Cryptanalysis of Blind Signature Schemes

Nitu Singh
M.Tech Scholar
Dept. of Cmputer Science & Engineering
Centurion University of Technology and Management.

Sumanjit Das
Assistant Professor
Dept of Computer Science & Engineering
Centurion University of Technology and Management

ABSTRACT

Security of the consumer’s data over internet is the major problem in present time. In this paper we have analyzed blind signature schemes based on RSA and with taking advantage of elliptic curve cryptography to achieve the security goals. Blind signature scheme is one of the security protocol to obtain signature from a signer such that signer sign the message without reading the content of the message and also he could not link the protocol with the resulting message signature pair [7]. Blind signature scheme is used to achieve certain security goals like blindness, untraceability, authenticity, unforgeability [1]. We have analyzed blind signature scheme to achieve the security goals using Elliptic Curve Cryptosystem. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The use of elliptic curves in cryptography was initially presented by Neal Koblitz and Victor S. Miller. Elliptic curve cryptosystem has advantages in terms of smaller key size and lower computational overhead in comparison with public key cryptosystem [2]. Many researchers have been presented the secure blind signature scheme with their own goals and limitations. Two properties a blind signature scheme should hold digital signature and blind signature. By using concept of Elliptic Curve Cryptosystem and blinding algorithm, the signer generates the blind signature without reading content of the message [5]. The scheme avoids the collision between different digital signatures generated by the same singer. The blind signature is a secure technique can be applied in e-business and other applications. Blind signature schemes are widely used for various applications of E-commerce like digital payment systems and electronic voting system etc where to maintain the privacy of consumer is necessary [9].

Keywords

RSA, Blind Signature, Digital Signature, ECC, Security.

1. INTRODUCTION

Now a day’s transaction over the internet has been increased vastly. When data are transmitted through the Internet, it is better that the data are protected by a cryptosystem to prevent them from tampering by an illegal third party. Basically, an encrypted document is sent, and it is impossible for an unlawful party to get the contents of the message, except he gets the sender’s private key to decrypt the message. Under a mutual agreement between the senders and receivers, each sender holds a private key to encrypt his messages to send out, and a public key used by the receiver to decrypt his sent-out messages [1]. When the two message digests are verified to be identical, the recipient can have the true text message. Thus, the security of data transmission can be made sure. User need to be authenticated for many of the application they use. This service can be achieved by the cryptography protocol called Digital Signature. A digital signature scheme provides a way for signer to sign messages using his private key so that the signatures can later be verified by anyone else by using public key of signer [6].

Blind signature scheme is a special form of digital signature, which was first introduced by David Chaum 1982. In a blind signature scheme, a signer signs a message without knowing the contents of the message. The message is blinded by a requester. After receiving the signed message from the signer, the requester can derives the valid signature for the message from the signer. Anyone can verify the blind signature using the public key of the signer. If the message and its signature are published, the signer can verify the signature, but he/she cannot link the message-signature pair [3]. This scheme provides Authentication and non-repudiation to the original sign request sent from a requester so as to prevent fraudulent action by the signer. Blind signatures are widely used in many important cryptographic services, especially in those services that emphasize the privacy of users such as electronic voting over Internet and untraceable payment services [8].

Basically a bind signature scheme is a protocol for a group of requesters and a signer. Each requester sends an encrypted message to the signer and obtains a valid signature from him. Note that the signer only signs the message and does not decrypt it. Later, the signer can verify the genuineness of the signature whenever he receives the message-signature pair; however, he cannot link the message-signature pair to the particular phase of the signing protocol that has led to this pair.

2. DIGITAL SIGNATURE

The digital signatures are used in private communication, where customer privacy is main object. All messages are capable of being encrypted and decrypted so as to ensure the integrity and non-repudiation of them. The concept of digital signatures originally comes from cryptography, and is defined to be a method that a sender’s text messages are encrypted or decrypted through a hash function number in keeping the messages secured when transmitted. Especially, when a one-way hashing function is performed to a message, its related digital signature is generated which is called a message digest. A one way hash function is a mathematical algorithm that makes a message of any length as input, but of a fixed length as output. Because its one-way property, it is impossible for the third party to decrypt the encrypted messages. Two phases of the digital signature process is described in the following.

2.1 Signing Phase

A sender firstly makes his message or data as the input of a one-way hashing function and then produces its corresponding message digest as the output. Secondly, the message digest will be encrypted by the private key of the sender. Thus, the digital signature of the message is done. Finally, the sender sends his message or data along with its related digital signature to a receiver [1,8].

2.2. Verification Phase

Once the receiver has the message as well as the digital signature, he repeats the same process of the sender does, letting the message as an input into the one-way hashing function to get the first message digest as output. Then he decrypts the digital signature by the sender's public key so as to get the second message digest. Finally, verify whether these two message digests are identical or not.

2.3 Blind Signature

The signer signs the requester's message and knows nothing about process and no one knows about the correspondence of the message-signature pair except the requester. Blind signature scheme should satisfy following properties [5].

Correctness: The correctness of the signature of a message signed through the signature scheme can be checked by anyone using the signer's public key.

Unforgeability: only the signer can give a valid signature for the associated message.

Blindness: The content of the message should be blind to the signer; the signer of the blind signature does not see the content of the message.

Untraceability: The signer of the blind signature is unable to link the message-signature pair even when the signature has been revealed to the public.

2.3.1 Blind Signature phases

2.3.1.1 Blinding phase

A sender firstly chooses a random number called a blind factor to mess his message such that the signer will be blind to the message.

2.3.1.2 Signing phase

When the signer gets the blinded message, he directly encrypts the blinded message by his private key and then sends the blind signature back to the sender.

2.3.1.3 Unblinding phase

The sender uses his blind factor to recover the signer's digital signature from the blinded signature.

2.3.1.4 Signature verification phase

Any one uses the signer's public key to verify whether the signature is genuine.

3. ELLIPTIC CURVE CRYPTOSYSTEM

In 1985, Elliptic Curve Cryptography (ECC) was proposed by Neal Koblitz and Victor Miller. ECC is capable of improving the existed cryptogram systems in terms of having smaller system parameter, smaller public-key certificates, lower bandwidth usage, faster implementations, lower power requirements, and smaller hardware processor requirements. Therefore, using ECC to build a cryptosystem is commendable by the reasons of high security and efficiency. The mathematic settings of ECC are depicted below. The elliptic curves can be categorized into two classes: non prime and prime elliptic curves .The elliptic curve cryptography is based on the elliptic curve equation which is given as: $y^2 = x^3 + ax + b$

To plot an elliptic curve one needs to compute:
y = sqrt(x3 + ax + b)
So, value of y is calculated for each value of x, symmetric about y = 0 where values of a and b will be given. Groups are defined based on the set E (a, b) for values of a and b such that: $4a^3 + 27b^2 \neq 0$.

3.1 Non - Prime Curves

Here, is a point of infinity called as the "Zero Point" which is the third point of intersection of a straight line across the elliptic curve. One point that is to be noted is when three point on elliptic curve lie on a straight line they sum up to zero. There are some rules for operation addition '+'for elliptic curve points to follow. Those all are listed down as:

1) If point is O then
O = -O
2) If point P on the curve then
P + O = P
3) If two are P and negative of then that is. $P \equiv (x,y)$ and $-P \equiv (x,-y)$
P+ (-P) = P - P = O
4) If P and Q are two distinct points the addition is as follows:
a) Draw a straight line between P and Q
b) Extend the line and find the third point of intersection with the elliptic curve 'R'
c) To form the Group adds these three points as:
P + Q = -R

Thus, P + Q is the mirror image of the point R.
5) If both the points are the same point P then the steps are as follows:

a) Draw a tangent through point P
b) P + P = 2P = -R

3.2 Prime Curves

In case of these curve the cubic is applied. For prime curves a large prime number p is assumed, and values of all of the variables and coefficients are selected within the range of 0 to p-1 such that the following condition is satisfied. The condition is:
$y^2 \bmod p = (x^3 + ax + b) \bmod p$

Example: a = 1, b = 1, x = 9, y = 7, p = 23
$7^2 \bmod 23 = (9^3 + 9 + 1) \bmod 23$
3 = 3

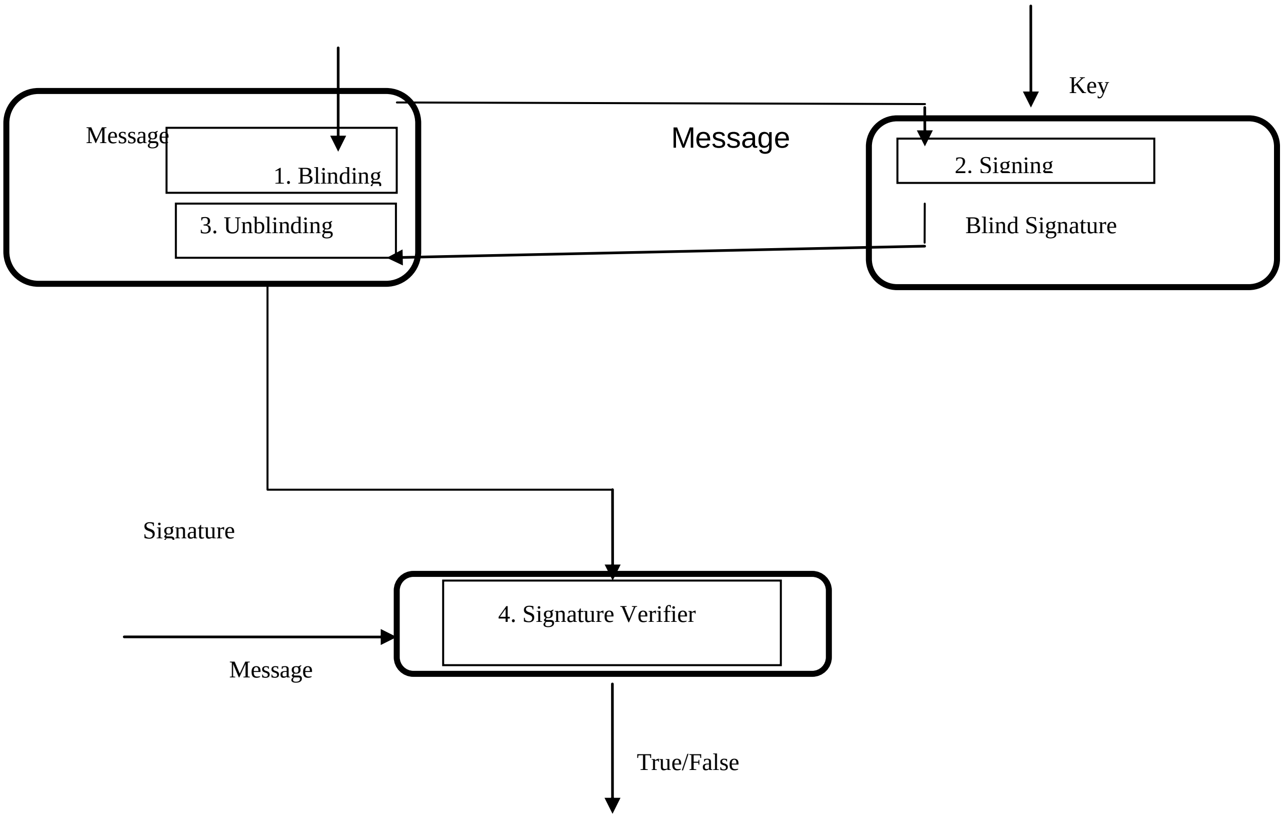

Fig 1: Flow of Blind Signature Structure

4. BLIND SIGNATURE BASED ON RSA

Let us consider standard RSA public key cryptosystems, in which the public key is denoted as a pair (*e*, *n*) and the private key is denoted as a number d. Here, the modulus *n* is a product of two large (secret) primes *p* & *q* and the large (e.g., > 200 digit numbers), such that it is infeasible to find either the factorization of *n* or the private key, *d* given only the public key, (*e*, *n*) . Let a message m ∈ [0, n] be given for which an RSA signature is to be produced.

Let a requester sends a message *m* to be signed by signer using Chaum's blind signature scheme using RSA [1]. The different phases are explained below in detail.

4.1 Blinding Phase

The requester picks a blinding factor *r*, which is a random integer between *0* and *n*, and computes the value:

$m' \;\square\; m * r^{e} \bmod n$ **LL**(1)

The requester sends *m'* to the signer. The *m'* is the message to be signed by the signer as in case of general signature without knowing the original message *m*.

The signer signs the message *m*' using his/her private key d as below signature without knowing the original message *m*.

4.2 Signing Phase

The signer signs the message m' using his/her private key d as below:

$s' = m'^{d} \bmod n,$ LL (2)

The signer returns s to the requester as the blind signature.

4.3 Extraction Phase

The requester after getting the s', he/she extracts the signature s as follows.

$s = s' / r \bmod n$

$m^{d} \bmod n$ LL(3)

$Q_s = (m')^{d} \bmod n$

$= (m * r^{e})^{d} \bmod n$

$= m^{d} * r^{ed} \bmod n$

So the requester finds the actual signature of m as (m,s) which satisfies (3).

5. BLIND SIGNATURE BASED ON ECC

The blind signature scheme which is based on ECC consists of following parameters.
Xs: private key of the signer
Qs: public key of the signer

k: randomly chosen number by the signer
u, v: randomly chosen number by the requester
m: message which the requester wants to blind
H(.): a collision-free hash function
P: a generator point in ECC

5.1 Working procedure

Here given an e-Payment application to indicate the effective of the proposed scheme. If a user (U) wants to withdraw a coin (E-cash) from the bank (B). The procedures of u proposed scheme works as follows:

1. U sends a request to B for withdrawing of E-coin, m.
2. B chooses a random number k, computes R' (=kP), and sends R' to U. After receiving R', U computes R (=uR'+vP) and e (=H (R||m)), using secret random value u and v. Then, U calculates the blinded value e' (e'=e/u) and sends it to B.
3. B uses his/her private key to generate a blind signature S' (=X_be'+k) for e' and sends it to U. Here X_b is B's private key.
4. U un-blinds B's signature S' by using u and v (i.e., S= S'u+ v), and verifies S by checking the equations: SP= eQ_b + R, where Q_b is a public-key of the bank. If the equation holds, U obtains a valid E-cash.

U stores the E-cash S to a diskette or smart card. When the user U wants to purchase merchandise over Internet, he/she sends the E-cash to the merchant. The merchant verifies the E-cash whether legal one or not by checking the equations: SP= eQ_b + R. If the equation holds, the merchant obtains a valid E-cash.

5.1.1Security Analysis

This section shows that this scheme preserves all the characteristic of a blind signature.

5.1.1.1 Blindness

The signer signs a message without knowing its contents. Blindness is the first important property in a blind signature. In this scheme, the requester calculates R = uR' + vP, and generates e' which is a concatenation of R and m with a hash function H (.). Then, he/she sends them to the signer. Hence, the signer cannot know the message m.

5.1.1.2 Unforgeability:

No one can forge (m, R, S) because the elliptic curve discrete logarithm problem is difficult to solve. Assume three situations as follows.

Situation 1: If someone tried to fake R_1, m_1, he/she cannot obtain S_1. Because $S_1P= e_1Q_s+ R_1$ and S_1 is unknown. It is an elliptic curve discrete logarithm problem and difficult to solve.

Situation 2: If someone gets S_1, m_1, he/she cannot obtain R_1. Because $S_1P = e_1Q_s + R_1$, R_1 is unknown, and $e_1 = H(R_1||m_1)$. It is also an elliptic curve discrete logarithm problem and difficult to solve.

Situation 3: If someone tries to fake R_1 and S_1, he/she cannot obtain m_1. Because $S_1P = e_1Q_s + R_1$, he/she cannot get e_1 without m_1. It is an elliptic curve discrete logarithm problem and is difficult to solve.

5.1.1.3 Untraceability

If anyone obtains the valid signature, he/she cannot link this signature to the message. In this scheme, if the signer keep a record set (k_i, R'_i, e'_i, S'_i), where i= 1, 2, …, n, he/she cannot trace the blind signature. Expand this as follows.

When the requester reveals n records (m_i, R_i, S_i) to the public, the signer will compute the values e_i and u', and obtain S_i and R_i, where e_i = H(R_i || m_i), and u'=e_t / e_t' However, the signer cannot trace the blind signature by detecting whether each R_i and R_{i+1} have the same relation. Therefore, the signer cannot trace the blind signature.

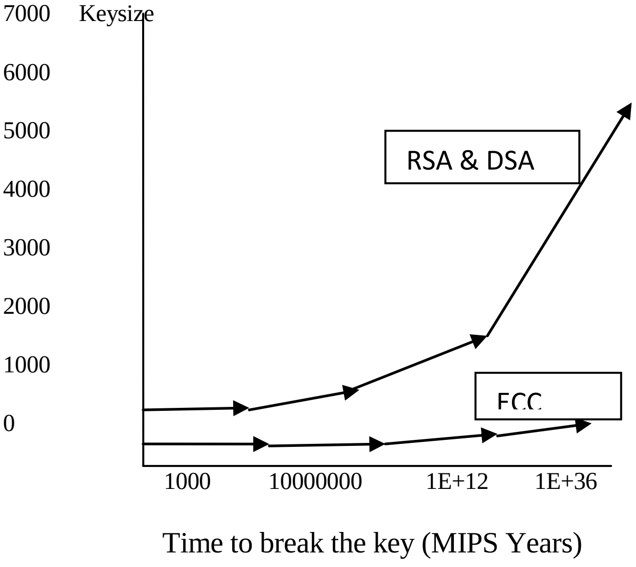

Fig.2 Comparison of Security Levels [2]

Table-1 Average computational time

Blind Signature schemes	Average computational time in ms
Blind Signature based on RSA	220 ms
Blind Signature based on ECC	83 ms

6. CONCLUSION

This paper has analyzed security of Blind Signature scheme based RSA and Elliptic curve [2, 3]. The advantage of ECC in terms of efficiency, storage, bandwidth & computational time and cost in comparison with public key system is more than RSA. Scheme proposed by Debasish Jena *et .al.* based on Nyberg-Rueppel Signature Scheme (NR SS) using Elliptic Curve Discrete Logarithm Problem satisfies all the properties of security goal, but it is implemented for 'offline digital cash' only[4]. The blind signature based on elliptic curve cryptosystem is more secure than the signature scheme based on RSA. The blind signature algorithm can be implemented in 'Electronic voting' system which satisfies all the security goals to reduce the fraud in e-voting [7]. We analyzed that, we can develop a secure Blind Signature scheme and implant it in e-commerce applications using elliptic curve cryptographic algorithm as it is difficult to solve[8, 9]. This can be also implemented using hyperbola to reduce the computational cost and communication overhead in future.

7. REFERENCES

[1] Hwang Lai Su. An efficient signcryption scheme with forward secrecy based on elliptic curve. Journal of applied mathematics and computation, pages 870-881, 2005.

[2] Debasish Jena, Sanjay Kumar Jena and Banshidhar Majhi "A Novel Untraceable Blind Signature Based on Elliptic Curve Discrete Logarithm Problem" IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.6, June 2007.

[3] Fuh-Gwo Jeng, Tzer-Long Chen, Tzer-Shyong Chen "An ECC-Based Blind Signature Scheme" JOURNAL OF NETWORKS, VOL. 5, NO. 8, pp.921-928, AUGUST 2010.

[4] MS.DHANASHREE M.KUTHE, PROF. AVINASH J. AGRAWAL "IMPLEMENTATION OF BLIND DIGITAL SIGNATURE USING ECC" International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 5, October 2012.

[5] Sumanjit Das and Biswajit Samal "An Elliptic Curve based Signcryption Protocol using Java" IJCA, Vol-66, No.4, Mar 2013.

[6] K. H. Huang, Y. F. Chung, C. H. Liu, F. Lai, and T. S. Chen (2007), "Efficient migration for mobile computing in distributed networks," Computer Standards & Interfaces, 2007.

[7] C. W. Shieh (2006), "An Efficient Design of Elliptic Curve Cryptography Processor," Master Thesis, Tatung University, Taipei, 2006.

[8] Y. F. Chung, H. H. Lee, F. Lai, and T. S. Chen (2008), "Access control in user hierarchy based on elliptic curve cryptosystem," *Information Sciences*, vol. 178, no. 1, pp. 230-243, 2008.

[9] Sumanjit Das and Prasant Sahoo "Cryptoanalysis of signcryption protocols based on Eliptic curve" IJMER, Vol-3, No.2, Feb 2013.