A Novel Identity Based Blind Signature Scheme using DLP for E-Commerce

Girish[#1], Krupa K T[#2], Dr.Phannedra.H.D[#3]

[#1] Associate professor, Dept. of PG Studies , [#2] PG Student, Dept. of Computer Science and Engineering, [#3] Professor, Dept. of Computer Science and Engineering

The National Institute of Engineering,

Manadavady Road, Mysuru, 570008 INDIA

[1]*hpgirish@yahoo.com*

[2]*krupakt45@gmail.com*

[3]*hdphanee@yahoo.com*

Abstract— Blind signatures are used in the most of the application where confidentiality and authenticity are the main issue. Blind signature scheme deals with concept where requester sends the request that the signer should sign on a blind message without looking at the content. Many ID based blind signature are proposed using bilinear pairings and elliptic curve. But the relative computation cost of the pairing in bilinear pairings and ID map into an elliptic curve are huge. In order to save the running time and the size of the signature, this paper proposed a scheme having the property of both concepts identity based blind signature that is based on Discrete Logarithm Problem, so as we know that DLP is a computational hard problem and hence the proposed scheme achieves all essential and secondary security prematurity.

With the help of the proposed scheme, this paper implemented an E-commerce system in a secure way. E-commerce is one of the most concern applications of ID based blind signature scheme. E-commerce consisting selling and buying of products or services over the internet and open network. ID based blind signature scheme basically has been used enormously as a part of today's focussed business. Our proposed scheme can be also be used in E-business, E-voting and E-cashing anywhere without any restriction

Keywords— Identity based encryption, Blind signature, DLP, E-Commerce

*****

I. Introduction

In 1984, the concept of ID-based Cryptography to simplify key management procedures in public key infrastructures was first introduced by Shamir [1]. In Crypto 2001, Boneh and Franklin [2] proposed the first practical ID-based encryption scheme. Since then, ID-based cryptography has been one of the most active research areas in cryptography and number of ID-based encryption and signature schemes has been proposed.

In ID-based cryptography any public information such as e-mail address, name, etc., can be used as a public key. Since public keys are derived from publically known information, their authenticity is established and there is no need for certificates in ID-based cryptography. The private key for a given public key is generated by a trusted authority and is sent to the user over a secure channel.

In the field of cryptography, a blind signature scheme, introduced by David Chaum [3] in 1983, is a special type of digital signature scheme in which the content of a message is hidden or disguised (blinded) before it is signed. The resulting blind signature obtained can be publicly verified against the original unblinded message in the manner of a normal digital signature. Blind signatures are usually used protocols or applications requiring privacy and anonymity, where the signer and message author are two different parties, for example in applications like cryptographic E-voting, E-Commerce and E-cash schemes.

This paper has an implementation of E-commerce system using the proposed scheme. As know due to the fast grow computer technologies, the efficiency of the data processing and the speed of information generation has been greatly improved. Moreover, the techniques of networks largely shorten the communicating time among distributed entities. In this aspect many advanced network services have been proposed. Among these services, E-Commerce is one of the popular services since it realizes the digitalization of traditional service. Using the proposed scheme, E-Commerce makes it possible for customer to pay to the merchant through communication networks under privacy protection. In the proposed E-Commerce system, the customer buys a product and the invoice for the product are generated by the merchant, then customer blinds the invoice. The blind invoice is sent to the merchant. The merchant then signed the invoice and then that signed invoice is sent back to the costumer for unblinding and then this unblind invoice is sent to bank for verification. If the invoice is verified then the amount from the customer's account will be deducted or else it will send a reply back to the customer that he/she is not an authenticated user.

II. RELATED WORK

In 1984, Shamir comes with Identity-based cryptography concept. The unique quality of this approach is that a user's public key may be any binary string. It can be an email address or any unique constraint that can identify the user or signer.

The concept of Identity-based scheme removed the need for a requester or sender to be required look up the recipient's public key before sending out an encrypted message. Identity-based cryptography provides a good convenient alternative to conventional public-key infrastured [10, 13]. There are many identity-based signature schemes [4, 6, 7, 8, 10, 14, 15, 17,18] have been proposed since 1984, but only appeared was in 2001 that was satisfied Identity-based encryption [23]. The advantage of ID Based scheme is that it simplified the process of key management. In the past couple of the year, there are several bilinear paring has been applied to various applications in cryptography [10, 12, 22].

In 1983, D. Chaum gave the idea of blind signature. This technique ensured the secrecy of user. In this approach two parties involved, one user A and other signer B. User A wants sign on a message M by signer B. User, firstly, used hash function on message M and changes to it in $M^{'}$, and transfer it to a signer. Signer creating the signature $s^{'}$ and put into $M^{'}$ and sends back to A. After getting $s^{'}$ user A unblinds into s this is nothing but the signature on a message M. So user A protect the information and not to be revealed. On the other hand, signer assigned a message signature pair (M, s), signer neither able in finding the information about user for he sign a message nor about message.

Later on one-year D.chaum comes with a new blind signature approach using RSA. This approach consists three parties along with five phases that were namely as Initializing, Blinding, Signing, Unblinding and Verifying.

The problem was with this scheme that the true blindness as well as unforgeability not achieved. In 2001, Y.M.Tseng et al. came with a blind signature approach that depended on factoring problem [19].The problem with this approach was a large key size required otherwise an adversary can forge the signature. The same problem with this scheme also exit's signer can trace the message.

This scheme has been satisfied in 1994, M. A. Stadler et al. al. proposed first Discrete logarithm based blind. The first one was blind signature d signature approach [5]. They presented two new blind signature schemes in their proposal scheme generated from a little alteration of Digital Signature Algorithm. Second was based on The Nyberg-Repels signature scheme. L .harm in 1995 announced that the blind signature derived from DSA was providing not a true blind signature [20].Signer can keep the message signature pair and after publishing the message signature pair he/she can trace. Therefore, Camenic's scheme did not satisfy the untraceable property. Later on, on E. Mogammed and E. Emarah proposed a scheme had less computational complexity and better in time from a technique that based on the RSA algorithm [11].The problem with this scheme that in unblinding phase requester has to keep some parameter and on the base of this, he can easily get the private key of signer. So this scheme also did not satisfy the unforgeability. In 2010, a novel blind signature scheme presented by R.L.SHEN that derived from discrete logarithm problem [21] was proposed. This scheme was satisfied all basic requirements.

IDBS approach being much more important since the public key of one's is simply used as his identity. For example, if an electronic case issued by the bank can be easily verified with the help of his identity it can be anything may be a combination of string like banks name, city, country, and year by any user or shops. They do not require to access or fetch a bank's key from PK center.

Generic parallel attack is an open problem for schemes, based on IFP of RSA scheme. The first IDBS scheme was proposed by Zhang and Kim, in 2002 [28]. The security of their scheme depends on the factorization of ROS problem. In 2002, Wagner claimed that the security of Zhang Kims scheme can be broken within time to break ROS problem. In 2002, K. Kim presented a scheme, but it was inefficient to implement and resistance against parallel attack was still not solved. Later in 2003 Zhang and Kim proposed a new ID based scheme that based on bilinear paring [24]. They claimed that their scheme is not depended on ROS problem. Huang et al. proposed an efficient IBBS scheme was more forgeable under problem is solvable. In 2010, Hu and Huang and Zhang et al. proposed an IBBS scheme in a standard model [18].

III. PRELIMINARIES

A. *Identity based Blind signature*

Identity based Blind signature approach being much more important since the public key of one's is simply used as his identity. For example, if an electronic case issued by the bank can be easily verified with the help of his identity it can be anything may be a combination of string like banks name, city, country, and year by any user or shops. They do not require to access or fetch a bank's key from PK center.

An Identity based blind signature scheme consists of following four phases [17].

Setup: The Key Generation Center runs to this phase on input, and makes the public parameter's prams of the scheme and a master challenge. Key Generation Center publishes prams and retains the master unrevealed to it.

Extract: For Given master secret, prams and identity ID, this phase created the secret key S_{ID}.

Issue: The signer put a signature blindly for a person by the present scheme, which is further broken into three phases (Blind, BlindSign, and Unblind).

Blind: User chooses some random string α or β for a given message m, it generates an output with the help of hash function, let's called it m ´and transfer it to the person who had been signing authority.

Blind Sign: In Blind Sign phase, as an input insert the signer's private key s_{ID} that he used for signing the message and blind message m´ then in output it makes a blind signature σ´and transfers it to user.

Unblind: It generates the unblinded signature σ, for given signature $\sigma^{'}$ and random string α or β that used previously.

Verify: Given an identity ID, a message m, a signature σ and prams, this phase output true if σ is a valid signature on m for identity ID, elsewhere false.

The Identity based blind signature scheme should preserve the following requirements,

1. *Blindness:* The message should be blind for a signer, on the other hand, we can say that signer also not disguised the original content.
2. *Unforgeable:* An adversary even if he can imitate the user and freely interact to the signer must not produce or copy a true signs on other documents except for that signer signed.
3. *Untraceability:* By this property , the signer cannot trace the sender of the message after the message-signature pair has been sent to the receiver as well as cannot determine whether an unblinded version of message was signed by him or not , if called upon to verify the same .
4. *Unlinkablity:* A malicious signer must not be able to link output final signature to the user for separate interaction with the user.

IV. PROPOSED SYSTEM

This paper proposed a Novel Identity based blind Signature scheme based upon DLP for E-Commerce, which provides untraceability, unforgeability and blindness to every entity. A secure trusted server involved in the proposed technique who initiates the blinding process. Identity of merchant is used for verification of signature.

The proposed scheme consists of four participants namely, Trusted server, Customer, Merchant and Bank. The proposed scheme will follow six phases.

Setup: The trusted server chooses p as a large prime and q as a prime factor of (p−1), after that he chooses primitive root modulo n, g as a generator in Z_n^*. The trusted server chooses his secret key X_A in Z_n^* and computes his public key Y_A as

$$Y_A = g^{XA} \text{ modp}$$

The trusted server randomly select k in Z_n^* and computes

$$r = g^k\text{modp}$$
$$S_s = (k + rX_A) \text{ modp}$$

Trusted server then sends (r, S_s) to the merchant so that he can calculate his ID and to check the authenticity of a trusted server.

Extract: The merchant checks trusted server's authentication as follows. $g^{SS} = r.Y_A^r(g^k.g^{r*XA} = r * Y_A^r)$ If the particular parameter given by trusted server is authenticated, then he chooses X_B in Z_n^* and computes Y_B as a parameter

$$Y_B = g^{XB} \text{ modp}$$

in a continuation merchant computes the secret key for signing purpose $s = S_s + X_B$ modp and the identity ID_B that will be used for verification purpose. The ID of signer calculated as,

$$ID_B = g^s\text{modp}$$

Blinding: The merchant executes following protocol with customer. The merchant has been provided some agreement parameter so that customer can blind his original message with some restriction. The merchant chooses l, t_R € Z_n^* and computes

$$t_3 = g^{–s}\text{modp}$$

$$t_1 = X_B * (l)^{-1}\text{modp}$$

$$t_2 = s * (X_B)^{-1}\text{modp}$$

$$\mu = g^l\text{modp}$$

And send (μ, t_1, t_2, t_3) to the customer.

The Customer chooses α, β in random fashion in Z_n^* and computes

$$tt = H(m,\mu^{t1}Y_B^{t2}g^{-\acute{\alpha}}\mu\, t_3^{\beta}) \text{ modp}$$
$$t = tt + \beta * \text{modq}$$

And send t to the merchant.

Signing: After receiving t, merchant use his secret key and sign the blind content that provides by the customer. Merchant computes

$$s = (l – t_s)\text{modp}$$

And send s the customer.

Unblinding: After receiving s, the signed blind content customer applied his random selected parameter for unblinding the message, and he get the signature along with their original message without losing his secret. Than the customer computes

$$s1= (s – \alpha) \text{ mod q}$$

(s1, tt, ID_B) This is nothing but the ID along with message m.

Verification: After receiving (s1, tt, ID_B), Bank will verify the signature by using the $ID_{B.}$

The bank computes tt as,

$$tt = H(m, Y_B\, ID_B^{(1+t')}\, g^{s1)}\text{modp}$$

Check if (tt = tt), then the signature is valid and acceptable continues with the transaction otherwise it should be rejected.

V. SECURITY ANALYSIS OF PROPOSED SCHEME

A. *Discrete Logarithm Problem*

Discrete Logarithm Problem: Given amodp or a^nmodp find n, put it in another way here need to compute $\log_a b$ where a,b,p€ Z_p^* this is called discrete logarithm problem. As we know DLP is an example of computational hard problem it is impossible to solve [4, 5, 7, 10, 29]

The public key of trusted server is calculated as

$$Y_A = g^{XA} \text{ modp}$$

this shows the discrete logarithm problem so for calculating X_A, need to calculate the discrete logarithm of Y_A to base g , is not possible to calculate because as we know DLP is a computational hard problem and hence the proposed scheme is secure.

The identity of merchant is computed as

$$ID_B = g^s\text{modp}$$

So if an attacker wants to know the sign parameter s, he/she should be computing a discrete logarithm of ID_B base g so it is also a computational hard problem, so the proposed scheme is secure.

B. *Diffie-Hellman Problem*

The diffie-hellman problem is a given prime p and generator g€ Z_p^* and given that the element g^mmodp and g^nmodp it is hard to find g^{mn}modp. The CDLP is treated as a hard computational problem reducible to DLP in a polynomial time. In proposed algorithm, we have used $g^{-\alpha}$modp and $g^{-\beta}$modp, but the attacker cannot be able to calculate $g^{-\alpha*\beta}$modp, so proposed scheme is also secure based on CDHP.

C. *Correctness*

The blind signature s for a message M is indeed a valid signature. This can be checked with the help of $ID_{B.}$

Theorem 1: *An attacker is not able to create a valid signature*

Proof: For creating a valid signature s attacker should know X_B,S_s both. This implies attacker have control on both the parties that is likely to be impossible because in proposed scheme, both trusted server and merchant are distinguishable even if both are not separate than also an attacker cannot create a valid signature, so it is completely impossible to create it. Even trusted server also cannot forge s because he does not have any idea about X_B.

Theorem 2: *The proposed scheme satisfied the blindness* *property.*

Proof: We have to use the message blindness along with some signer's sent parameter that is t_1, t_2, t_3. After attached this parameter user also generated random parameter α, β and put it with an input message which should pass through the hash function all this combination is present by this equation:

$$tt = H(m, Y_B\, ID_B^{(1+t')}\, g^{s1)}modp$$

The hash algorithm we used in proposed scheme is SHA2, which is the most secure message digest so if a anomalous merchant cannot able to know anything about a true message hence we can say that the scheme satisfied blindness property as well.

Theorem 3: *The proposed scheme can be verified by bank after publishing the message signature pair (s1, tt, ID_B).*

Proof: This can be verified by the following equation:

$$tt = H(m, Y_B\, ID_B^{(1+t')}\, g^{s1)}modp$$

After calculating the value of tt it can be verified if (tt = tt), it is true then a pair is original accepted or else rejected. Hence from this scheme is verifiable.

Theorem 4: *Trusted Server as well as Merchant both need equal authentication in our proposed scheme.*

Proof: In proposed design the identity of merchant is computed from the trusted server's public key Y_A, thus trusted server will not refuse to give his agreement. On the other hand merchant identity involved in blinding hence, the merchant can be identified from his identity ID_B, so after merchant did not deny his agreement also. So, we can say that both merchant and trusted server required authentication.

Theorem 5: *No one able to link the message signature pair even merchant also notable.*

Proof: The property of unlikability also known as untraceable that depend on the traceability or linkability of the message signature pair after publishing it. Untraceability is an important property of the blind signature scheme.

Supposed merchant keeps the message signature pair

$$(s1, tt, ID_B)$$

In proposed scheme, as we used hashing along with some random parameters α, β so it is totally impractical to get the value of arbitrary parameter and after applying the correct hash function also. Hence for an anomalous merchant it is definitely impossible to link the message signature pair.

VI. PERFORMANCE ANALYSIS OF PROPOSED SCHEME

The complexity of all signature schemes generally depends on four operations namely hash function, exponential, multiplication and inverse. As for the knowledge there is no Identity based Blind signature scheme based on the discrete logarithm problem. So the proposed scheme is novel, hence we are not comparing with any other schemes.

Here we are not commutated the time complexity of an Ecommerce application. And the computational complexity may vary for different application.

From this analysis we came to know that the proposed scheme takes lesser computational time and size of the signature is relatively smaller than elliptic curve and bilinear pairing, hence the proposed scheme is novel in every aspect.

VII. CONCLUSION

In this paper, a new Novel Identity based blind signature scheme using DLP for E-Commerce system that is satisfying all security features with low computational overhead as well as feasible has been proposed. Proposed scheme satisfying all the security goals of Identity based Blind Signature like Verifiable,Blindness, correctness, unlinkability, unforgeability and untracability. As best of our knowledge we are the first one to provide the concepts by using these two notations together. In future, optimisation of the algorithm in E-Commerce has to be done so, that it can be feasible enough to use in real time scenario. With the help of the proposed scheme a more secure E-cashing, E-voting, E-business can be implemented in great way. Our proposed scheme can also used for perfect crime avoidance. All the security faults of existing Identity Based Blind Signature system has solved by proposed scheme.

REFERENCES

[1] Shamir. Identity-based cryptosystems and signature schemes. In Proc. of CRYPTO'84, volume 196 of LNCS, pages 47–53. Springer- Verlag, 1984.

[2] Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In Proc. of CRYPTO'01, volume 2139 of LNCS, pages 213– 229. Springer-Verlag, 2001

[3] Chaum. Blind signatures for untraceable payments. In Proc. of Crypto'82, pages 199–203. New York: Plenum Press, 1983.

[4] Shamir, Adi.Identity-based cryptosystems and signature schemes, Advances in cryptology, 47- 53, 1985.

[5] Huang, Zhenjie and Chen, Kefei and Wang, Yumin. Efficient identity-based signatures and blind signatures, Cryptology and Network Security, 120-133, 2005.

[6] Victor R. L. Shen, Yu Fang Chung, Tsar Shying Chen. A blind signature based on discrete logarithm problem, ICIC International, 5403-5416, September 2011.

[7] Jingfeng Su,Juxia Liu. A Identity Based Proxy Blind Signature Scheme Based on DLP, Internet Technology and Applications, 2010 International Conference on, 1-4, September 2010.

[8] Li, M. Zhang, and T. Takagi. Identity-based partially blind signature in the standard model for electronic cash Mathematical and Computer Modelling,2012.

[9] C.-I. Fan. Ownership-attached unblinding of blind signatures for untraceable electronic cash, Information Sciences, 176(3):263 -284, 2006.

[10] D. He, J. Chen, and R. Zhang. An efficient identity-based blind signature scheme without bilinear pairings, Computers Electrical Engineering 37(4):444-450, 2011.

[11] E. Mohammed, A. E. Emarah, Kh. ElShennawy.A Novel Blind Signature Using El- gamal, IEEE Arab Academy for Science and Technology, pages 189196. Air Defense Research Center, 2000

[12] Chen, Min Qin and Wen, Qiao Yan and Jin, Zheng Ping and Zhang, Hua. Secure and Efficient Certificateless Signature and Blind Signature Scheme from Pairings, Applied Mechanics and Materials, 1262-1265, 2014.

[13] D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. SIAM J. Computing, 30(2):391-437, 2000.

[14] Xiaoming Hu,Shangteng Huang.Analysis of ID-based restrictive partially blind signatures and applications,The Journal of Systems and Software 81 (2008) 19511954.

[15] Chen, X.F., Zhang, F.G., Liu, S.L., 2007. ID-based restrictive partially blind signatures and applications. The Journal of Systems and Software 80 (2), 164171.

[16] S.M. Chow, C.K. Hui, S.M. Yiu and K.P. Chow, Two improved partyially blind signature schemes from bilinear pairings, ACISP 2005, LNCS 3574, Springer, pp. 316-328.

[17] Xiaofeng Chen , Fangguo Zhang and Shengli Liu. ID-based Restrictive Partyially Blind Signatures. Cryptology ePrint Archive, Report 2005/319.

[18] X. ming and S.Huang,Secure IDBS Scheme in the Standard Model,Journal of information science and engineering 26, 215-230 (2010).

[19] H. Y. Chien, J. K. Jan and Y. M. Tseng, RSA-based partially blind signature with low computation, IEEE, pp.385-389, 2001.

[20] L. Harn, Group-oriented threshold DS scheme and DMS, IEEE, vol.141, no.5, pp.307-313, 1994.

[21] L. J. Wang, J. J. R. Chen, Novel DSMS, ICIC, pp.1251-1256, 2010.

[22] K.A.ajmath,T.gowri,An IDBS Scheme from Bilinear Pairings,IJCSS volume(4),2003.

[23] D. Boneh and M. Franklin, IDE from the Weil pairingProceedings of Crypto, LNCS 2139, 2001, pp. 213-229.

[24] F. Zhang, K. Kim, Eﬃcient IDBS and PS from bilinear pairings, ACISP2003 , Springer-Verlag, 2003, pp.312-3323.

[25] L. Zhang,X. Tian,Novel Identity-based BS for Electronic Voting System,2010 Second International Workshop on Education Technology and Computer Science .

[26] Ni.Zhang,Jian Ping,ID-based Proxy blind signature scheme with unlinkability,DOI:10.1109/ICEICE.2011.

[27] S. Prabhadevi, A. M. Natarajan,Utilization of IDB Proxy BS Based on ECDLP in Secure Vehicular Communications IJEIT,, November 2013.

[28] F. Zhang, K. Kim, IDBS and ring signature from pairings,LNCS 2501,Springer Verlag, 2002, pp.533-547.

[29] G. B. Agnew, R. C. Mullin and S. A. Van- stone Improved digital signature scheme based on discrete exponentiation, Electronics Letters, vol.26, 1024-1025, 1990.