)K. H(m) is the message digest of message m which is to be digitally signed. Using the values computed, a pair of signature (S_1, S_2) is generated where S_1 is M_1 and S_2 is defined as $M_{1.}\ (x_1^p+x_2^q) \bmod ϕ\ (n).(r_1^p+r_2^q) \bmod ϕ(n)+ (r_1^p+r_2^q) \bmod ϕ(n)$.

The user whoever wants to verify the signature generated computes a message digest H(m) from the message received. Then the user retrieves the message digest from digital signature. To retrieve the message digest from the signature generated, the user computes $S_1/ (S_2 – S_1Y)$. If the message digest computed and the message digest that is retrieved matches then the signature is said to be a valid one.

Proposed Digital Signature Algorithm

Step by step explanation of proposed digital signature algorithm is as follows:

Key Generation phase

1. SSelect two distinct large prime numbers p and q
2. Select two values $x_1 < (p\text{-}1)$ and $x_2 < q$
3. Compute $ϕ(n)= (p\text{-}1)(q\text{-}1)$
4. Compute the public key Y where, $Y= (x_1^p+x_2^q) \bmod ϕ(n)$

   Y is made public.

Signature Generation phase

1. Randomly select two numbers $r_1<(p\text{-}1)$ and $r_2 <q$
2. Compute $K= (r_1^p+r_2^q) \bmod ϕ(n)$
3. Compute $M_1 = H(m)K$
4. Generate the signature (S_1, S_2) where $S_1 = M_1$ and

   $S_2 = M_{1.}\ (x_1^p+x_2^q) \bmod ϕ\ (n)\ .\ (r_1^p+r_2^q) \bmod ϕ(n)+ (r_1^p+r_2^q) \bmod ϕ(n)$

Verification phase

1. Compute H(m) from M
2. Determine H(m) from $S_1/ (S_2 – S_1Y)$.
3. If H(m) computed in step1 and step 2 are the same then the signature is valid.

RESULTS AND DISCUSSION

The security analysis for the proposed digital signature scheme is as follows

- Forge ability

The security of the proposed digital scheme depends on the four unknown values r1, r2, p and q. If the K computed which uses r1 and r2 is equal to Y which uses x1 and x2, it is computationally infeasible to determine p and q and hence ϕ(n). The complexity and security of the algorithm depends on discrete logarithmic problem

- Integrity

The signature is valid only when the computed H(m) and the H(m) that is sent along with the signature is same. Thus, if any change is made on the signature that is transmitted cannot produced the same hash function of the message H(m) and the signature is incorrect.

- Non-repudiation

The values H (m), p, q, ϕ(n) ensures that only a signer has generated the valid digital signature.

Table 1: below summarizes the security analysis of proposed digital signature scheme

Table 1 Security Analysis of Proposed Digital Signature Scheme

Parameters	ESRKGS	Proposed Scheme
Forgeability	No	No
Integrity	Yes	Yes
Non-repudiation	No	Yes

Cryptanalysis of Digital Signature Schemes

Cryptanalysis is used to break cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown. In addition to mathematical analysis of cryptographic algorithms, cryptanalysis includes the study of side-channel attacks that do not target weaknesses in the cryptographic algorithms themselves, but instead exploit weaknesses in their implementation.

Table 2 shows a comparative analysis of security properties for existing digital signature scheme ESRKGS and proposed digital signature scheme. Like the existing scheme, the proposed scheme preserves the integrity and shows that the proposed digital signature scheme is secure against forgeability. The use of hash function value in proposed digital signature scheme for generating signature shows that only the signer has generated the signature thus preserves non-repudiation.

Table 2. Cryptanalysis of Digital Signature Schemes

Forge ability	No
Integrity	Yes
Non-repudiation	Yes

CONCLUSION

The security of the proposed digital scheme depends on the four unknown values r_1, r_2, p, and q. The results show that even if the value of K computed using r_1 and r_2 is equal to Y which is computed using x_1 and x_2, it is computationally infeasible to determine p and q and hence φ(n). Brute force attack on p and q is infeasible as p and q are large distinct prime numbers which lead to a sort of integer factorization problem. The complexity and security of the algorithm depend on the discrete logarithmic problem. The values p, q, φ (n) ensures that only a signer has generated the valid digital signature. The hash function used to determine hash value of message m is a one-way function and thus it is irreversible and any change on m will result in a different hash value H (m') and thus H(m') ≠ H(m).

.

REFERENCES

[1] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol.21, No. 2, pp.120-126, 1978.

[2] William Stallings, Cryptography and Network Security: Principles and practice.Tsinghua press, 2002, 253-299.

[3] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", Information Theory, IEEE Transactions on Information Theory, Vol. 31, No. 4, pp.469- 472, 1985.

[4] A.Fiat, and A. Shamir, "How to proveyourself: practical solutions to identification and signature problems", Advances in Cryptology-Proceedings of Crypto '86, LNCS, Vol. 263, Springer, pp. 186–194, 1987.

[5] C. Popescu, "An identification scheme based on the elliptic curve discrete logarithm problem", The 4th InternationalConference on High-Performance Computing in the Asia-Pacific Region, Vol. 2, pp. 624–625, 2000.

[6] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)", International Journal of Information Security, Vol. 1, No. 1, Springer, pp. 36–63, 2001.

[7] Iuon-Chang Lin, and Chin-Chen Chang, "Security enhancement for digital signature schemes with fault tolerance in RSA", Information Sciences, Vol.177, pp. 4031- 4039, 2007.

[8] D. Poulakis, "A variant of Digital Signature Algorithm", Designs, Codes and Cryptography, Vol. 51, No. 1, pp. 99-104, 2009.

[9] Qin wen, and Zhou Nan-run, "New concurrent digital signature scheme based on the computational Diffie-Hellman problem", The Journal of China Universities of Posts and Telecommunications, Vol.17, No. 6, pp. 89-94, 2010.

[10] Jianhong Zhanga, and Jane Mao, "An efficient RSA-

based certificateless signature scheme", The Journal of Systems and Software,Vol. 85, pp.638–642, 2012.

[11] Minni R, Sultania K, Mishra S, and Vincent DR, "An algorithm to enhance security in RSA", Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, pp 1-4, 2013.

[12] M. Thangavel, P. Varalakshmi, Mukund Murrali, and K. Nithya, "An Enhanced and Secured RSA Key Generation Scheme (ESRKGS), Journal of information security and applications, Vol.20, No.1, pp. 3 -10,2015.

[13] Aswathi Thomasa, and Ebin M. Manuelb,"Embedment of Montgomery Algorithm on Elliptic Curve Cryptography over RSA Public Key Cryptography", Procedia Technology, Vol. 24, pp.911 – 917, 2016.

[14] Prakash Kuppuswamy, Peer Mohammad Appa, Saeed Q Y Al-Khalidi, "A New Efficient Digital Signature Scheme Algorithm based on Block cipher", IOSR Journal of Computer Engineering (IOSRJCE), Vol. 7, No. 1, pp. 47-52, 2012.

[15] Sandro Gerić, Tomislav Vidacic, "XML Digital Signature and its Role in Information System Security", MIPRO, Opatija, Croatia, 2012.

[16] Minh H. Nguyen, Duy N. HOi, Dung H. Luu, Alexander A. Moldovyan, and Nikolay A. Moldovyan, "On Functionality Extension of the Digital Signature Standards", International Conference on Advanced Technologies for Communications, 2011.

[17] Qiuxia Zhang, Zhan Li ,Chao Song, "The Improvement of digital signature algorithm Based on elliptic curve cryptography", IEEE, 2011.

[18] Deng Jian-zhi, Cheng Xiao-hui, Gui Qiong, "Design of Hyper Elliptic Curve Digital Signature", International Conference on Information Technology and Computer Science, 2009.

[19] Xiang Can, You Lin, "A New Conic Curve Digital Signature Scheme", Fifth International Conference on Information Assurance and Security, 2009.

[20] Chen Hai-peng, Shen Xuan-jing, Wei Wei, "Digital Signature Algorithm Based on Hash Round Function and Self-certified Public Key System", First International Workshop on Education Technology and Computer Science, 2009.

[21] Santi Jarusombat and Surin Kittitornkun, "Digital Signature on Mobile Devices based on Location", IEEE, 2006.

[22] L. Harn, "Group-oriented (t, n) threshold digital signature scheme and digital multi signature", IEEE Proceedings of Computer Digital Tech., Vol. 141, No. 5, 1994.

[23] Scott Campbell, "Supporting Digital Signatures in Mobile Environments", Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, IEEE, 2003.

[24] Gordon W. Romney, "Digital signature signing engine to protect the integrity of digital assets", IEEE, 2006.

[25] Hamid MalaNafiseh Nezhadansari ,"New Blind Signature Schemes Based on the (Elliptic Curve) Discrete Logarithm Problem". Computer and Knowledge Engineering (ICCKE), IEEE, 2013.

[26] Abhishek roy and Sunil karforma, "A survey on digital signatures and its applications", Journal of Computer and Information Technology, Vol.3, No. 1&2, pp.45-69, 2012.