IJICTR International Journal of Information & Communication Technology Research

ITRC

Volume 4- Number 5- December 2012

Research Note

A New Blind Signature Scheme Based on Improved ElGamal Signature Scheme

Ali Zaghian
Department of Mathematics
Malek-Ashtar university of Technology
Esfahan, Iran.
a_zaghian@mut-es.ac.ir

Mohsen Mansouri
Department of Mathematics
Malek-Ashtar university of Technology
Esfahan, Iran.
mohsen.mlksh@gmail.com

Received: June 2, 2012- Accepted: October 9, 2012

***Abstract*—Blind signature scheme, an important cryptographic primitive, is applicable in protocols that guarantee the anonymity of the participants. This scheme is increasingly used in untraceable payment and electronic voting systems. In this paper we improve ElGamal signature scheme and then we propose a new blind signature based on that. ElGamal signature scheme has an important advantage into RSA signature scheme which is non-deterministic and means that there are many valid signatures for any given message. This property also exists in our new blind signature scheme. Having low computational complexity for signature requester and the signer is one of the advantages of the newly developed scheme and as a result makes it very efficient.**

Keywords: ***digital signature, blind signature, ElGamal digital signature, RSA, electronic payment system, electronic voting system.***

I. INTRODUCTION

A blind signature scheme is a protocol allowing requester to obtain a valid signature for a message from a signer without him or her seeing the message. The concept of blind signature was first introduced by David Chaum [3] in 1983 using RSA system. In this scheme the content of a message is blinded before signing and sent to the signer. The signer signs the blind message using his/her private key and anyone can verify the legitimacy of the signature using signer's public key. A secure blind signature scheme should satisfy the following five requirements [1,10]:

I. *Randomization:* The signer has better injected one or more randomizing factors into the blinded message such that the attackers cannot predict the exact content of the message the signer signs. In a secure randomized signature scheme, a user cannot remove the signer's randomized factor.

II. *Unforgeability*: Only the signer can generate the valid signatures.

III. *Unlinkability*: Only the requester can link a signature protocol to a valid signature.

IV. *Untraceability*: This property ensures that requester is not identified by a signer.

V. *Blindness*: It allows a requester to acquire a signature of a message without revealing anything about the message to the signer.

There were many proposals for blind signature schemes published based on discrete logarithm problems; which one of them is blind signature scheme based on ElGamal suggested by Mohammed et al. [2]that has been proved by Hwang et al. [4], or blind digital signature has been suggested by Camenisch et

al. [6], which is simpler than the scheme proposed by Lee et al. [7].

In this paper we propose a new blind signature scheme based unimproved ElGamal signature which its advantage is that with keeping the same security, it has very low computational complexity and contains simple verification condition. The proposed ElGamal signature scheme has lower computational complexity than the original scheme since we eliminated the inverse operation in signature generation phase. Also, the proposed signature schemes are compared with the counterparts. The remainder of this paper is organized as follows. Section 2describes discrete logarithm problem. Section 3 reviews ElGamal signature scheme. The improvement of ElGamal signature scheme is provided in Section 4. Section 5 proposes a new blind signature based on improved ElGamal signature scheme. Section 6 presents the performance comparisons. Section 7 describes the experimental results. The security analysis is discussed in Section 8 and finally section 9 concludes the paper.

II. THE DISCRETE LOGARITHM PROBLEM

Let G be a cyclic group of order n with a generator α so that$G = \{\alpha^0, \alpha^1, \dots, \alpha^{n-1}\}$. For every$\beta \in G$there is a unique $a \in Z_n$ such that $\alpha^a = \beta$ and a is called the discrete logarithm of β with respect toα. The discrete logarithm assumption states that there exists group G such that computing the discrete logarithm is hard andhence we have the discrete logarithm problem.

III. THE ELGAMAL SIGNATURE SCHEME

The ElGamal signature scheme was described in 1985 by Dr. T. ElGamal. This algorithm is non-deterministic which means that there are many valid signatures for any given message, and the verification algorithm must be able to accept any of these valid signatures as authentic. A short description of this algorithm is given as following:

3.1 Initial phase: Let p be a prime number such that the discrete logarithm problemin Z_p^* is intractable, and let $\alpha \in Z_p^*$ be aprimitive element. Define$K = \{(p, \alpha, a, \beta): \alpha^a = \beta(mod p)\}$ as the set ofall possible keys. The values $(p, \alpha, \beta)$are the publickey, and a is the private key.

3.2 Signing phase: The signer to sign message x, first for $K = \{(p, \alpha, a, \beta)\}$, and fora(secret)random number $k \in Z_{p-1}^*$, defines

$$\begin{cases} sig_k(x, k) = (\gamma, \delta) \\ \gamma \equiv \alpha^k \ mod p \\ \delta \equiv (x - a\gamma) k^{-1} mod (p-1) \end{cases} \quad (3.1)$$

3.3Verification phase: To verify the signature (γ, δ)on x, we observethat

$$Ver(x, (\gamma, \delta)) = true \Leftrightarrow$$

$$\beta^{\gamma} \gamma^{\delta} \equiv \alpha^x \bmod p \quad (3.2)$$

IV. IMPROVEMENT OF ELGAMAL SIGNATURE SCHEME

In this section we improve the original ElGamal signature scheme with removing inverse operation from secret random number $k \in Z_{p-1}^*$.

4.1 Initial phase: See section 3.1

4.2 Signing phase: The signer to sign message x, chooses a(secret)random number $k \in Z_{p-1}^*$ andthen implements following computations.

$$\begin{cases} sig_k(x, k) = (\gamma, \delta) \\ \gamma \equiv \alpha^k \ mod p \\ \delta \equiv [(x - a)\beta - (\gamma + k)] mod (p-1) \end{cases} \quad (4.1)$$

He/she introduces the pair (γ, δ)as signature on message x.

4.3Verification phase: Now anyone can use the signer's public parameters to verify the authentication of the signature (γ, δ) by checking the following equation.

$$Ver(x, (\gamma, \delta)) = true \Leftrightarrow$$

$$\alpha^{x\beta} \equiv \alpha^{(\gamma+\delta)} . \beta^{\beta} . \gamma^{\gamma} \bmod p \quad (4.2)$$

Proof:

From

$$\delta \equiv [(x - a)\beta - (\gamma + k)] mod (p-1)$$

We have

$$x\beta \equiv (\delta + a\beta + \gamma + k) mod (p-1)$$

Thus

$$\alpha^{x\beta} \equiv \alpha^{(\delta + a\beta + \gamma + k)} \equiv \alpha^{\delta} . (\alpha^a)^{\beta} . \alpha^{\gamma} . \alpha^k$$

$$\equiv \alpha^{\delta} . \beta^{\beta} . \alpha^{\gamma} . \gamma \equiv \alpha^{(\gamma+\delta)} . \beta^{\beta} . \gamma^{\gamma} \ (\text{mod } p). \quad \square$$

V. NEW BLIND SIGNATURE SCHEME BASED ON IMPROVED ELGAMAL SIGNATURE SCHEME

In this section we use new ElGamal signature scheme and create a new blind signature scheme. Proposed scheme is given in five phases as following

5.1 Initial phase: See section 3.1

5.2 Blinding message: The requester to blind message x, chooses a blinding factor $A \in Z_p$ and blinds the message $x$as below

$$\bar{x} \equiv (x + A) \bmod (p-1) \quad (5.1)$$

Then the requester sends$\bar{x}$ to signer for signing.

5.3 Signing: The signer uses his/her private key to sign blinded message. i.e., chooses a(secret)random number $k \in Z_{p-1}^*$and then implements following computations.

$$\begin{cases} \gamma \equiv \alpha^k \ mod p \\ \bar{\delta} \equiv [(\bar{x} - a)\beta - (\gamma + k)] mod (p-1) \end{cases} \quad (5.2)$$

Then he/she sends the pair$(\gamma, \bar{\delta})$ to requester.

5.4 Unblinding: The requester extracts the valid signature upon receiving the$(\gamma, \bar{\delta})$as below.

$$\delta \equiv (\bar{\delta} - A\beta) \bmod (p-1) \qquad (5.3)$$

Proof:

We have:

$$\delta \equiv (\bar{\delta} - A\beta) \bmod (p-1)$$
$$\equiv (\bar{x} - a)\beta - (\gamma + k) - A\beta$$
$$\equiv (x + A - a)\beta - (\gamma + k) - A\beta$$
$$\equiv x\beta + \cancel{A\beta} - a\beta - \gamma - k - \cancel{A\beta}$$
$$\equiv (x - a)\beta - (\gamma + k)$$
$$\equiv \delta \bmod (p-1). \qquad \square$$

5.5 Signature verification: Anyone can use the signer's public key to verify whether the signature is genuine. Indeed the signature is valid if:

$$Ver(x, (\gamma, \delta)) = true \Leftrightarrow$$
$$\alpha^{x^{\beta}} \equiv \alpha^{(\gamma+\delta)} . \beta^{\beta} . \gamma \bmod p \qquad (5.4)$$

Otherwise, the signature will be forged.

VI. PERFORMANCE COMPARISON

In general, the security of ElGamal signature scheme is based on the hardness of discrete logarithm problem. In other words, if one finds a solution for this problem, then the signature scheme is breakable and unsecure. However most attention is paid on the improvement of ElGamal signature scheme's computational complexity. The time complexity in original version and newElGamal signature Algorithms is compared in our study. For calculating of the complexity, there are five operations in all phases: addition, subtraction, multiplication, inverse and modular exponentiation. Suppose that p is a ℓ-bit primenumber, and$0 \le x, a, \gamma, \beta, k \le p-1$. It is clearthat addition and subtraction operation of the two numbers inmodular p that lie in interval $[0, p-1]$ are executable in time$O(\ell)$and their multiplication in time$O(\ell^2)$. Also theinverse of a number in modular p in this interval, executes intime(ℓ^3) [11]. Therefore calculating of complexity forδin the original version performs in time$O(\ell) + O(\ell^2) + O(\ell^3) = O(\ell^3)$. That's enough tocalculate the complexity of $\gamma = \alpha^k (modp)$or$\beta = \alpha^a (modp)$. First the complexity of$\gamma = \alpha^k (modp)$should be obtained. Suppose m isthe number of bits in the binary representation of k.I.e.,$k = \sum_{i=0}^{m-1} k_i 2^ifork_i \in \{0,1\}$. Considering thewell-known *square-and-multiply algorithm* [11].It is observed that if$k_i = 1$, two multiplication operations and if$k_i = 0$, only one multiplication operation exist. Then the numberof required modular multiplications to compute $\alpha^k (modp)$is at most $2m$. Moreover, every multiplication operation requiresthe time$O((logp)^2)$, where $log\, p$the length of is bits inthe binary representation of$p$. So, the maximum required timecomplexity is$(2m(logp)^2)$. Now, if ℓbe the binarylength of p, we have$m < l$, because $k < p$ such that$\ell = logp$. Hence required time complexity for calculating $\alpha^k \ modp$ is$O(\ell^3) = O((logp)^3)$. Similarly the timecomplexity forcalculation of $\beta = \alpha^a (modp)$is$O(\ell^3)$.

Suppose $T_1$and T_2be the time complexity of original and improved ElGamal signature schemes, respectively. The results are summarized in Table **1**. Since we removed the inverse operation in signing phase it can be seen that $T_2 < T_1$.

Table 1 Time Complexity of Original and New ElGamal Signatures.

Complexity	Initial Phase	Signing Phase	Verification Phase
T_1	$O(\ell^3)$	For γ: $O(\ell^3)$ For δ: $O(\ell) + O(\ell^2) + O(\ell^3) = O(\ell^3)$	$O(\ell^3)$
T_2	$O(\ell^3)$	For γ: $O(\ell^3)$ For δ: $O(\ell) + O(\ell^2) = O(\ell^2)$	$O(\ell^3)$

Also letT_1' be the time complexity of Elsayed blindsignature scheme [5] (which is the most similar scheme to theproposed one) and T_2' be the time complexity of new ElGamalsignature scheme. Table **2**compares the time complexities. It is clear that our method are performs Essayed blind signature scheme.

Table 2 Time Complexity of Elsayed and New Blind Signatures.

Complexity	Blinding Message	Blind Signature	Unblinding
T_1'	$O(\ell^2)$	$O(\ell^3)$	$O(\ell^3)$
T_2'	$O(\ell)$	$O(\ell^2)$	$O(\ell^2)$

VII. EXPERIMENTAL RESULTS

Our new signature schemes are implemented using the C/C++ MIRACLLIBRARY [12]. All experiments are carried out in a 32 bit operating system with 2.00GB installed memory and a process or dual-core CPU 5300. We choose ElGamal cryptosystem parameters in Table **3**[16]. The ElGamal cryptosystem used in Table **3** has a1024 bit prime, a base $\alpha$with 512-bit order$n$.

Table 3 ElGamal Parameters.

p	11838184372471710174946159675664648223090589766046312362456039456380760993395604226539234152095602888644631771664207057053879231168634640942410140411181283316085659935320027832070906986302148069534969208735860164025083645711880093251235268088221149165473251353285154670278619087767951265337570934555271330240 1
α	10438851351172103101582226926949477575301310922887591959044719238066480611925670159164484130618566553957172065131510914771071115423095329962224676443129529
a	59660846376012012299732062167070449913568079369759726390943366472735655747125035179031089451125540857538031073871730574393537580324435989370818322776711385170287961641652843108956199416275969391836776116950834964228187667553031050881716218984733944262206823833143460937854518070649325296332195764146328701846
n	10643279190065436658189986618064406421644965048931123759059399961267188560280838103148616561846017372648276481588281249312389181981519220200679285520165533

Also Elapsed time in microsecond for all phases of signature schemes summarized in Table **4** and Table **5**.

Table 4 Elapsed time (µs) for computation of Original and New ElGamal Signature Schemes.

Complexity	Initial Phase	Signing Phase	Verification Phase
T_1	**3740**	**25000**	**16000**
T_2	**3740**	**15000**	**16300**

Table 5Elapsed time(µs) for computation of Elsayed Blind and New Blind Signature Schemes.

Complexity	Blinding Message	Blind Signature	Unblinding
$T_1^{'}$	**22**	**25000**	**20000**
$T_2^{'}$	**12**	**15000**	**940**

VIII. SECURITY DISCUSSION

In this section, we discuss some security properties of our proposed Blind Signature scheme. Precisely, we mainly focus on the properties of blindness, enforceability, intractability and unlink ability.

8.1 Blindness: Blindness is the main property of a blind signature, which ensures both the user privacy and data authenticity. Observe the issuing protocol, the requester picks a blind factor $A \in Z_p$ to compute the blindedmessage $\bar{x} = (x + A)mod(p-1)$ and sends it to signer. Asthe blind factor A is randomly chosen and kept secret only bythe requester, the signer cannot get the message x from blinded message $\bar{x}$. Therefore, the property of blindness can be satisfied.

8.2 Unforgeability: The security of our scheme is based on the difficulty of solving the discrete logarithm problem. No one can forge a valid signature pair(γ, δ) on messages x to pass the verificationcondition in equation$\alpha^{x\beta} \equiv \alpha^{(\gamma+\delta)}.\beta^{\beta}.\gamma(modp)$, because it is very difficult to solvethe discrete logarithm problem [6, 13-15].

8.3 Untraceability: It is obviously that the signer cannot trace the blind signature. Because he/she does not know the blind factor A in$\bar{\delta} \equiv [(\bar{x} - a)\beta - (\gamma + k)]mod(p-1)$such that $\bar{x} = (x + A)mod(p-1)$. Therefore, without the knowledge of the secure number$A$, the signer cannot trace theblind signature and so the requester is not identified by a signer.

8.4 Unlinkability: Only the requester can link a signature protocol to a valid signature. Because only the requester enables to blind x according toequation $\bar{x} = (x + A)mod(p-1)$ and to unblind$\bar{\delta}$using equation$\delta = (\bar{\delta} - A\beta)mod(p-1)$. Therefore the property of unlink ability can be satisfied.

IX. CONCLUSION

In this paper the original ElGamal signature was improved to a better signature scheme. Then, according to our new ElGamal signature scheme a new blind signature scheme was introduced in which it has the least computational complexity. Therefore, our new blind signature protocol is appropriately efficient in applications like electronic payment and electronic voting systems[8,9] and to protect the privacy of customers or voters.

ACKNOWLEDGEMENT

This research was financially supported in part by a grant received from Iranian Telecommunication Research Center (ITRC).Additionally the authors would like to thank the anonymous reviewers and referees of this paper for their helpful comments.

REFERENCES

[1] Huang, H-F, and Chang."A new design of efficient blind signature scheme". *The Journal of Systems and Software*, 73,397-403, 2004.

[2] E. Mohammed, A. E. Emarah, and K. El-Shennawy."A blind signatures scheme based on ElGamal signature".*IEEE/AFCEA EUROCOMM 2000 Information Systems for Enhanced Public Safety and Security*, pp.51-53, 2000.

[3] D. Chaum. "Blind signatures for untraceable payments". *Advances in Cryptology. CRYPTO 82*, pp. 199-203, 1982.

[4] Min-Shiang Hwang and Yuan-Liang Tang Yan-Chi Lai. "A Blind Signature Scheme Based on ElGamal Signature". *Technical Report CYUT-IM-TR- 2001-010, CYUT*. Aug. 2001.

[5] E.Mohammed, A.E.Emrah, K.El-shennawy. "A blind signatures scheme based on Elgamal signature".*in IEEE/AFCEA EUROCOMM 2000 information Systems for Enhanced Public Safety and Security*, pp.51-53, 2000.

[6] J. L. Camenisch, J. M. Piveteau and M. A. Stadler."Blind Signatures Based on the Discrete Logarithm Problem". *Advances in Cryptology- EUROCRYPT'94, Rump session*, pp. 428-432, 1994.

[7] C. C. Lee, M. S. Hwang and W. P. Yang. "A New Blind Signature based on the Discrete Logarithm Problem for Untraceability". *Applied Mathematics and Computation*, vol., pp.837-841, May 2005.

[8] A.Fujioka, T.Okamoto, and K.Ohta. "A practical secret voting scheme for large scale elections". *In Advances in Cryptology - AUCRYPT 92 Proceedings*, Springer, 15-19, 1993.

[9] C.I. Fan. "Ownership-attached unblinding of blind signatures for untraceable electronic cash" .*Information Sciences*, vol. 176. No. 3, pp. 263-284, 2006.

[10] 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.

[11] Stinson, D. R. "Cryptography Theory and Practice". 3rd edition. CRC Press, Inc., pp. 175,176,177, 2005.

[12] Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL). URL: http://indigo.ie/~mscott.

[13] T. ElGamal. "A public-key cryptosystem and a signature scheme based on discrete logarithms". *IEEE Transactions on Information Theory IT-31*. (July) 469–472. 1985.

[14] M.-S. Hwang, C.-C. Chang, K.-F. Hwang. "An ElGamal-like cryptosystem for enciphering large messages". *IEEE Transactions on Knowledge and Data Engineering*. 14 (2) 445– 446. 2002.

[15] M.-S. Hwang, C.-C. Lee, E.J.-L. Lu."Cryptanalysis of the batch verifying multiple DSA-type digital signatures". *Pakistan Journal of Applied Sciences.* 1 (3) 287–288. 2001.

[16] Allen, Bryce D."Implementing several attacks on plain ElGamal encryption". *Graduate Theses and Dissertations*. Paper 11535. 2008. http://lib.dr.iastate.edu/etd/11535.

Ali Zaghian was born in Isfahan, Iran in 1959 and received his B.Sc. degree in mathematics from Isfahan University, and his M.Sc. and Ph.D. degrees respectively in mathematics and cryptography-mathematics from Tarbiat Moalem University, Tehran, Iran, in 2008. He is currently assistant professor in Cryptography-Mathematics Department of Malek-Ashtar University of Technology (MUT), Isfahan, Iran. His research interests include Coding and cryptography algorithms.

Mohsen Mansouri was born in Isfahan, Iran in Oct the 16th in 1982 and received his B.Sc. degree in applied mathematics from Isfahan University, in 2008, and his M.Sc. degree in cryptography-mathematics from Malek-Ashtar University of Technology (MUT), Isfahan, Iran, in 2011. His research interests include public-key cryptosystems, with a focus on elliptic curve cryptography (ECC), blind signatures and authentication protocols.