ISSN:0975-9646
Girish et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2678-2681

Survey on Identity Based Blind Signature

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

[#1] *Department of PGS ,*

[#2] *Department of Computer Science and Engineering,*

[#3]*Department of Computer Science and Engineering*

[1,2,3]*The National Institute of Engineering, Mysore, 570008 INDIA*

***Abstract*— In this paper, we survey the state of research on Identity Based Blind Signature. We start from reviewing the basic concepts of identity based encryption and blind signature schemes and subsequently review the framework of ID-based blind signature, and classification of ID-based blind signature. Lastly, we discuss the applications of ID-based blind signature.**

***Keywords*— Identity Based Encryption, Blind signature**

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 publicly 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 election systems and digital cash schemes.

II. BASIC CONCEPTS OF IDENTITY BASED ENCRYPTION

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].

III. BASIC CONCEPTS OF BLIND SIGNATURE

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.

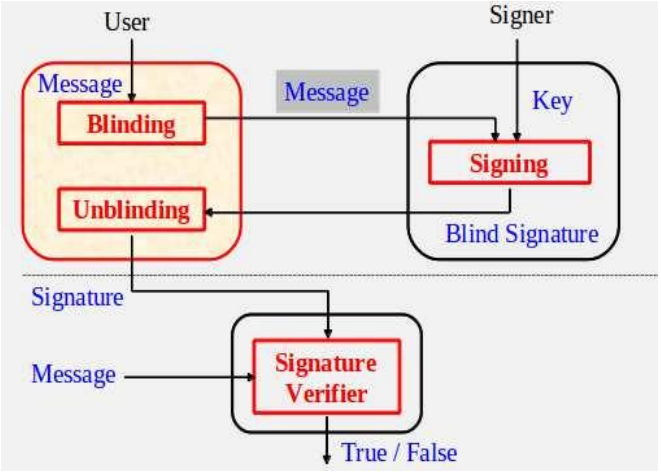

Fig1: Blind Signature Process

The blind signature scheme should preserve the following requirements,

A. *Blindness:* The message should be blind for a signer, on the other hand, we can say that signer also not disguised the original content.
B. *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.
C. *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 .
D. *Unlinkablity:* A malicious signer must not be able to link output final signature to the user for separate interaction with the user.

IV IDENTITY BASED BLIND SIGNATURE

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].

V. CLASSIFICATION OF IDENTITY BASED BLIND SIGNATURE

There are five types are schemes that are mainly divided into five categories:

A. ID Based Blind Signature:

These schemes are based on a simple blind signature concept, only change is that instead of public-key signer's ID used for verification process. No need to manage a PKI unit at all. ID can be used by anyone for verification purpose [4, 6, 8, 9,18].

B. *ID Based Restrictive Blind Signature:*

Restrictive blind signature schemes which allow a user to receive a signed message without getting to reveal his private content of the message, but the selection of the message should be restricted. It should follow some constraint.

C. *ID Based Partially Blind Signature:*

Signer should explicitly add some extra information. Extra information can be anything, date of expiration, time stamp, or whatever .On the resultant signature under some prerequisite agreement with user [16].In 2007, a partial blind signature concept was given efficient than had less computation complexity and equal privacy concern than Chan et al's scheme [15].Chan's scheme does not satisfy the restrictiveness and double spending problem.

D. *ID Based Restrictive partially Blind Signature*

Restrictiveness and partially both are an important security concerns on cryptography. A blind signature scheme which is based on this two property called IDPR-blind signature [14, 15, 16, 17]. Fangguo Zhang claimed that their scheme was secure (provably) in the random oracle model [14].Their scheme was used to build an off-line, an untraceable E-cash system.

E.ID Based Proxy Blind Signature:

A proxy signer used his/her private key for signature instead of original signer. This is a combination of proxy and blind signature concept. In 2008, first proxy based scheme was given but the problem with the scheme is that it does not fulfill the untraceability property. The proxy signer can forge the secret key of original signer and grant the authorities to others. In 2011, Ni Zhang had presented an efficient scheme that satisfied the untraceability [26].In 2013, a more feasible and secure ECDLP based scheme presented by sundram which solved a common problem of revoke of delegation by original signer [27].

VI. FRAMEWORK OF IDENTITY BASED BLIND SIGNATURE

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 σ´ 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.

VII. APPLICATION OF IDENTITY BASED BLIND SIGNATURE

A. *E-Voting System*

E-voting is a most important application of blind signature scheme [15, 25].To cast vote and counting the electronic vote is known as electronic voting. Voter is free from of any fair because he/she put cast their vote blindly admin is nothing but the authority who provides the sign. E-voting application may be organized by any government representative, private organization, or any special group of people. The privacy of user who cast the vote is keeping blind. Every user's cast vote can be easily verified with the help of admin's identity. The confidentiality issue related to digital signature is a bit solved by IDBS scheme.

B. E-Cashing

E-cashing is most concern applications of IDBS scheme [14].E-cashing consisting selling and buying of products or services over the Internet and open network [9].IDBS scheme is a simply has been used in today's competitive market. Android based applications have been designed using IDBS idea. User has to execute blind signature and verify phase and the merchant distinguished with a bank's authority.

C.E-Business

E-Business is a combination of e-mail and e-commerce. Both services conduct under the open network or in the Internet, the selling and a significant part of the early worry about the security of a business transaction on the Web, can be solved with IDBS system.

CONCLUSIONS

In this paper, we survey the state of art of the Identity based blind Signature. We discuss the different types of Identity Based Blind Signature and framework of IDBS. The area in the field is still growing and many new applications of the IDBS will be added. We believe our survey helps in providing best knowledge of IDBS. With the help of our survey, IDBS can be used in many real world applications like E-cashing, E-voting and E-business and may be used in perfect crime avoidance also.

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 pairing, in Proceedings 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.