New Blind Signature Scheme Based on Modified ElGamal Signature for Secure Electronic Voting

[1]Monira M. khater, [2]Ayman Al-Ahwal, [3]Mazen M.Selim, [4]Hala H. Zayed
[1, 3, 4] *Department of Computer Science, Faculty of Computer & Informatics, Benha University, Benha, Egypt*
[1]monira.khater@fci.bu.edu.eg , [3]Selimm@fci.bu.edu.eg, [4]hala.zayed@fci.bu.edu.eg
[2] *Department of Communication and electronics, pyramid-institute for Engineering and Technology, Egypt, Egypt*
Dr.ayman.hiet@gmail.com

Abstract—The Blind signature is similar to digital signature except that a message is signed by a signer without knowing the content of the message. It is one of the most famous cryptographic techniques in E-voting system (EVS) that guarantee the anonymity of the voters. In this paper, first, we analyze a recently introduced blind signature scheme and show that, the attacker can forge a legitimate signature for any desired message without obtaining the signer's private key. In other words, Mohsen et al.'s blind signature scheme is universally forgeable. Then, a new blind signature scheme based on the discrete logarithm problem (DLP) and the modified ElGamal digital signature is presented. The proposed blind signature scheme meets all properties of blind signature such as correctness, blindness, unforgeability and untraceability. Therefore, the proposed blind signature scheme is more efficient in EVS to ensure voter anonymity, in other words to remove voter's identity from his cast ballot.

Index Terms— Blind signature, Confidentiality, DLP, EVS, Harn digital signature, Unforgeability, Untraceability

1 INTRODUCTION

Recently, Election is a fundamental instrument of democracy that provides an official mechanism for citizens to present their views to the government. In the traditional system, the voting process is quite complex because voter must come personally to cast his vote [1] [2]. This problem resulting low participation rate at elections. Electronic voting system (EVS) can control those problems in national election, by enabled the voter to vote from his home or office or from any remote place.

Although remote EVS is more flexible and easier for voters than the traditional voting, but also it more susceptible than traditional voting due to the nature of digital election data which can be easily spread, tamper within the network, for this reason, may result in widespread fraud and corruption [1]-[3].

A blind signature is a special form of digital signature which allows a party to get another party to sign a message without revealing the content of a message. Compare this to an envelope, containing a piece of carbon paper and a message to be signed. The carbon paper will copy anything written on the envelope to the message, including a signature. Thus, signer can sign the envelope, while the secret message is not known to him. The envelope (the blind) can later be removed, revealing a signed message.

The concept of blind signature is first presented by Dr. Chaum's based on RSA in 1982 [4]. In blind signature scheme, signer use his private key to sign the blind message and anybody can use the signer's public key to check the legitimacy of the signature [5].

A trusted blind signature scheme should meet the following properties [6] [7]:-

Correctness: Anyone can check the validity of the signature of a message signed through the signer by using the signer's public key.

Unforgeability: the signer is the only one can give a valid signature for the associated message, and no one else can achieve any forged signature and pass it through the verification phase.

Blindness: The content of the message should be blinded to the singer to don't allow him to see the content of the message.

Untraceability: Ensure that the signer of message unable to link the message-signature pair after the signature has been disclosed to the public.

Blind signature is one of the most popular protocols in EVS that guarantee secrecy (privacy) of the voter's vote, a voter casts a ballot then blinds a vote using blind factor and sends it to the committee of election. The committee of election then signs the blinded vote after verifying identity of the voter. After receiving the signed ballot, it is unblinded by the voter to get the valid digital signature of the committee of election for the ballot [8].

The digital signature is used to authenticate the voter without discovering the vote's content. The authority is unable to know whom a voter votes for (anonymity property) [8]. In addition to Voter verify the integrity of the ballot by unblinding the ballot and compare it with the original one. In the final election, counting center can check the validity of ballot by using the committee of election's public key to

achieve (Unforgeability property).

This paper propose new blind signature which is based on modified ElGamal signature. ElGamal digital signature shows randomness of k. Thus randomness assures that if the same message is signed twice, the two signatures generated will be different [9]. This scheme will achieve the security requirements of voting process [10]-[12]. In addition to reduction human faults that occurred in the traditional voting process and also reduce the fraud of voting with making the process of voting easier and more flexible for the voters [1].

The rest of the paper is organized as follows: In section II, A brief description of Mohsen et al.'s blind signature, we show a universal forgery attack on this scheme. In Section III, New blind signature scheme based on modified ElGamal signature and its security analysis are presented. In section IV, the experimental results are explained. In the end, conclusions and future work are presented in Section V.

2 CRYPTANALYSIS OF A B LIND SIGNATURE SCHEME

In this section, first we briefly describe a recently introduced blind signature scheme [13], and then propose a forgery attack on this signature.

2.1 Brief Review of Mohsen et al.'s blind signature

In this paper [13], a new blind signature scheme based on DLP and modified ElGamal signature scheme is proposed. ElGamal signature has a significant advantage which is non-deterministic and means that there are many valid signatures for any given message. This scheme is given in five phases as following:

Initialization phase: Signer chooses big prime numbers $p \in Z_p^*$, g is the Primitive root $of\ p \in Z_p^*$, define set of all possible keys$\{(p,g,x,y): g^x = y\ mod p\}$. The values (p,g,y) are public key and x is the private key.

Blinding phase: Requester has a message m and wants to have it signed by the signer, he randomly select (a) as blind factor then blinds the message m as below:

$$m' = (m + h)\ mod\ p - 1 \qquad (1)$$

Then blinded message m' is transmitted to the signer for signing.

Signing phase: Signer select random number k to compute:

$$r = g^{\,k}\ mod\ p \qquad (2)$$

Then, calculate blind signature as below:

$$S' = [(m' - x)y - (r + k)] mod\ p - 1 \qquad (3)$$

Then s' is transmitted to requester.

Unblinding phase: Requester extract the valid digital signature as below:

$$s = s' + hy\ mod\ (p-1) \qquad (4)$$

Then send the message m - signature pair (r,s) to the verifier.

Verification phase: From the public key (p,g,y), verifier check the following equation:

$$g^{my} = rg^{r+s}y^{y}\ mod\ p \qquad (5)$$

To verify the validity of the signer's signature.

2.2 Forgery Attack on Mohsen Mansouri et al.'s Blind Signature

In this section, we analyze the blind signature proposed in [13] and show that without aware the signer's private key, everybody can forge a valid signature on the desired message. Assume an attacker has eavesdropped a valid message/signature $m\ and\ (r,s)$. He can make a valid signature for his own message m', by following these steps:

He can make a valid signature on message m', by following these steps:

Compute blind factor $(f) = m' - m\ mod\ (p-1)$, and $r^{\sim} = rg^{f} = g^{k+\mathrm{f}}\ mod\ p$,then compute $s^{\sim}$ as below:

$$s^{\sim} = s * \left(\frac{r}{r}\right)$$
$$s^{\sim} = [(m' - x)y - (r + k)]$$
$$= [((m + f) - x)y - (r^{\sim} + k + f)$$
$$= [(m^{\sim} - x)y - (r^{\sim} + k + f) mod\ p - 1$$

Finally, the forged signatures$(s^{\sim}, r^{\sim})$ are verified as a valid signature for message m', since the verification equation is satisfied as blow:

$$s^{\sim} = \left(m^{\sim} - x\right)y - (r^{\sim} + k + f)\big)\ mod\ p - 1$$
$$s^{\sim} = m^{\sim}\mathrm{y} - xy - (r^{\sim} + k + f) mod\ p - 1$$
$$m^{\sim}\mathrm{y} = s^{\sim} + xy + (r^{\sim} + k + f) mod\ p - 1$$
$$g^{m^{\sim}y} = g^{s^{\sim}} g^{xy} g^{r^{\sim}} g^{k+f} mod\ p$$
$$g^{m^{\sim}y} = g^{r^{\sim}+s^{\sim}} y^{y}\ \mathrm{r}^{\sim}\ mod\ p$$

So, Mohsen et al.'s scheme is unsecure.

3 THE PROPOSED SCHEME

L. Harn and Y. Xu proposed the modified ElGamal digital signature based on discrete logarithm problem in 1994 [14]. In their research, without loss of generality, they expressed the generalized equation for all modified ElGamal digital signature schemes as $ax = bk + c\ mod\ p - 1$ where(a,b,c) were the three parameters from the set of values (m,r,s). Each parameter could be a mathematical combination of (m,r,s). For instance, the parameter a could be rm or r, etc. The verification equation could be $y^a = r^b g^c mod\ p$. But there are some of restrictions were applied on parameters (a,b,c) for security considerations briefly presented in [14].

The new blind signature derived from the modified version of ElGamal digital signature scheme No.13 (harn scheme) (see Table 1 in [14]).

3.1 Harn digital signature Scheme

A new digital signature scheme based on the discrete logarithm problem is presented by Harn in 1994 [15]. In this algorithm, there is no need to determine the inverse of any parameters which makes the process simpler and also enlarge the search space for the attackers. In addition to it simplifies the signature generation process, speeds up the signature verification process, and it can provide an efficient multi-signature. There were two participants, namely, the signer and the verifier and two phases, namely signing, and verification phases. It was described as follows:

Parameters: p is a large prime number in Galois field Z_p and g is the Primitive root of Z_p, One hash function f and the secret key is $x\ from\ [1, p-1]$ and $gcd\ (x,\ p-1) = 1$. The corresponding public key is $y = g^x\ mod\ p$ and open $p,\ g,\ y$.

Signing: The signer randomly selects $k \in Zp\ from$

$[1, p-1]$, Then the signer computes:

$r = g^k \bmod p$, then compute:

$$s = x(h(m) + r) - k \bmod (p-1) \quad (6)$$

, where m the primitive message and (r, s) is the final signature.

Verifying: If the following equation is correct:

$$rg^s \equiv y^{h(m)+r} \bmod p \quad (7)$$

Then the signature (r, s) is valid, otherwise invalid.

3.2 New Blind Signature Scheme

In this section, new blind signature is proposed which is based on Harn digital signature which is presented in section III.1, The proposed blind signature scheme include three participants namely, the requester, the signer and the verifier. In this scheme, the requester performs the tasks of Blinding and Unblinding, the signer signs the blinded message and the verifier verifies the signature, then accepts or rejects the message. In addition to it consists of five phases. These are: initialization, blinding, signing, unblinding, and verification phases. The signer first publishes the public keys in the initialization phase. In the blinding phase, the user blinds his message then sends it to the signer for asking his signature. Then the signer signs on the blinded message in the signing phase. In the unblinding phase, the user conclude the signature from the blinded signature. Finally, anybody can prove the validity of the signature in the verification phase. The details of the proposed scheme is as follows.

Initialization phase: Signer chooses big prime numbers $p \in Z_p^*$, g is the Primitive root $of\ p \in Z_p^*$ and x randomly as private key $(2 < x < (p-2))$. He calculate $y = g^x \bmod p$ as public key and choose hash function $h(g)$ such as MD5 or SHA-1,then publish p, g, y as public key, but keep the private key x in a secret.

Blinding phase: Requester sends a request to the signer for signing his message m, then Signer chooses random number k to computes $r' = g^k \bmod p$, then sends r' to the requester. Requester randomly chooses two random numbers (a, b) to compute

$$r = r'^a\, g^b \bmod p \quad (8)$$

Then use hash function $h(g)$ to compute his blinded message m'

$$m' = a^{-1}(h(m) + \mathrm{r}) - r' \bmod p - 1 \quad (9)$$

Requester sends m' to the signer.

Signing phase: Signer calculates blind signature as below:

$$s' = x(m' + r') + k \bmod p - 1 \quad (10)$$

Then blind signature s' is transmitted to requester.

Unblinding phase: Requester extract digital signature as below:

$$s = a\, s' + b \bmod (p-1) \quad (11)$$

Then send the message m - signature pair (r, s) to the verifier.

Verification phase: From the public key (p, g, y), Verifier check the legitimacy of the signer's signature as below:

$$g^s = ry^{r+h(m)} \bmod p \quad (12)$$

3.3 Security Analysis

In this section we show that the proposed blind signature scheme is unforgeable based on the difficulty of solving the discrete logarithm problem over a large finite field Z_p^*. Moreover, this blind signature is untraceable, that is the malicious signer of the blind signature is unable to understand who the requester of the corresponding blind signature is.

Our blind signature scheme satisfies all the properties of blind signature namely Correctness, Blindness, Unforgeability, and Anonymity. The security of our scheme is based on both the strength of the hash function and hardness of the DLP in $\boldsymbol{Z_p^*}$

- Correctness: The following steps confirm the verification equation:

$$g^s = ry^{r+h(m)} \bmod p$$

$$\equiv g^{a[x(m'+r')+k]+b}$$
$$\equiv g^{[axm'+axr'+ak]+b}$$
$$\equiv g^{[ax[a^{-1}(h(m)+r)-r']+axr'+ak]+b}$$
$$\equiv g^{[h(m)x+rx-axr'+axr'+ak]+b}$$

$$\equiv \mathrm{r}g^{x(h(m)+r)}$$

- Blindness: The signer cannot obtain the message m from blinded equation $m' = a^{-1}(h(m) + r) - r' \bmod p - 1$, because the signer has two unknown parameters, namely, a and r, so the signature scheme is blind.
- Unforagablility: No one can forge a valid signature pair (r, s) on the message m to pass the verification, because it is very difficult to solve the discrete logarithm problem given $y\ and\ g$, it is impossible to compute x (private key) from$y = g^x \bmod p$.For passing verification equation: $g^s = ry^{r+\mathrm{h}(m)} \bmod p$, The attacker attempt to forge a signature pair of a given message . He attempt to select random integer $\boldsymbol{r'}$ first and then compute the corresponding s'.This difficulty is based on difficulty of solving the DLP. On the other hand, he attempt to randomly select an integer $\boldsymbol{s'}$ first and then compute the corresponding r'. This is also an extremely difficult problem.
- Anonymity: Suppose the malicious signer has kept a set record $\{k'_i, r', m'_i, s'_i\}$for all the blinded messages. When requester reveals $\{m_j, r_j, s_j\}$ in public. The signer unable to own any information from the set of values that he keeps. Because the signer does not know the values including a, b.He cannot link the relationship between the message-signature pair and the blind signature.so the scheme signature satisfies anonymity.

In this paper, Mohsen et al.'s and the proposed scheme were compared in terms of requirements of blind signature namely, correctness, blindness, anonymity and unforgeability. Based on modifications of parameters such as blinding factor, blinded message, blind signature and Signature pair, we find out Mohsen et al.'s blind signature scheme was unsecure, it suffered from universally forgeable Attack. But the proposed scheme satisfied all requirements of blind signature as shown in Table 1.

4 Experimental Analysis

4.1 Experimental Setup

A simulation of the proposed blind signature scheme has been execution, and the computation time requirements for blinding, signing, unblinding and verification operations have been measured. The environment consists of a 1.50 GHz CPU with 4.00GB of RAM running on windows 7 operating system. Programming language is java. It provides socket-based programming through classes in package java.net. Stream socket, which use Transport Control Protocol (TCP) is chosen to provide communication channel between client and server application. TCP protocol offers connection-oriented service, which ensures reliable data delivery.

We generate ElGamal cryptosystem parameters (p, g, x, y) in Table 2. The ElGamal cryptosystem used in Table 2 has a1024 bit prime and a base g with 1024-bit. Sender and receiver data receiving time and travelling time of message is supposed to be negligible i.e. all computation time do not contain the communication time.

4.2 Experimental Results

Table. 3 shows the computation time requirement to handle various operations i.e. blinding, signing, unblinding and verification operations employing the proposed scheme. In this table shows that to blind a message and it requires 78.0ms.Then to sign on the blinded message by the signer, it requires 0.0ms. Then to unblind the signed message by the user, it takes 0.0ms. Finally the verification of the blind signature by the verifier using signer's public key, it requires 47.0ms.

TABLE 1
COMPARISION BETWEEN MOHSEN ET AL.'S AND THE PROPOSED SCHEMES

Prosperities	Mohsen et al.'s scheme	The proposed scheme
Correctness	Yes	Yes
Blindness	Yes	Yes
Unforgeability	No	Yes
Anonymity	Yes	Yes
Blind factors	1	2
Weakness	Universally Forgeable Attack	------
Review security status	Unsecure	Secure

TABLE 2
INITIALIZATION PHASE OF THE PROPOSED SCHEME

p	617805664751386330373921826351983439496525793453554436252719148849974556093287360372153955485080000379125490314379771456651569250078926360495758731281314607567535611498995147712759515994906499126397360979008359500859616330373325392908610442708361025516071292319921852631970737439834951683268311096218188436896832048729
g	288387158440099855742197801114117424640436197764462233792779400501500112440851369933595760898021504770934506525413441459631992301041435909538103265573311932093249675364170239543021893510139163749396924174596060819857012716616315995459147435047477298935505759768601897561174680762175673730060681949820370491389390399999
x	727203556439538144978604757646880197943251977665428591055919064562763584747381081039221140035712887878950847287096650534650920904012517589641885563489185819651019492352573508632821280666735597116204503168547735137192892364943160670987534268934256211987601088824232742759404515218680066661246786215671141343481369448465
y	134513782064551232427890537153805164115963379653180151151923329382415786292487781377516312997047153662981548090253046295962128697971192803206664226791075623932078890112872422322357765314438017693822732115661569584146515277577578262072610513466488278700444290695692541564679394430737944831136729460600018560014900786279

TABLE 3
EXECUTION TIME IN (MILLISECOND) REQUIREMENT BY PROPOSED BLIND SIGNATURE SCHEME FOR A MESSAGE SIZE OF 1055 BITS.

Operation	The proposed scheme
Blinding phase	78.0
Signing phase	0.0
Unblinding phase	0.0
Verification phase	47.0
Total time	125.0

5 Conclusion and Future Work

In this paper, we presented a universal forgery attack on Mohsen Mansouri et al.'s blind signature scheme. Then, we proposed a new blind signature which is based on the hardness of the discrete logarithm problem and the modified ElGamal digital signature. We showed that this scheme is secure. It satisfy all requirements of blind signature namely, correctness, unforgeability, blindness and untraceability. In addition to, it has low computation time requirements of the cryptographic operations involved in different steps of the scheme such as blinding phase, signing phase, unblinding phase and verification phase. Therefore, the proposed blind signature protocol is appropriately efficient in applications like EVS to achieve voter anonymity, in other words to remove voter's identity from his cast ballot, in order to ensure voter privacy.

6 References

[1] RM Kouta, EEF Elfakharany, Proposed Secured Remote E-Voting Model based on Blind Signature, *Global Journal of Computer Science and Technology (GJCST-E)*, 2013. 13(13),p. 2

[2] S Ibrahim, M Salleh, M Kamat, Electronic Voting System: Preliminary Study, *Jurnal Teknologi Maklumat*, 2000.12, pp. 31 - 40.

[3] Ibrahim, S., Salleh, M., & Kamat, M., Design of a Secure Web-Based Electronic Voting System, *Proceedings of Malaysian Science and Technology Congress*, 1999.

[4] D Chaum, Blind signatures for untraceable payments, in Advances in cryptology, Springer US, 1983.

[5] AA Thu, KT Mya, Implementation of an Efficient Blind Signature Scheme, *International Journal of Innovation, Management and Technology*, (2014).5(6), p. 2.

[6] Singh, Nitu, and Sumanjit Das, "A Novel Proficient Blind Signature Scheme using ECC," "*IJCA Proceedings on International Conference on Emergent Trends in Computing and Communication (ETCC-2014)*, 2014.

[7] Singh, Nitu, and Sumanjit Das, "Cryptanalysis of Blind Signature Schemes," *International Journal of Computer Applications*, vol. 71, no.19, 2013.

[8] Ibrahim S, Kamat M, Salleh M, Aziz SR. Secure E-voting with blind signature. *In Telecommunication Technology*, NCTT 2003 Proceedings. 4th National Conference on 2003 Jan 14 (pp. 193-197). IEEE.

[9] AE Emarah, K El-Shennaway, A blind signature scheme based on ElGamal signature.Radio Science Conference"17th NRSC'. IEEE, 2000.pp. C25-1.

[10] Kalaichelvi, V., and R. M. Chandrasekaran, Design and Analysis of Secured Electronic Voting Protocol, *Asian Journal of Information Technology*, 2012 .11(2), pp. 50-55.

[11] HK Abd-alrazzq, MS Ibrahim, Secure internet voting system based on public key Kerberos, International Journal of Computer Science Issues (IJCSI),2012 .9(2), pp.428-434.

[12] CL Chen, YY Chen, JK Jan, A Secure Anonymous E-Voting System based on Discrete Logarithm Problem, *An International Journal of Applied Mathematics & Information Sciences*. 2014. 5, pp. 2571 -2578.

[13] Zaghian A, Mansouri M. A New Blind Signature Scheme Based on Improved ElGamal Signature Scheme. International Journal of Information & Communication Technology Research. 2012 .Dec 30; 4(5):61-5.

[14] L. Harn and Y. Xu, Design of generalized ElGamal type digital signature schemes based on discrete logarithm, *Electronics Letters*, 1994. 30(24), pp. 2025-2026.

[15] L. Harn, "New digital signature scheme based on discrete logarithm", Electronics Letters, 1994. 30(5), pp. 396 - 398.