IMPLEMENTATION OF BLIND DIGITAL SIGNATURE USING ECC

[1]MS.DHANASHREE M.KUTHE, [2] PROF. AVINASH J. AGRAWAL

[1,2]DEPARTMENT OF COMPUTER SCIENCE AND ENGNEERING
SHRI RAMDEO BABA COLLEGE OF ENGNEERING AND MANAGEMENT, NAGPUR, MAHARASHTRA, INDIA

Abstract

In this paper, we proposed a scheme to implement ‘Electronic Voting’ an important application of Blind digital Signature using elliptic curve cryptographic algorithm. The selection of this algorithm is its difficulty in solving it. The algorithm is used in combination with the blinding factor to scramble the contents of the message to be signed by the signer so that the signer do not come to know what the message is all about. The signer then signs the blinded message that is the vote of the voter and authenticates him/her.

Keywords: Blind Digital Signature, Elliptic Curve Cryptography, Zero knowledge.

I. INTRODUCTION

Now days, online communication is at its hike, many a times data travelling over the communication links is secret and the entire users ought to be authenticated for many of application they use. This is best served by implementing Blind Digital Signature. This blind digital signature is best implemented in the application where secrecy of the user’s data is to be conserved. Blind Digital Signature was first introduced by David Chaum in [1] with the help of a carbon lined envelop which finely explained the concept. The scheme goes as the sender requests for a digital signature as an authentication to his message. The signing authority in return provides with a digital signature but without gaining knowledge about any of the message contents. And hence, the innovation of digital signatures as Blind Digital Signature.

Now, why would one sign a document unless he do not know the contents of the document. The answer is that Blind Digital Signature seems to mean that the authority signs the document blindly but, that’s not the case. Basically, the concept is that the user is authenticated for his identity from the signing authority and not for the message that too without any knowledge of message contents. Now how one proves his identity, in this paper the concept of zero knowledge is used, explained in section III. Then obtained Blind Digital Signature can be verified as the traditional Digital Signature for the same unblinded message.

Blind Signatures are very useful in applications that guarantee the anonymity of the participants [9]. The important application of blind digital signature is electronic voting and electronic cash. In section II the paper shows the relative work done on the blind digital signature by the researchers. The third section gives the complete idea about the proposed system

II. RELATED WORK

Blind digital signature was implemented using many of the cryptographic algorithms. BDS was first proposed using RSA algorithm which was proposed by Rivest, Shamir and Adleman [2] in 1977 which gives the problem of factoring big primes; ElGamal [3] in 1985 proposed ElGamal algorithm which was also used to implement blind digital signature based on the discrete logarithm problem. Also in 1985 elliptic curve cryptal algorithm proposed by Miller and Kblitz[4-6] independently depends on the discrete logarithm problem of elliptic curve. An identity based blind signature algorithm of XTR system in proposed in [8]. XTR algorithm is based on the trace discrete logarithm problem.

Another Blind digital Signature scheme was proposed by Debasish Jena, *et.al.* [9] based on Nyberg-Rueppel Signature Scheme (NRSS) using Elliptic Curve Discrete Logarithm Problem. Here the scheme is implemented for application ‘Offline Digital Cash’ as an instance. The security threats and system weakness of present digital fingerprint schemes were analyzed. In [10] Xuanwu Zhou , *et.al.* Combined blind signature and digital fingerprint, and formed a scheme that reflected digital fingerprint scheme to be asymmetric with conditional anonymity based on elliptic curves cryptosystem. Fuh-Gwo Jeng *et.al.* , in [11]proposed an elliptic curve based blind signature scheme that possesses both the fundamental properties, blindness and intractability and stated that all blind signature schemes proposed so far are based on one of the following: integer factorization problem, discrete logarithm problem, and quadratic residues. However, Lee et al. declared that none of the schemes is able to meet the two fundamental properties above.

III. PROPOSED SCHEME

In this paper, scheme proposed is based on elliptic curve cryptographic algorithm named “The Electronic Voting”.The elliptic curve cryptographic algorithm gives a discrete logarithm problem of elliptic curve which in itself very tedious to solve as in the factors for an elliptic curve equation are non-repetitive..The selection of this algorithm is its difficulty in solving. The algorithm is used in the combination with a hashing function as the blinding factor to scramble the contents of the message to be signed by the signer. The electronic voting scheme has been implemented using the ECC scheme but the blinding factor was being selected randomly [8] within a particular range, but this paper employs a hash function that serves the purpose of blinding factor. Here after, both the algorithms are compared in context to certain parameters.

The voting system needs to possess certain necessities to be a fair system. Those can listed as:

(1)Actuality: Only legal voter could elect.
(2)Honesty: Dishonest elector couldn't disrupt the election.
(3)Confidentiality: All the votes must be kept confidential. Anyone cannot know other's vote.
(4)Unrepeatable: Each voter can elect only once.
(5)Verifiability: All the voters could see whether their ballots are counted in the final statistical table.
(6)Security: Anyone would not tamper with other's vote.

The above all necessities are fulfilled in the proposed scheme.

1) Basics of Elliptic Curve Cryptography

In 1985, Elliptic Curve Cryptography (ECC) was proposed by Neal Koblitz [12] and Victor Miller [12].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 [13]. Therefore, using ECC to build a cryptosystem is commendable by the reasons of high security and efficiency [14]. The mathematic settings of ECC are depicted below [14, 15].

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:

$$y = \mathrm{sqrt}(x^3 + ax + b)$$

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:

$$4a^3 + 27b^2 \neq 0$$

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 add 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

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 coefficiants 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

$$7^2 \bmod 23 = (9^3 + 9 + 1) \bmod 23$$

$$3 = 3$$

2) What is a Zero- Knowledge Proof.

A zero-knowledge proof is a way that a "prover" can prove possession of a certain piece of information to a "verifier" without revealing it. This is done by manipulating data provided by the verifier in a way that would be impossible without the secret information in question. Zero-knowledge proofs are proofs that yield nothing beyond the validity of the assertion. That is, a verifier obtaining such a proof only gains conviction in the validity of the assertion. This is formulated by saying that anything that is feasibly computable from a zero-knowledge proof is also feasibly computable from the (valid) assertion itself (by a so-called simulator) because it enables to force parties to behave according to a predetermined protocol (that is., the protocol requires parties to provide zero-knowledge proofs of the correctness of their secret-based actions, without revealing these secrets).

3) Proposed Scheme is Represented as Phases

Phase I: Key Generation:

In this phase, the private keys and public keys are generated using elliptic curve cryptographic algorithm.

In this phase, a number 'k' is chosed randomly between 1 to (n-1) to be served as the private key. This private key is then treated with the base point of the formed elliptic curve and computes the public key.

Phase II: Blinding:

Here, the voter elects the vote (message). As the votes of the individuals should be kept confidential the votes(message) are blinded. A blinding factor is selected and the vote (message) is then treated with this blinding factor to blind the vote that is to hide the vote from others.

One thing to note is that the blinding factor chosed should possess an existing inverse of itself so that the message blinded could also be unblinded when required.

Phase III: Requester Phase:

In this phase, the voter generates a digital signature using his private key using the scheme of ECC. The voter then sends in entire four entities to the signer as a request for authentication. The entities comprise of identification details, blinded message computed in phase II, digital signature and a proving factor that proves the voter to be a valid citizen.

Here, the factor that proves the voter to be a valid citizen uses the concept of zero knowledge. A valid citizen possesses a private key to oneself but to prove oneself to be a valid citizen one cannot reveal the private key as it is to be kept confidential or intruder may misuse it. The zero knowledge concepts work best in this situation. As we discussed above that a zero-knowledge proof is a way that a "prover" can prove possession of a certain piece of information to a "verifier" without revealing it.

In this scheme, the voter will prove to possess a private key without revealing the private key.

Phase IV: Signing Phase:

In this phase, the signer initially will have the incoming request from the voter with four entities. After receiving the request message the signer verifies for two matters. First, whether requester is a valid voter or not and this is done by cross verifying the proving factor. Secondly, signer notes the identification details and checks whether requester has already voted or not. In other words, signer verify for the actuality of the user applying the voter's (requester) public key and also for the redundancy of voter.

If the requester through both the matters the signer generates blind signature for the particular requester and authenticates the voter. The signer then replies the requester with message – signature pair. The signer displays the identification details and the public keys of the the voters those whose have voted.

In this way all the voters they get authenticated without revealing any secret information of them that is zero knowledge proof.

Phase V: Unblinding:

Voter after receiving the message - signature pair, the message is unblinded and the unblinded message – signature pair is sent to the voting centre acting as a verifier and the counter of the votes.

Here, the message is unblinded as when the message – signature pair is sent to the voting centre the counter must know to whom the voter has voted to be able to count the number of vote for individual elective.

Phase: VI: Verification:

Verifier after receiving the unblinded message – signature verifies the signer's blind digital signature using the public key of the signer. As the signature is verified the count is incremented for elective that is voted. Verifier now displays all the digital signatures and blind digital signatures pairs.Hence the voter is ensured that his/her vote is counted. And no would come to know who voted to whom because only voter know about his own digital signature and blind digital signature recieved from signer.

The voter after choosing the vote blinds it as the signer should not be able to know to whom the voter has voted so the voter's vote remains confidential. Next, signer signs the blinded message and hence the blind digital signature. Now when the blind digital signature – message pair is received by the voter, the message is unblinded. This unblinded message along with blind digital signature is sent to the verifier so that the verifier would see to whom the voter has voted for and update the counters.

IV. CONCLUSION

In this paper, the scheme proposes as to implement ‘Electronic Voting’ an important application of Blind digital Signature using elliptic curve cryptographic algorithm . The selection of this algorithm is its difficulty in solving. The blinding factor to scramble the contents of the message to be signed by the signer .

In this scheme confidentiality of the vote is maintained from each and every aspect , vote of the voter is not revealed at any point except the verifier who counts the vote.Also the signer signs only when the voter is found to be valid.The validity of the signer is verified by the verifier using the signer’s public key. At the verifier’s end the count of the votes for an elective automatically increments as soon as the vote from voter encounters. And hence, the electronic voting is implemented.

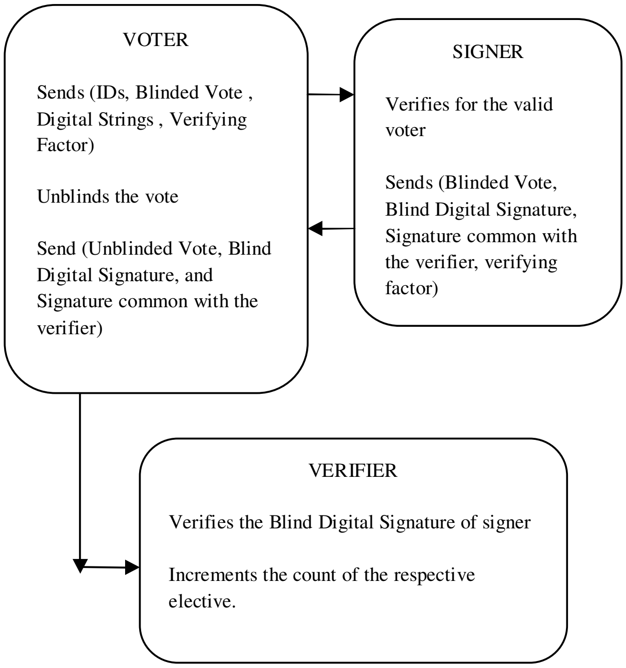
VOTER
Sends (IDs, Blinded Vote , Digital Strings , Verifying Factor)
Unblinds the vote
Send (Unblinded Vote, Blind Digital Signature, and Signature common with the verifier)
SIGNER
Verifies for the valid voter
Sends (Blinded Vote, Blind Digital Signature, Signature common with the verifier, verifying factor)
VERIFIER
Verifies the Blind Digital Signature of signer
Increments the count of the respective elective.

Figure:Flow of the electronic voting scheme.

REFERENCE

[1] David Chaum, “Blind signatures for untraceable payments”, Advances in Cryptology - Crypto ‘82, Springer-Verlag (1983), 199-203.

[2] Rivest R, Shamir A, and Adleman L, “A method for obtaining digital signatures and public key cryptosystems”. Communication of the ACM, February 1978.

[3] ElGamal T, “A public key eryposystem and a signature scheme based on discrete logarithms [J]” . IEEE Trans on Info Theory, 1985, 31(4): 469-472.

[4] V Miller, “Uses of elliptic curves in cryptography [C]” . In: advance in cryptology- CRYPTO’85, Lecture notes in computer science, volume 218, Springer-Verlag, 1986: 417-426.

[5] N Koblitz. , “Elliptic curve cryptosystems [J]”. Math Comp, 1987, (48): 203-209.

[6] Wang H Q, Zhang L J, Zhao J X., “ (t, n) threshold group signature based of elliptic curve without trusted party [J]”. Signal processing, 2006, 22(2): 189-192.

[7] Han Ran College of science, communication university of China Beijing, 100024, China Email: hanran@cuc.edu.cn Wu Zheng peng College of science, communication university of China Beijing, 100024, China Email:wuzhengpeng@126.com

[8]Zhao Jia, Liu Jiqiang, Han Zhen, Shen Changxiang(1 School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044 China) (2 College of Computer Science and Technology, Beijing University of Technology,Beijing 100022)04112070@bjtu.edu.cn

[9] Debasish Jena, Sanjay Kumar Jena and Banshidhar Majhi, “ A Novel Blind Signature Scheme Based on Nyberg-Rueppel Signature Scheme and Applying in off-line Digital Cash” , 10th International Conference on Information Technology.

[10] Xuanwu Zhou1,2, Xiaoyuan Yang1, Ping Wei1, Yupu Hu2, BSADF: “Blind Signature Based Anonymous Digital Fingerprint”, Fourth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2007).

[11]Fuh-Gwo Jeng,Tzer-Long Chen,Tzer-Shyong Chen , “A Blind Signature Scheme Based on Elliptic Curve Cryptosystem”, 2009 Fifth International Joint Conference on INC, IMS and IDC

[12] N. Koblitz, “Elliptic Curve Cryptosystems,” Mathematics of Computation, vol. 48, no. 177, pp. 203-209, 1987.

[13] V. S. Miller,“Use of Elliptic Curves in Cryptography,”Advances in Cryptology: Proceedings of Crypto '85, vol. 218, pp. 417-426, 1986.

[14] S. T. Wu, “Authentication and Group Secure Communications Using Elliptic Curve Cryptography,” Doctoral Dissertation, National Taiwan University of Science and Technology, Taipei, 2005.

[15] 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.