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.mlks@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 2 describes discrete logarithm problem. Section 3 reviews ElGamal signature scheme. Section 4 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 $\alpha$ so that $G = \langle \alpha^n \rangle$. For every $\beta \in G$ there is a unique $a \in \mathbb{Z}_n$ such that $\alpha^a = \beta$ and $\alpha$ is called the discrete logarithm of $\beta$ with respect to $\alpha$. The discrete logarithm assumption states that there exists group $G$ such that computing the discrete logarithm is hard and hence 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 problem in $\mathbb{Z}_p^*$ is intractable, and let $\alpha \in \mathbb{Z}_p^*$ be an primitive element. Define $K = \langle (p, \alpha, a, \beta) : \alpha^a = \beta \pmod{p} \rangle$ as the set of all possible keys. The values $(p, \alpha, \beta)$ are the public key, and $a$ is the private key.

3.2 Signing phase: The signer to sign message $x$, first for $K = \langle (p, \alpha, a, \beta) \rangle$, and for a (secret) random number $k \in \mathbb{Z}_p^*$, define

\[
\begin{align*}
\text{sig}_x(x, k) &= (\gamma, \delta) \\
\gamma &= \alpha^k \pmod{p} \\
\delta &= (x - \alpha^k) \cdot k^{-1} \pmod{(p - 1)}
\end{align*}
\]

3.3 Verification phase: To verify the signature $(\gamma, \delta)$ on $x$, we obserber that

\[
\begin{align*}
\text{Ver}(x, (\gamma, \delta)) = \text{true} & \iff \\
\beta^\gamma & = \alpha^\delta \pmod{p}
\end{align*}
\]
5.4 Unblinding: The requester extracts the valid signature upon receiving the $(\gamma, \delta)$ as below.

$$\delta = (\overline{\delta} - A \beta) \mod (p - 1) \quad (5.3)$$

*Proof:*

We have:

$$\delta = (\overline{\delta} - A \beta) \mod (p - 1)$$

$$\equiv (\overline{x} - a \beta) \mod (p - 1)$$

$$\equiv (x + \overline{\alpha} - a) \beta - (\gamma + k) - \overline{\alpha} \beta$$

$$\equiv (x - a) \beta - (\gamma + k)$$

$$\equiv \delta \mod (p - 1).$$

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:

$$\text{Ver}(x, (\gamma, \delta)) = \text{true} \iff\alpha^{\gamma \delta} = \alpha^{(\gamma + \delta) \beta \gamma} \mod p \quad (5.4)$$

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 insecure. However, most attention is paid on the improvement of ElGamal signature scheme's computational complexity. The time complexity in original version and new ElGamal 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 $\ell$-bit primenumber, and $0 \leq x, a, y, b, k \leq p - 1$. It is clear that addition and subtraction operation of the two numbers in modular $p$ that lie in interval $[0, p - 1]$ are executable in time $O(\ell)$ and their multiplication in time $O(\ell^2)$. Also the inverse of a number in modular $p$ in this interval, executes in time $O(\ell^2)$ [11]. Therefore calculating of complexity for the original version performs in time $O(\ell^2) + O(\ell^2) + O(\ell^2) = O(\ell^3)$. That's enough to calculate the complexity of $\gamma = \alpha^{\gamma \delta} \mod p = \alpha^{a^\ell (\mod p) \mod b}$. First the complexity of $\gamma = \alpha^{a^\ell (\mod p) \mod b}$ should be obtained. Suppose $m$ is the number of bits in the binary representation of $k$. i.e., $k = \sum_{i=0}^{m-1} k_i 2^i$, for $k_i \in \{0, 1\}$. Considering the well-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 number of required modular multiplications to compute $\alpha^{\ell (\mod p) \mod b}$ is at most $2m$. Moreover, every multiplication operation requires the time $O((\log p)^2)$. Therefore, the maximum required time complexity is $(2m(\log p)^2)$. Now, if $\ell$ be the binary length of $p$, we have $m < \ell$, because $k < p$ such that $\ell = \log p$. Hence required time complexity for calculating $\alpha^\ell \mod p = O(\ell^3)$. Similarly the time complexity for calculation of $\beta = \alpha^{a^\ell (\mod p) \mod b}$ is $O(\ell^3)$.

Suppose $T_1$ and $T_2$ be 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>
<thead>
<tr>
<th>Complexity</th>
<th>Initial Phase</th>
<th>Signing Phase</th>
<th>Verification Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_1$</td>
<td>$O(\ell^3)$</td>
<td>$O(\ell^3)$</td>
<td>$O(\ell^3)$</td>
</tr>
<tr>
<td>$T_2$</td>
<td>$O(\ell^3)$</td>
<td>$O(\ell^3)$</td>
<td>$O(\ell^3)$</td>
</tr>
</tbody>
</table>

Also let $T_1'$ be the time complexity of Elsayed blind signature scheme [5] (which is the most similar scheme to the proposed one) and $T_2'$ be the time complexity of new ElGamal signature scheme. Table 2 compares the time complexities. It is clear that our method are performs Elsayed blind signature scheme.

<table>
<thead>
<tr>
<th>Complexity</th>
<th>Blinding Message</th>
<th>Blind Signature</th>
<th>Unblinding</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_1'$</td>
<td>$O(\ell^3)$</td>
<td>$O(\ell^3)$</td>
<td>$O(\ell^3)$</td>
</tr>
<tr>
<td>$T_2'$</td>
<td>$O(\ell^3)$</td>
<td>$O(\ell^3)$</td>
<td>$O(\ell^3)$</td>
</tr>
</tbody>
</table>

VII. EXPERIMENTAL RESULTS

Our new signature schemes are implemented using the C/C++ MIRACL LIBRARY [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 a 1024 bit prime, a base $\alpha$ with 512-bit ordem.
the message $x$ from blinded message $\tilde{x}$. 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 $(\tilde{y}, \delta)$ on messages $x$ to pass the verification condition in equation $\psi^\delta \equiv (\tilde{y} + \alpha \beta) \mod (p-1)$, because it is very difficult to solve the 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 $A \in \mathbb{Z}_p$ such that $\tilde{x} = (x + A) \mod (p-1)$. Therefore, without the knowledge of the secure number $A$, the signer cannot trace the blind 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 to equation $\tilde{x} = (x + A) \mod (p-1)$ and to unblind $\tilde{x}$ using equation $\delta = (\tilde{y} - \alpha \beta) \mod (p-1)$. Therefore the property of unlink ability can be satisfied.

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 $A \in \mathbb{Z}_p$ to compute the blinded message $\tilde{x} = (x + A) \mod (p-1)$ and sends it to signer. Asthe blind factor $A$ is randomly chosen and kept secret only by the requester, the signer cannot get

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

<table>
<thead>
<tr>
<th>Complexity</th>
<th>Initial Phase</th>
<th>Signing Phase</th>
<th>Verification Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_1$</td>
<td>3740</td>
<td>25000</td>
<td>16000</td>
</tr>
<tr>
<td>$T_2$</td>
<td>3740</td>
<td>15000</td>
<td>16300</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Complexity</th>
<th>Blinding Message</th>
<th>Blind Signature</th>
<th>Unblinding</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_1'$</td>
<td>22</td>
<td>25000</td>
<td>20000</td>
</tr>
<tr>
<td>$T_2'$</td>
<td>12</td>
<td>15000</td>
<td>940</td>
</tr>
</tbody>
</table>

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


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.