BIOINFO Security Informatics
ISSN: 2249-9423 & E-ISSN: 2249-9431, Volume 2, Issue 2, 2012, pp.-66-68.
Available online at http://www.bioinfo.in/contents.php?id=344

PROCESSING A NEW BLIND SIGNATURE BASED ON ELGAMAL

DAMERI A.[1]* AND BOOSTANI R.[2]

[1]IT Masters, Electronic Collage, Shiraz University, Shiraz- 71454, Iran.
[2]Science & Computer Department, Shiraz University, Shiraz- 71454, Iran.
*Corresponding Author: Email- amirdameri@yahoo.com

Received: September 18, 2012; Accepted: December 12, 2012

Abstract- One of the main challenges of blind signature algorithms is their high computational complexity. In order to overcome this problem, a novel scheme is proposed which is a modified version of Elgamal digital signature. Moreover, this algorithm guarantees a high security during the signing process.

Keywords- RSA, Elgamal, Blind signature, Digital signature

Citation: Dameri A. and Boostani R. (2012) Processing a New Blind Signature Based on ElGamal. BIOINFO Security Informatics, ISSN: 2249 -9423 & E-ISSN: 2249-9431, Volume 2, Issue 2, pp.-66-68.

Introduction

Blind signature is a kind of digital signature that should have some properties such as enforceability, unlikability and untracibility [13]. The enforceability provides the signer to be the only one who produces a valid sign. The unlikability property forms the sign such that only the requester can make a relation between the protocol and sign. Also, blind signature should have the untracibility property which assures the requester not being tracked by the signer. Blind signature algorithms are used in many applications such as E -voting [5,11], E-payment [6, 7] and the data base security [2]. In this paper a new blind signature is offered to reduce the complexity of signing process. The proposed scheme is also provide a high security during the process. The first blind signature was presented by Chaum, et al. [1] And was based on Rivest, Shamir, Adleman (RSA) digital signature which suffered from chosen plain text attack. From another side, Elgamal [3] proposed a digital signature which is still a state of art algorithm for cryptography. Then, Alseyyed, et al. [8] offered a new blind signature based on Elgamal digital signature which has been attacked and lost its security. Ibrahim, et al. [10] Presented an E-voting system based on blind signature. In their system, voter's privacy is guaranteed by using both blind and digital signatures to increase the authentication and confidentiality. Xenakis, et al. [9] Explore the security related procedures that are required for the successful development and deployment of electronic voting in legally-binding government elections. In view of the increased complexity of the e-voting processes which can involve multi-channel e-voting options and the increase in the number of agents involved in the administration of E-elections. They relate procedural security to the need for transparent allocation of responsibilities among the different agents and used a blind signature to gain that. Jena, et al. [12] Presented a novel Blind Signature Scheme (BSS) based on Nyberg-Rueppel Signature Scheme (NRSS) using Elliptic Curve Discrete Logarithm Problem (ECDLP). This algorithm is employed in off line digital cash payments [12] which can be easily extended to E-voting application. Cetinkaya, et al. [13] formal definitions of security requirements for cryptographic voting protocols (privacy, eligibility, uniqueness, fairness, receipt-freeness, accuracy, and individual verifiability) were provided, and elaborate checklists for each requirement were presented. The Voting problem is clearly defined in terms of security requirements. The voting problem arises from the trade-off between receipt-freeness and individual verifiability. His research suggests the Predefined Fake Vote scheme as an applicable solution to overcome the voting problem [13].

Furthermore, Junjie, et al. [14] Illustrated a new identity-based proxy blind signature scheme which satisfies unforgeability, nonrepudiation, blindness, unlinkability and other security requirements of proxy blind signatures and produced less traffic [14].

Here, a new algorithm is designed based on Elgamal method to improve the security and complexity of blind signature. As follow in the second part Elgemal digital signature and Elsayed Blind signature will be explained; in the Third part a modified new digital signature based on Elgemal Digital signature will be represented and using that a new blind signature shall be offered and would be analyzed.

Elgamal Digital and Blind Signature

In this part Elgamal Digital Signature [3] will be described and base on that the Elsayed Blind Signature will be represented which is covered by Elgamal digital signature.

Elgamal Digital Signature

Elgemal digital signature was presented in 1985 for the first time. This scheme is a non-deterministic model which means a data can have many different signs. In this way, first a prime number p and a generator value $\alpha(\alpha \in Z_p^*)$ are chosen. The other parameter of the Elgamal algorithm is $\beta \equiv \alpha^a \bmod p$ which (α, β, p) are the public keys and α is a primary key.

Signing

For signing a data like x, first $k\,(k \in Z_{p-1}^*)$ is randomly chosen and the signing process is preformed as $Sig_k(x,k) = (\gamma, \delta)$ which (γ,δ) are defined as follows:

$$\delta \equiv (x - a\gamma)k^{-1} \bmod p - 1 \qquad (1)$$

$$\gamma \equiv \alpha^k \bmod p \qquad (2)$$

Where (a,k) are signer's private keys and (δ,γ) are the signs of the data.

Verifying

To confirm a verifier, the following process should be carried out. If the equation $\beta^\lambda \gamma^\delta \equiv ?\alpha^x$ works properly, then the verifier approves the sign unless it is not a valid sign.

Elsayed Blind Signature

Elsayed,, et al. [8] proposed a blind signature schemes which are based on Elgamal signature. There are three phases in their schemes explained as follows:

Initialization Phase

The requester chooses two random numbers *k* and *h* such as that $\gcd(k, p-1) = 1$ and $\gcd(h, p-1) = 1$ where *p* is a large prime number. Next, the requester computes $r = g^k \bmod p$ and $m' = hm$ where *g* is a primitive element of *p*. Finally, the requester sends m' to the sign -er to be signed.

Signing Phase

After receiving the blind data the (m'), signer generates a blind signature s' from m' such that:

$$s' = k^{-1}(m' - xr) \bmod (p-1) \qquad (3)$$

Unblinding Phase

The requester receives the message *m* and its signature *s* which is signed by the signer as follows.

$$m = h^{-1}m' \bmod (p-1) \qquad (4)$$

$$s = xrk^{-1}(h^{-1} - 1) + h^{-1}s' \bmod (p-1) \qquad (5)$$

A verifier can validate the message *m* and signature (r,s) using the following equation.

$$g^m = y^r r^s \bmod p \qquad (6)$$

In Elsayed schemes, the parameter *k* is chosen randomly and *r* is computed by the requester. When the requester received the blind signature s', due to the parameter *r, k,* s' and *m'* are known to the requester. The requester can derive the signer's privacy key *x* from s' as follows.

$$s' = k^{-1}(m' - xr) \bmod (p-1) \Rightarrow x = r^{-1}(m' - s'k) \bmod (p-1) \quad (7)$$

The requester can make a counterfeit signature with signer's private key. Therefore, Elsayed blind signature scheme is insecure.

A New Digital and Blind Signature

In this part two novel algorithms are presented. The proposed schemes can be considered as a modified version of Elgamal signature.

New Digital Signature

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.

Signing

To sign the data x, first $k \in Z_{p-1}^*$ is chosen randomly such as Elgamal signing process but (δ,γ) are defined differ from Elgamal's one. In the proposed algorithm the δ,γ are determined as follows:

$$\delta \equiv (x - (a + k))\gamma \bmod p - 1 \qquad (8)$$

$$\gamma \equiv \alpha^k \bmod p \qquad (9)$$

So (a,k) are the signer's private keys and (δ,γ) are the signs for *x*.

Verifying

If the following equation is satisfied, a verifier accepts the sign for the data

$$\alpha^{\gamma x} \equiv \alpha^\delta (\beta\gamma)^\gamma \bmod p \qquad (10)$$

Proof: $\alpha^{\gamma x} \equiv \alpha^\delta (\alpha^a \alpha^k)^\gamma \equiv \alpha^{\delta + \gamma(a+k)} \bmod p$
$\Rightarrow \gamma x \equiv \delta + \gamma(\alpha + k) \bmod p - 1$

Such that:

$$\delta \equiv (x - (a + k))\gamma \bmod p - 1 \qquad (11)$$

New Blind Signature Scheme

By using the above digital signature, in this part, a novel blind signature is proposed which not only increase the security but also decrease the complexity of calculation in blind signature. To prove the scheme mathematically, four phases should be considered; blinding, signing, unblinding, verifying

Blinding

Consider a requester blinds the data as below by choosing $h \in z_p$ randomly

$$\bar{x} \equiv x + h \bmod p - 1 \qquad (12)$$

Where $\bar{x}$ is the blind message and *h* is a random factor. Finally $\bar{x}$ is sent to the signer.

Signing

The signer receives $\bar{x}$ and chooses a random number $k(k \in Z_{p-1}^{*})$ to calculate $\bar{\delta}$:

$$\bar{\delta} \equiv (\bar{x} - (a+k))\gamma \bmod p-1 \tag{13}$$

$$\gamma \equiv \alpha^{k} \bmod p \tag{14}$$

Then the signer sends $(\bar{\delta}, \gamma)$ as a blind signature to the requester.

Unblinding

In this step the requester generates the digital signature (δ) from the blind signature $(\bar{\delta})$ which he received from the signer as follows:

$$\delta \equiv \bar{\delta} - \gamma h \bmod p-1 \tag{15}$$

Where (δ, γ) are the signatures for *x*.

Proof:
$$\begin{aligned} \delta &\equiv \bar{\delta} - \gamma h \equiv \gamma(\bar{x} - (a+k)) - \gamma h \\ &\equiv \gamma(x+h) - \gamma(a+k) - \gamma h \\ &\equiv \gamma(x - (a+k)) \bmod p-1 \end{aligned}$$

Verifying

The verifying is done by the following formula:

$$\alpha^{\gamma x} \equiv \alpha^{\delta}(\beta\gamma)^{\gamma} \bmod p \tag{16}$$

Analyses

Compare to Chaum signature scheme, the proposed blinding phase has less computational complexity and is much faster because only an adding operator is employed while RSA blind signature need a powering and a multiplying operators. The verifying phase of the proposed blind signature is slower than Chaum's blind signature consequently; run time of the proposed algorithm is slower than that of the Chaum. Nevertheless, the essential need of a blind signature is its security which Chaum blind signature suffers from the chosen plain text attack while the proposed blind signature is robust to the mentioned attack. The converted DDS [4] blind signature unblinding stage contains multiplying, exponential function and an inverted operator while the proposed algorithm just uses multiplying and adding operators. Beside the algorithm does not need to invert the factor *k* or any other parameters which means every number can be used for all parameters which makes it harder to be attacked. The new blind signature has just five operating stages which makes it a low computational cost algorithm compare to its rivals. In addition of low computational cost, it has a high security which has been taken form ElGamal mathematics. Therefore, this algorithm can be used as a safe algorithm in e-voting and e-payment protocols because of its simplicity and high security properties.

References

[1] Chaum D., Fiat A. and Naor M. (1992) *Advanced in Cryptology, -CRYPT*0'88, Springer-Verlag.

[2] Chaum D. and Pedersen T.P. (2003) *Advanced in Cryptrology-CRYPT*0'92, 89-105.

[3] Elgamal T. (1995) *IEEE Transactions on Information Theory*, IT -31(4), 469-472.

[4] Camenisch J.L., Piveteau J.M., Stadler M.A. (2004) *Advanced in Cryptology Eurocrypt*, 94, Perugia, Italy, 428-432.

[5] Fujioka A., Okamoto T. and Ohta K. (2004) *A Practical Secret Voting Scheme for Large Scale*.

[6] Fan C.I. and Lei C.L. (2002) *Journal of Network and Computer Applications*, 25(2), 93-107.

[7] Fan C.I. (2006) *Information Sciences*, 176(3), 263-284.

[8] Elsayed Mohammed A.E. Emarah and Kh. El-Shennawy (2000) *Information Systems for Enhanced Public Safety and Security IEEE/AFCEA*, 5153.

[9] Xenakis A., Macintosh A. (2004) 37*th Annual Hawaii International Conference on System Sciences*.

[10] Ibrahim S., Kamat M., Salleh M., Aziz (2003) 4*th National Conference on Telecommunication Technology*.

[11] Jinn-Ke Jan, Yu-Yi Chen, Yi Lin (2001) 35*th International Carnahan Conference on Security Technology*, IEEE.

[12] Jena D., Jena S.K., Majhi B. (2007) 10th *International Conference Information Technology*.

[13] Cetinkaya O. (2008) *Third International Conference on Availability, Reliability and Security*.

[14] Junjie He, Chuanda Qi, Fang Sun (2012) *International Conference Information Science and Technology*.