International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2000-000X
Vol. 1 Issue 7, September – 2017, Pages: 149-154

A New Multiple Blind Signatures Using El-Gamal Scheme

Muthanna Abdulwahed Khudhair
Dijlla University College, Iraq

Abstract: *This paper presents a new secure blind signature. In order to secure the blind signature, this scheme generates two blind signatures. Each of the blind signatures has its own blind factors. In addition, the author of the message encrypts the information sent to the signing author by an encryption key generated by El-Gamal cryptosystem, which is considered a strong cryptographic key. This key adds a secure and hidden layer to the message being signed. In addition, the author of the message binds an agreement factor for each type of message and a context that characterized the type of message signed. This method provides the most important properties for a secure blind signature.*

Keywords: Blind Signature, Message Context, Agreement Factors, El-Gamal cryptosystem.

1. INTRODUCTION

David Chaum introduced the concept of blind signatures. The aim is to generate an electronic way of money transfer such that e-coin cannot be easily traced from the center of the bank to the customer. In such a way, any two spending of the same user have no ability to linked together. Chaum explained that when applying blind signatures we could get two important properties; namely untraceability and unlinkability. In the blind signature the signer does not know anything about the contents of any sent message. One important and derivate of digital signatures is a blind signature. We can generate blind signature by adding some other properties to any type of digital signature. The concept of a blind signature is that it is considered a protocol for generating a signature s for a message m from a certain signer SG such that SG does not know anything about s and m . So the contents of the message are hidden from SG. The operation of this protocol is that any user U can select a random number k and merge this r into m to produce m'. m' is sent to SG who will generate a signature s' corresponding to m' . SG returns back s' to the user U. The user U will remove the blind factor to get s which is the signature of m . So according to this procedure, both m and s are hidden from SG. The most important property of blind signature is that it unforegeable . Blind signatures are used in many sensitive applications such as cash protocol to provide a strong protection for the privacy of customers[1] .

Blind signature scheme consists of three parts. The first part is key generation which is a probabilistic polynomial time. The second part is blind signature generation. This generation is an interactive protocol between the signer SG and the user U. The last part is blind signature verification which is a deterministic polynomial time algorithm [1,2] .

Blind signatures use the traditional public key cryptography in which each user has two different cryptographic keys, a private and a public key. This needs to simplify the key management, Shamir [3] invented the idea of identity-based public key cryptography .In this scheme each user must identify himself/herself and we need a way to facilitate the users to register them at Key Generator Centre (KGC).

There are different proposed blind signatures schemes [4–9]. The blind signature schemes are useful especially when we need o provide an anonymity .Such applications are sensitive, for example the online voting systems and the electronic cash systems [8].

ElGamal is a cryptographic scheme used to provide a signature. If we compare it with symmetric algorithms in terms of encryption and decryption speed, we find that ElGamal is relatively slower [10-12]. This scheme is one type of a non- deterministic public key cryptography. This scheme has different signatures for the same message because it chooses different random factors. The generated signature allows message recovery and so it has many advantages [13-18]. One advantage is that it generates a shorter signatures corresponding to shorter plaintexts. ElGamal scheme combines the plaintext with the validation of the signature [4]. An improvement to ElGamal mode had been suggested by Nyberg and Rueppel . In this modification it is possible to receive a series of signature schemes .These new schemes can provide verification to the signature at the time of performing a message recovery [17-19].

El-Gamal signature scheme was first introduced by TaherElgamal in 1984. This scheme can generate a signature based on difficulty of computing the discrete logarithms so it is considered a type of public key cryptosystem. There are two attacks that are may occur against El-Gamal scheme. These attacks are low modulus attack and plaintext attack [20]. The first attack can arise when we use values of modulus that are low while plaintext attack is applicable when the enemy discovers the plaintext which is corresponding its ciphetext and in this case it is easily to find the cryptographic key.

In order to provide security for digital data transmitted through communication channels, the best and effective way is bu using cryptography system. Cryptography is fundamental for securing and protecting private information and other applications of most organization [21].

Cryptography is defined simply as a study for mathematical techniques. The aim of cryptography is providing different services such as confidentiality, authentication, data integrity and non-repudiation [22].

The early version of ElGamal scheme depends on applying Diffe-Hellman which is used for key exchange [23,24]

2. RELATED WORKS

In [25] a new scheme of blind signature was proposed. This scheme depends on ElGamalmethod . In this scheme, when a message is signed different multiple times, the generated corresponding signature wills still the same. This property is an important modification for blind signature in that it provides anonymity to the signature. In order to achieve this goal, the proposed scheme uses both number theory and modular arithmetic techniques. The result of this scheme shows that it is faster than the compared blind signature of RSA.

A paper presented the usage of blind signature to design an electronic voting algorithm using ElGamal signature. This research is based on XML to analyze the security of such scheme. The result of this method shows that it provides a high level of secrecy and can be implemented practically [26].

Using the properties of blind signatures especially blindness and untraceability , a paper proposed two blind signatures based which are untraceable . These blind signatures are based on the difficulty of solving the factoring problem . These types of proposed blind signature are different in traditional blind signatures in that the later schemes are based on the difficulty of solving factoring problem and quadratic residues. The signatures in this paper can fully provide all properties of the standard blind signature [27].

One of the most important applications of a blind signature is the electronic voting. Most blind signatures use an elliptic curve algorithm which it is characterized by the difficulty of solving such an algorithm. This paper presents a new scheme for implementing an electronic voting method in such a way that the elliptic curve algorithm is combined with the blind factor. The aim of this procedure is to scramble the message's content and then it is signed. So , the signer of the message does not what the content of the message is. This scheme is also provide a way to let the voter to vote and authenticate himself/herself [28].

3. PROPOSED SYSTEM

This system generates a new blind signature using El-Gamal Scheme. There are two players used to cooperate for generation the blind signature. The first one is the author of the message named as AM and the other player is the signing authority SA . Each chooses some number. AM chooses a number r and SA chooses a number S. El-Gamal scheme is a public key cryptosystem which is useful to solve the problem of key exchange so it used to bypass the possibility of an intercepted key. The proposed system generates two blind signatures instead of one signature as applied in the traditional blind signature. The players in this system must generate two values. Each value generated by on player is sent to the other player to compute an encryption key. After that the author of the message selects two random numbers K1 and K2as an initial parameters forgeneratingthe two blind signatures. In this step the author of the message uses his/her public key and sends the results to the signing authority that is responsible for producing the blind signatures. The result must include the context of the message and an agreement factor for each calculated result. So , the signing authority must examine the context of each message and the corresponding agreement factor. The context (c) and their agreements factors (ag) for each user (u) are illustrated in table 1. These two blind signatures are sent back to the author of the message who can then remove the blinding factors to reveal the actual signatures sent from signing authority.

Users	Message Context	Agreement
u1	{u1c1,u1c2,…..,u1cn1}	{u1c1ag1, u1c2ag2, …., u1c1agn1}
u2	{u2c1,u2c2,…..,u2cn2}	{u2c1ag1, u2c2ag2, …., u2c1agn2}

. . . um	{umc1,umc2,…..,umcnm}	{umc1ag1, um2ag2, …., um1agnm}

The Algorithm
Let m be the message
Let a be the public base
Let N be the module
Let U be as set of users ; U={u1,u2,…….,un}
Let C be a set of message contexts ;C={c1,c2,….,cm}
Let AG be a set of agreement value ;AG={ag1,ag2,…..,agk}
Let e is a public key
Let d is the private key
A: Step 1(Encryption Key Generation):
1: AM chooses some number r
2: SA chooses another some number s
3: AM computes a^s mod N and sends it to SA
4: SA computes a^r mod N and sends it to AM
5: AM computes the encryption key (eK) by taking SA's number s as following and sends it to SA:
$K=s^r$ mod N
Step 2: (Generating the Blind Signatures)
1: AM chooses two random numbers k1 and k2 .
2: AM generates two encrypted messages using his/her public key (e)as following:

A: $m1 \equiv m(k1)^e$ mod N
B: m11≡ (m1)*eK mod N||Ci||AGi
C: $m2 \equiv m (k2)^e$ mod N
D: m22≡ (m2)*eK mod N ||Ci||AGi
3: AM sends both m11 and m22 to SA
Step 3: SA performs the following steps(generating the two blind signatures s'1and s'2 respectively):
1: SA takes m11 and m22 and he/she generates two blind signatures as following:
2: SA extracts Ci from both m11 and m22 and search for the corresponding agreement factor (AGi) in the table 1. If the AGi is found and authenticated then SA generates s'1 and s'2 , otherwise AM is considered an unauthenticated party.
3: If AGi matches the its context Ci then:
$S'1 \equiv (m11)^d$ mod N
$S'2 \equiv (m22)^d$ mod N
4: SA sends both s'1 and s'2 to AM
Step 4: AM can assure the validity of these signatures by removing the blind factors k1 and k2 as following:
$S1 \equiv s'1.k1^{-1}$ (mod N)
$S2 \equiv s'2.k2^{-1}$(mod N)
RESULTS
Suppose base =7 , N =71 and m=20.
AM chooses r=9 and AS chooses s=11.
1: AM computes a value of base to the power of r :
$B= base^r=7^9$ mod 71= 47
2: This value is sent to AS
3: AS computes:
$A= base^s$ mod 71= 7^{11} mod 71=31
4: This value is sent to AM
5: Generating the encryption key :
A: AM takes the by using the value created by SA as following :

Ke= A^s mod N
Ke=31^{11} mod 71 =52
B: Encryption is performed as following: (the cihpertext here is denoted by C)
C= (Ke*m) mod N
C= (52*20) mod 71= 46 . This C is sent to SA
In order to perform decryption , SA finds 52^{-1} mod 71 = 56
Then he calculates M as following :
M= 56 x 46 mod 71= 20
Step2 (Generating the blind signatures):
We need here to select two prime numbers p and q to generate the public key e and the corresponding private key , d using the RSA scheme.
Let p=11 and q= 7.
N1=pxq=11x7=77.
φ(N1)=(p-1)(q-1)=(11-1)(7-1)=60.
Let e=9
Then d= e^{-1} mod 60= 9^{-1} mod 60= 50
MA selects two random numbers k1=3 and k2=7 such that GCD(K1,N)=1 and GCD(K2,N)=1.
M1≡ m $(k1)^e$ mod N
≡ $20(3)^{13}$ mod 71 =5
Let G1= 2 and AG1=4
M11≡ (m1)*(ek) mod N || G1||AG1
≡ 5* 52 mod 71=47||2||4
M2≡ m$(k2)^e$ mod N
≡2$(7)^{13}$ mod 71= 63
Let G2=3 and AG2=7
M22≡ m2(ek) mod N ||G2||AG2
≡ 63(52) mod 71=10 ||3||7
Generating the two blind signatures S1' and S2' by the SA after extracting G1, G2, AG1 and AG2:
S1'≡ $(M11)^d$ mod N
≡ 47^{37} mod 71= 63
S2' ≡ $(M22)^d$ Mod N
≡ 10^{37} mod 71=

STEP 3 : Recovering the signatures by the MA:
S1≡ S1'. $K1^{-1}$ (mod N)
≡ 63. 3^{-1} mod 71= 21
S2≡ S2'. $K2^{-1}$ (mod N)
≡ 29 . 7^{-1} mod 71= 65

4. CONCOLUSION

This paper presents a new blind signature based on ElGamal scheme. The importance of this scheme is that it generates two blind signatures by using two parameters for the same message .Each content generated by step the author of the message is encrypted by an encrypted key. This key is come from the ElGamal scheme. So this is the first modification that enforces the security of the message and increases the blindness of the message. Another important support of this new scheme is that the author of the message desires to sign his/her message depending on its context. So the signer must check the context of each message sent . Also a corresponding agreement factor is attached to its context .So this method provides most properties of blind signature and it increases the degree of hiding for the message which is a desirable and strong property of perfect blind signatures.

REFERENCES

[1] D.Chaum, Blind signatures for untraceable payments. Advances in Cryptology, Crypto'82, pp.199-203, 1982
[2] S. Han and E. Chang, A pairing-based blind signature scheme with message recovery. Ardil, C. (ed), Sixth International Enformatika Conference (IEC), pp. 303-308, 2005

[3] Shamir A. Identity-based cryptosystems and signature schemes. 1984 International cryptology conference on advances in cryptology, 1984. p. 47–53.
[4] Fan C, Wu L, Huang V. Cryptanalysis on Chen-Qiu-Zheng blind signature scheme. Appl Math Sci 2008;2(16):787–91.
[5] Moldovyan N. Blind collective signature scheme based on discrete logarithm problem. Int J NetwSecur 2010;11(2):106–13.
[6] Pointecheval D, Stern J. Security arguments for digital signatures and blind signatures. J Cryptol2000;13:361–96.
[7] Tripathy A, Parta I, Jena D. Proxy blind signature based on ECDLP. Int J Comp NetwSecur 2010;2(6):93–8.
[8] Popescu C. Blind signature schemes based on the elliptic curve discrete logarithm problem. Stud Inform Control 2010;19(4):397–402.
[9] Moldovyan N. Blind signature schemes from digital signature standards. Int J NetwSecur 2011;12(3):202–10.
[10] CHEN Zhi-ming. An inproved encryption algorithm on ELGamalalgorithm[J]. Computer Applications and Sostware, 2005, 22 (2): 82-85.
[11] Wang Li, Xing Wei, XuGuang-zhong. ElGamalpublickey cryptosystem based on integral quaternions[J]. Computer Applications, 2008,28(5):1156-1157.
[12] Lu Hong-wen, Sun Yu-hua. A Public-key Cryptography Using Integral Quaternions[J]. Journal of Tong Ji University, 2003, 31(12).
[13] HUANG Zhen-jie, WANG Yu-min, CHEN Ke-fei. Generalization and improvement of Nyberg-Rueppel message recovery blind signatures[J]. Journal on Communications, 2005, 26(12): 131-135.
[14] CHEN Hui-yan, LB Shu-wang, LIU Zhen-hua . Identity Based Signature Scheme with Partial Message Recovery [J]. ChineseJournal of Computers, 2006, 29 (9) : 1622- 1627 .
[15] Cao Tian-jie, Lin Dong-dai. Security analysis of a signature scheme with message recovery[J]. Journal of Zhejiang University(Science Edition) , 2006,33 (4) :396～ 397
[16] Kan Yuan-ping. A Signature Scheme with Message Recovery Based on Elliptic Curves[J]. Computer engineering and science, 2010, 32(2):58-59.
[17] Yberg,K.andRueppel,R.A. "message recovery for signature schemes based on the discrete logarithm problem," in EUROCRYPT,1994, 182~193.
[18] Wang Qing-ju, Kang Bao-yuan, Han Jin-guang.. Several New ELGamal Type Digital Signature Schemes and Their Enhanced Schemes[J]. Journal of East China Jiaotong University, 2005, 22(5): 127-138
[19] Zhang Hui-ying, Zhang Jun. Research and Design of an Improved ELGamal Digital Signature Scheme[J]. Computer Engineering and Scinece, 2009, 31(12): 35-38.
[20] Rashmi Singh, Shiv Kumar, "Elgamal's Algorithm in Cryptography", International Journal of Scientific & Engineering Research,2012, Volume 3
[21] AllamMousa,"Security and Performance of ElGamal Encryption Parameter," Journal of Applied Sciences 5, Asian Network foe Scientific Information, 883-886, 2005.
[22] Alfred J Menezes, Paul C van Oorschot, Scot A Vanstone, Handbook of AppliedCryptography, CRC Press, 1997.
[23] TaherElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In G. R. Blakley and D. Chaum, editors, Advances in Cryptology − Proceedings of CRYPTO 84, volume 196 of Lecture Notes in Computer Science, pages 10–18. Springer, 1985.
[24] TaherElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4):469–472, 1985. 9.
[25] E. Mohammed ; A.-E. Emarah ; K. El-Shennaway , A blind signature scheme based on ElGamal signature, Radio Science Conference, 2000.17th NRSC '2000. Seventeenth National
[26] F. Song. , Z. Cui , Electronic Voting Scheme About ElGamal Blind-signatures Based on XML, 2012 International Workshop on Information and Electronics Engineering (IWIEE) , 2012
[27] Cheng-Chi Lee , Wei-Pang Yang , Min-Shiang Hwang, Untraceable blind signature schemes based on discrete logarithm problem , FundamentaInformaticae , Volume 55 Issue 3-4, September 2002 Pages 307 - 320 , IOS Press Amsterdam, The Netherlands, The Netherlands
[28] MS.DHANASHREE M.KUTHE, PROF. AVINASH J. AGRAWAL , IMPLEMENTATION OF BLIND DIGITAL SIGNATURE IMPLEMENTATION OF BLIND DIGITAL SIGNATURE USINGECC ,

International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 5, October 2012 www.ijcsn.org ISSN 2277-5420