International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-4, Issue-1, January 2016

A Strong Blind Signature Using Cascade Blind Factors

Dr.Ayman A.Rahim A.Rahman, Dr.Abdulameer K.Hussain,

Abstract— **This paper presents a modified version of blind signature . The proposed method adds more complex blind factors to increase the blindeness property of the message sent . In order to achieve this goal , the proposed system suplements the traditional blind signature methods by multiple random variables which are called blind factors attached at different locations in the original message . The blind signature method in this paper is implemented in sensitive applications such as voting and cash transfer.**

Index Terms— **Digital Signature , Blind Signatures, Blind factors , Cryptography .**

I. INTRODUCTION

In cryptography , digital signature schemes are essential for electronic commerce because they allow one party to authorize digital documents that are transmit across networks. Typically, a digital signature comes with not only the document body but also with attributes such as "date of issue" or "valid until", which may be controlled by the signer rather than the receiver. One can find more about those attributes in public key cryptography standards ,PKCS [1].

II. DIGITAL SIGNATURE

Blind signature is a form of digital signature in which the content of a message is disguised (blinded) before it is signed. The resulting blind signature can be publicly verified against the original, unblinded message in the manner of a regular digital signature. Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties. Examples include cryptographic election systems and digital cash schemes.[2]

One type of blind signatures is a partially blind signature that allows the signer to explicitly include common information in the blind signature under some agreement with the receiver. For instance, the signer can attach the date of issue to his blind signatures as an attribute. If the signer issues a huge number of signatures in a day, including the date of issue will not violate anonymity. Accordingly, the attributes of the signatures can be decided independently from those of the public key [3].

Manuscript received October 13, 2015.
Ayman A.Rahim A.Rahman, CIS, Jerash University/ Jerash, Jordan
Abdulameer Hussain, CS, Jerash University/ Jerash, Jordan

III. CONCEPT OF BLIND SIGNATURE

The concept of blind signature was introduced by David Chaum in 1982 [2,4]. A blind signature scheme facilitates to ensure that the user's private information would not be revealed when he/she proceeds with casting or purchasing over the internet. According to Chaum who offered the concept, two parties, namely a group of requesters and a signer, are the participants of a blind signature scheme. Suppose one of the requesters asks for a blind signature from the signer, first the requester blinds a message using the blind factor and then sends the blinded message to the signer. After receiving the blinded message, the signer signs it using his/her private key and then sends the blinded signature back to the requester. Afterwards, the requester can extract the signature signed by signer by eliminating the blinding factor from the blinded signature. To verify successfully the legitimacy of the signature; one can utilize the signer's public key. The typical applications of blind signatures include e-cash, where a bank signs coins withdrawn by users, and e-voting, where an authority signs public keys that voters later use to cast their votes. Another application of blind signature scheme is anonymous credentials, where the issuing authority blindly signs a key [5,6]. Recently, Microsoft introduced a new technology called U-prove to overcome the long standing dilemma between identity assurance and privacy which uses as a central building block blind signatures [7,8].

IV. BLIND SIGNATURE SCHEME

The blind signature scheme is supposed to satisfy the following requirements: [4, 9, 10]:

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

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

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

4: 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.

There are many blind signature schemes have been proposed. Recently, many researchers proposed a variety of blind signature schemes [11, 12,13]. The most widely used

blind signature schemes are: RSA blind signature schemes [2], ElGamal signature scheme [14], and Schnorr Blind signature scheme [15]. RSA blind signature scheme security is based on the problem of integer factorization, while ElGamal and Schnorr blind signature schemes are based on the problem of discrete logarithm.

V. RELATED WORKS

In [16] a research of an efficient blind signature scheme under which information can be hidden in the signature and uncovered later for security purposes. This scheme when it is applied to an untraceable electronic cash system, cash owners are able to claim and identify lost cash; when applied to an anonymous electronic voting protocol, no election results are revealed until the entire voting process is finished.

A new work had been proposed to provide a novel blind signature scheme based on Elliptic Curve Cryptography (ECC) . The security of the proposed method results from the infeasibility to solve the discrete logarithm over an elliptic curve. This work had developed the blind signature scheme with more complexity as compared to the existing schemes [17].

In [18] , a paper presented a new generalized blind signature scheme based on modified Elgamal signature. The new design has an important property that ensures if a message is signed multiple times, the corresponding signatures are different (this property is one of the properties of Elgamal signature). With the blind signature scheme proposed in this paper, one with the use of quality of common Elgamal signature can produces the blind signature. New design in comparison with RSA blind signature scheme has less computational complexity and is faster as well.

A new blind signature scheme based on factoring and discrete logarithms had been proposed . This scheme provides a longer or higher security than that scheme based on a single hard problem. This is due the impossibility of attackers to solve two hard problems simultaneously. Some possible attack have also been considered and we showed that the scheme secure from those attacks. The newly developed scheme also has the advantage of having low-computational complexity for the signature-requester and the signer, thus makes it very efficient [19] .

VI. PROPOSED SYSTEM

This method applies the RSA method to generate a more complex blind signature . The first step of this method is to take a message (m) and convert it to a digital representation . Then the original message is blinded by multiplying it with two random variables r_1 and r_2 such that r_1 and r_2 are relatively primes . This means that GCD (r_1,N)=1 and GCD (r_2,N)=1 , where n is the product of two prime numbers p and q respectively . These two random numbers , r_1 and r_2 , are raised to the public key (e) of the sender . Then the parties choose two prime numbers p and q and compute N=p*q.

This procedure generates a double blind message representing as :

$m'=mr_1^e r_2^e \bmod N$

where $r_1^e r_2^e \bmod N$ is called a combined blind factor.

In this case we need an authenticated trusted entity called signing authority (SA) . Then m' is sent to this entity . The signing authority signs m' using his/her private key (d) to produce the signature SG such that :

$SG=(m')^d \bmod N$

SG is sent back to the author of the message m' who can then remove the combined blinding factor to reveal SG.

In this method we propose two alternative methods to recover SG. The first one is that the author of the message can extract the two known random numbers from m' . The second method is to use RSA algorithm . These steps are explained below :

$SG_{new}=SG^{-1}r_1^{-1}r_2^{-1} \bmod N$

So $SG_{new} = (m')^d r_1^{-1} r_2^{-1} = m^d r_1^{ed} r_2^{ed} r_1^{-1} r_2^{-1}$

The Algorithm

Choose two prime numbers p an q .

Compute N=p * q

Compute Phi(N)=(p-1)(q-1)

Choose a public key (e) such that GCD (e, N)=1

Compute the corresponding private key (d) such that $d=e^{-1} \bmod n$

Compute $m'=mr_1^e r_2^e \bmod N$

Generate the signature by SA as $SG=(m')^d \bmod N$

Recover and ensure the signature as :

$SG_{new}=SG^{-1}r_1^{-1}r_2^{-1} \bmod N$

So $SG_{new} = (m')^d r_1^{-1} r_2^{-1} = m^d r_1^{ed} r_2^{ed} r_1^{-1} r_2^{-1}$

VII. CONCLUSION

This method proposes strong blind signatures. Most of traditional blind signatures use one blind factor to hide the content of the message and still this procedure is subjected to active attacks to recover the original message. In this method we add extra blindness by adding two blind factors in which the original blind message is blinded at different levels and thus we design a new concept which is called a cascade blindness. This system enhances the blindness property because it is not sufficient to use a single random number. In the traditional blind signatures, one random bit b belongs to R in terms of {0,1} and this value may be subjected to forgeability property in such a way that the signer controls the random selection but not the signing entity . However, in this case the signing entity tries to do two signatures for one random number, but if the signer adds another random number to the message, the signing entity cannot forgeable the signature and hence we can prevent the forgeability property which may occur. We can also make more enhancement to blind signature by using multiple blind factors and in such case the system must breakdown the signature into different parts from the a trusted signing entity .

REFERENCES

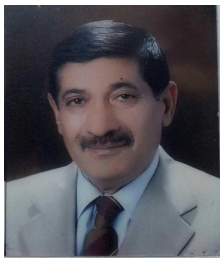
[1] RSA Laboratories. PKCS #9: Selected Object Classes and Attribute Types, 2.0 edition, February 2000.

[2] Chaum, David . "Blind signatures for untraceable payments". Advances in Cryptology Proceedings of Crypto 82 (3): 199–203

[3] A. Juels, M. Luby, and R. Ostrovsky. Security of blind digital signatures. In B. S. Kaliski Jr., editor, Advances in Cryptology — CRYPTO '97, volume 1294 of Lecture Notes in Computer Science, pages 150–164. Springer-Verlag, 1997

[4] Chaum, D., (1983) "Blind signatures system",in Advances in cryptology , CRYPTO'83, pp:153-156,1983.
[5] Stefan A.Brands., (2000), " Rethinking Public Key Infrastructures and Digital Certificates : Building in Pravacy":.MIT Press, Cambridge, MA, USA,2000.
[6] Jan Camenisch and Thomas GroB,(2008) "Efficentt attributes for anonymous credentials" In Peng Ning, Paul F. Syverson, and Somesh Jha, editor s, ACM CCS 08: 15th Conference on Computer and Communications Security, Alexandria, Virginia, USA, October 27-31, pp: 345-356, 2008.
[7] Ronny Bjones, (2010) " U-prove technology overview".http://www.itforum.dk/downloads/ Ronny_Bjones_Uprove.pdf , October 2010.
[8] Microsoft (2011), MICROSOFT U-PROVE. Microsoft u-prove ctp release 2. http://connect.microsoft.com/site642/Downloads/DownloadDetails.aspx?DownloadID=26953 , March 2011.
[9] Chu-I Fan, Chen,W.K. & Yeh,Y.S., (2000) "Randomization enhanced Chaum's blind signature scheme Computer communications , Vol 23, 2000, pp 1677-1680.
[10] Zuhua Shao,(2000) "Improved user efficient blind signatures", Electronics Letters , Vol.36, no.16, pp.1372-1374, 2000.
[11] Verma,G.K., (2008) " Blind signature schems over Braid groups" http://eprint.iacr.org/2008/027.
[12] Markus Ruckert, (2008) " Lattice-based Blind signatures", http://eprint.iacr.org/2008/322.
[13] Fuh-Gwo Jeng, Tzen-Long Chem, & Tzer-Shyong Chen, (2010) "An ECC-Based Blind Signature Scheme",Journal of Networks,Vol 5, No 8, 2010.
[14] Carmenisch,J.L., Piveteau,J.M. & Stadler,M.A., (1994) "Blind signature based on the discrete logarithm problem", EUROCRYPT '94, Perugia, Italy,1994.
[15] David Pointcheval & Jaques Stern, (1996) "Provably Secure Blind Signature Schemes" ,Advances in Cryptology – Proceedings of ASIACRYPT ' 96, M. Y. Rhee and K. Kim Eds.Springer-Verlag, LNCS 1163, pages 252-265, 1996.
[16] Chun-I Fan, Wei-Kuei Chen , An Efficient Blind Signature Scheme for Information Hiding , International Journal of Electronic Commerce ,Volume 6, Issue 1, 2001
[17] E.H. El Kinani, Fatima Amounas , Proposed Developments of Blind Signature Scheme based on The Elliptic Curve Discrete Logarithm Problem , Computer Engineering and Applications Journal , Vol 3, No 2 (2014)
[18] Amir Aliabadian , Ali Delavari Ghara, New Blind Digital Signature Based On Modified Elgamal Signature in Electronic Voting , international Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 –8958,Volume - 1, Issue -6, August 2012
[19] N. M. F. Tahat, E. S. Ismail and R. R. Ahmad , A New Blind Signature Scheme Based On Factoring and Discrete Logarithms , International Journal of Cryptology Research 1 (1) : 1-9 (2009)

Dr. Ayman A. Rahim A. Rahman, Jerash University-Jordan. PhD,MSc,BSC. He has completed Master degree in Information Technology, and his PhD in Computer Information System , and presently working as Assistant Professor in Jerash Uiversity



Dr. Abdulameer K. Husain, Jerash University- Jordan.He has completed Master degree in computer science ,university of Sadam , Iraq , in 1991 and his PhD in computer science , computer security from Al-Neelain University ,Sudan . He has total 20 years teaching experience and presently working as Associate professor in Jerash University –Jordan.