International Journal of Cryptology Research 1 (1): 1-9 (2009)

A New Blind Signature Scheme Based On Factoring and Discrete Logarithms

N. M. F. Tahat, E. S. Ismail and R. R. Ahmad
School of Mathematical Sciences, Faculty Science and Technology
University Kebangsaan Malaysia
43600 UKM, Bangi, Selangor, Malaysia
Email: nidal730@hotmail.com

ABSTRACT

Blind signature scheme, an important cryptographic primitive, is useful in protocols that guarantee the anonymity of the participants. Most of the developed blind signatures are based on a single hard problem. If one finds a solution to this problem then the blind scheme is breakable. In this paper, we presented a new blind signature scheme based on factoring and discrete logarithms. This kind of scheme provides a longer or higher security than that scheme based on a single hard problem. This is due the impossibility of attackers to solve two hard problems simultaneously. Some possible attack have also been considered and we showed that the scheme secure from those attacks. The newly developed scheme also has the advantage of having low-computational complexity for the signature-requester and the signer, thus makes it very efficient.

INTRODUCTION

A blind signature scheme is a protocol allowing recipient to obtain a valid signature for a message, m from a signer without him or her seeing the message or its signature. If signer sees m and its signature later, he or she can verify that the signature is genuine but unable to link the message-signature pair to the particular instance of the signing protocol which has led to this pair. The concept of a blind signature scheme was first developed by (Chaum, 1983). It allows realizing secure electronic payment systems (Chaum, 1989; Chaum et al. 1989) or voting systems (Chaum et al. 1988; Okamoto and Ohta, 1991) protecting customer's or voter's privacy as well as other cryptographic protocols protecting the participants anonymity. There were many proposals for blind signature schemes published based on a single hard problem such as factoring (fac) or discrete logarithm (dl) problems (Huang and Chang, 2004; Camenisch et al. 1994). These proposals one day in a near future will no longer be secure if one finds a solution for the underlying hard problem. In this paper, we designed a new blind signature scheme based on two hard problems namely factoring and discrete logarithms. This scheme definitely provides a longer and higher security than that blind scheme based on a single hard problem. This is due to the impossibility of attackers to solve the two hard problems simultaneously.

BRIEF REVIEW OF A NEW SIGNATURE SCHEME

To design the new blind signature scheme, we first introduce an ordinary signature scheme as a basic structure of our developing blind signature scheme. We need the following notations and parameters to describe the process of this basic structure: $h(\cdot)$ is a cryptographic hash function whose output is a *t*-bit length and assume $t = 128$. A number p is a large prime and n a factor of $p-1$ is the product of two safe prime (contains no small prime divisors) and $\phi(n)$ is a phi-Euler function. An integer g is a primitive element in $Z_p^* = \{1, 2, ..., p-1\}$ with order n satisfying $g^n \equiv 1 \pmod{p}$ and let $\gcd(a, b)$ be the greatest common divisor of a and b. Now we describe the process of the basic structure before it gets transformed to the new blind signature scheme.

Key generation algorithm: Pick randomly an integer $e \in Z_n^* = \{1, 2, ..., n-1\}$ such that $\gcd(e, n) = 1$. Calculate an integer d satisfying the congruence $ed \equiv 1 \pmod{\phi(n)}$. Next select at random an integer x from Z_p^* and compute $y \equiv g^x \pmod{p}$. Finally, publishes (e, y) as a pair of public key whereas kept (d, x) as a pair of secret key of the scheme.

Signature generation algorithm: To sign message m, the signer selects randomly a secret integer $1 < r < n$ such that $\gcd(r, n) = 1$ and compute $k \equiv g^r \pmod{p}$. Next calculate $s \equiv h(m)x + kr \pmod{n}$ and $u \equiv s^d \pmod{n}$. The signer then produces (k, u) together with message m as a signature to the verifier.

Signature verification algorithm: The verifier can check the signature's authenticity by checking the equality of $g^{u^e} \equiv y^{h(m)} k^k \pmod{p}$.

THE NEW BLIND SIGNATURE SCHEME

The following protocol is the new blind signature scheme developed from the ordinary signature scheme reviewed as above. The scheme is described as two-ways of three interactions between the signer and the signature-requester.

First Interaction: The signer selects an integer $1 < \hat{r} < n$ such that $\gcd(\hat{r}, n) = 1$ and compute $\hat{k} \equiv g^{\hat{r}} \pmod{p}$. Then the signer checks that $\gcd(\hat{k}, n) = 1$. If this is not the case, he or she goes back to select another integer $\hat{r}$. Otherwise, he or she sends the owner of a message m, signature-requester the value of $\hat{k}$. The signature-requester upon receiving the given value then determines if $\gcd(\hat{k}, n) = 1$ holds or not. If this is the case, he selects two blinding factors $\alpha, \beta \in Z_n^*$ and compute $k \equiv \hat{k}^{\alpha} g^{\beta} \pmod{p}$ and checks that $\gcd(k, n) = 1$. If this is not case, he goes back to select another blinding factors. Otherwise, he computes and sends the signer $h(\hat{m}) \equiv \alpha^{-1} h(m) \hat{k} k^{-1} \pmod{n}$.

Second Interaction: The signer computes and sends $\hat{s} \equiv h(\hat{m}) x + \hat{k}\hat{r} \pmod{n}$ to the signature-requester which proceed the task by calculating and sending the signer $s \equiv \left(\alpha \hat{s} k \hat{k}^{-1} + \beta k\right)\left(\hat{s}^{-1}\right)^{e} \pmod{n}$.

Third Interaction: The signer computes and sends $\hat{u} \equiv s^{d} \pmod{n}$ to the signature-requester.
The signature-requester finally computes $u \equiv \hat{u}\,\hat{s} \pmod{n}$.
The above three interactions completes the blind signature scheme. The signature-requester produces (k, u) as a valid signature on message, m. This is shown by the following theorem.

Theorem 1. *If (k, u) is a signature of the message m produced by the proposed new blind signature scheme, then $g^{u^e} \equiv y^{h(m)} k^{k} \pmod{p}$, and the protocol above is a blind scheme.*

Proof: Note that,

$$u^e \equiv (\hat{u}\hat{s})^e \equiv \left(s^d \hat{s}\right)^e \equiv s\hat{s}^e \equiv \left(\alpha \hat{s} k \hat{k}^{-1} + \beta k\right)\left(\hat{s}^{-1}\right)^e \hat{s}^e \equiv \alpha\left(h(\hat{m}) x + \hat{k}\hat{r}\right) k\hat{k}^{-1} + \beta k$$

$$\equiv \alpha k \hat{k}^{-1}\left(\left(\alpha^{-1} h(m) \hat{k} k^{-1}\right) x + \hat{k}\hat{r}\right) + \beta k \equiv h(m) x + \alpha k r + \beta k$$

and thus

$$g^{u^e} \equiv g^{h(m)x + \alpha k r + \beta k} \equiv \left(g^{x}\right)^{h(m)} \left(g^{\alpha r + \beta}\right)^{k} \equiv y^{h(m)} \left(\hat{k}^{\alpha} g^{\beta}\right)^{k} \equiv y^{h(m)} k^{k} \pmod{p}.$$

In order to proof the blindness of the protocol we show that given a valid signature (k,u) and any view ν there exists a unique pair of blinding factor (α,β) since the signature-requester chooses the blinding factor randomly, the blindness of the scheme follows. Assume that the signature has been generated during the protocol with view consisting of $\left(\hat{r},\hat{k},h(\hat{m}),\hat{s},\hat{u}\right)$ then the following equations must hold for α,β :

$$k \equiv \hat{k}^{\alpha} g^{\beta} \pmod{p}$$
$$h(\hat{m}) \equiv \alpha^{-1} h(m) \hat{k} k^{-1} \pmod{n}$$
$$s \equiv \left(\alpha \hat{s} k \hat{k}^{-1} + \beta k\right)\left(\hat{s}^{-1}\right)^{e} \pmod{n}$$

It is easy to see that the unique solution for α,β is given by

$$\alpha \equiv \hat{h(m)}^{-1} h(m) \hat{k} k^{-1} \pmod{p} \text{ and } \beta \equiv \left(s\hat{s}^{e} k^{-1} - \hat{s}\hat{k}^{-1}\alpha\right) \pmod{n}.$$

Now it remains to show that $k \equiv \hat{k}^{\alpha} g^{\beta} \pmod{p}$. Note that

$$\begin{aligned}
\hat{r}\alpha + \beta &\equiv \hat{r}h(\hat{m})^{-1} h(m) \hat{k} k^{-1} + s\hat{s}^{e} k^{-1} - \hat{s}\hat{k}^{-1}\alpha \\
&\equiv \hat{r}h(\hat{m})^{-1} h(m) \hat{k} k^{-1} + s\hat{s}^{e} k^{-1} - \hat{s}\hat{k}^{-1}\left(h(\hat{m})^{-1} h(m) \hat{k} k^{-1}\right) \\
&\equiv \hat{r}h(\hat{m})^{-1} h(m) \hat{k} k^{-1} + s\hat{s}^{e} k^{-1} - \hat{s}\left(h(\hat{m})^{-1} h(m) k^{-1}\right) \\
&\equiv \hat{r}h(\hat{m})^{-1} h(m) \hat{k} k^{-1} + s\hat{s}^{e} k^{-1} - \left(h(\hat{m}) x + \hat{k}\hat{r}\right)\left(h(\hat{m})^{-1} h(m) k^{-1}\right) \\
&\equiv \hat{r}h(\hat{m})^{-1} h(m) \hat{k} k^{-1} + s\hat{s}^{e} k^{-1} - \left(xh(m) k^{-1} + \hat{k}\hat{r}h(\hat{m})^{-1} h(m) k^{-1}\right) \\
&\equiv s\hat{s}^{e} k^{-1} - xh(m) k^{-1} \\
&\equiv u^{e} k^{-1} - xh(m) k^{-1}.
\end{aligned}$$

Thus we have

$$\hat{k}^{\alpha} g^{\beta} \equiv g^{\hat{r}\alpha+\beta} \equiv g^{\left(u^{e} - xh(m)\right)k^{-1}} \equiv \left(g^{u^{e}} y^{-h(m)}\right)^{k^{-1}} \equiv k \pmod{p} \quad \square$$

SECURITY ANALYSIS

In this section, we discuss some security properties of our new blind signature scheme. A secure blind signature schemes should satisfy the following four requirements (Huang and Chang, 2004):

Randomization: The signer had 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 randomizing factor.

Unforgeability: Only the signer can generate the valid signatures.

Unlinkability: In a secure blind signature scheme, it is computationally infeasible for the signer to link a signature-message obtained for verification to the instance of the signing protocol that produced the signature.

Blindness: It allows a user to acquire a signature on a message without revealing anything about the message to the signer. It also ensures that no one can derive a link between a view and valid blind signature except the signature-requester. A view of the signer is defined to be the set of all messages that the signer has received and generated when issuing the signature. Owing to the blindness property, blind signatures have been widely used in untraceable electronic cash systems (Okamoto and Ohta, 1991).

Blindness

The blindness property of all signature issued by the signer contain a clear common information and agreed by the signature-requester and the signer, and the signature-requester is unable to change or remove the embedded information while keeping the verification of signature successful. In the proposed scheme, the signature-requester has to submit the blinded data $h(\hat{m})$ to the signer, and then the signer computes and sends $\hat{s} = h(\hat{m})x + \hat{k}\hat{r} \pmod{n}$ to the recipient. If the signature-requester can successfully change or remove the $\hat{k}$ from the corresponding signature (k, u), then he or she computes $\hat{s} = h(\hat{m})x + \hat{k}\hat{r} \mod n$. However, it is difficult to derive the secret key x. Also the signature-requester has to submit the blinded data s to the signer then the signer computes and sends $\hat{u}$ to the signature-requester. The signature-requester cannot change or remove $\hat{u} \equiv s^d \pmod{n}$ because it is difficult to derive the secret key d. Hence, in the proposed scheme, the signature-requester cannot change or remove the $\hat{k}$, $\hat{s}$ and $\hat{u}$ from the corresponding signature (k, u) of message m to forge the unblinded part of the signature.

Randomization

In the proposed scheme, the signer randomizes the blinded data using the random factor $\hat{r}$ before signing it in the signing phase. In the requesting phase, the signer selects an integer $\hat{r}$ and sends $\hat{k} \equiv g^{\hat{r}} \pmod{p}$ to the

recipient. Then, the recipient sends $h(\hat{m})$ to the signer, and the signer returns $\hat{s} = \left(h(\hat{m})x + \hat{k}\hat{r}\right) \pmod{n}$ to the signature-requester. If the signature-requester tries to remove $\hat{r}$ from $\hat{s}$, then he has to derive x from $y \equiv g^x \pmod{p}$.

However, it is difficult to determine x because that the derivation is discrete-log problem. Hence, in the proposed scheme, the signature-requester cannot remove the random $\hat{r}$ from the corresponding signature (k, u).

Unlinkability

For every instance, the signer can record the transmitted messages $\left(h(\hat{m})_i, s_i\right)$ between the signature-requester and the signer during the instance i of the protocol. The pair $\left(h(\hat{m})_i, s_i\right)$ is usually referred to as the *view* of the signer to the instance i of the protocol. Thus, we have the following theorem:

Theorem 2. *Giving a signature* (k, u) *produced by the proposed scheme, the signer can derive the blinding factors* (α_i', β_i') *for every* $\left(h(\hat{m})_i, s_i\right)$ *such that*

$$h\left(\hat{m}_i\right) \equiv \left(\alpha_i'\right)^{-1} h(m) k k^{-1} \pmod{n}, \quad s_i \equiv \left(\hat{s}\, k\, \hat{k}^{-1} \alpha_i' + \beta_i' k\right)\left(\hat{s}^{-1}\right)^e \pmod{n}.$$

Proof: For every $\left(h(\hat{m})_i, s_i\right)$, we have

$$h(\hat{m})_i = (\alpha_i')^{-1} h(m) \hat{k} k^{-1} \bmod n \quad \text{and} \quad s_i \equiv (\hat{s}\, k\, \hat{k}^{-1} \alpha_i' + \beta_i' k)(\hat{s}^{-1})^e \bmod n.$$

It is easily to obtain,

$$\alpha_i' \equiv h(\hat{m})^{-1} h(m) \hat{k} k^{-1} \bmod n \quad \text{and} \quad \beta_i' \equiv \left(s_i \hat{s}^e k^{-1} - \hat{s}\ \hat{k}^{-1} \alpha_i'\right) \bmod n.$$

Note that, giving a signature (k, u) produced by the proposed scheme, the signer can always derive the two blinding factors for every transmitted record $\left(h(\hat{m})_i, s_i\right)$. This implies that the signer is unable to find the link between the signature and its corresponding signing process instance and thus the unlinkability property is achieved.

Unforgability

The intruder may try to derive some forged signatures by using different ways. We will show that all the attacks fail on our scheme.

Attack 1: Intruder tries to derive the signature (k, u) for a given message, m by letting one integer fixed and finding the other one. For example, intruder selects k and tries to figure out the value of u satisfying $g^{u^e} \equiv y^{h(m)} k^k \pmod{p}$ and vise-versa. To do this, intruder first chooses at random an integer k. He or she then computes $\alpha \equiv y^{h(m)} k^k \pmod{p}$. Finally he or she solves $\alpha \equiv g^{u^e} \pmod{p}$ for u and successful only if both fac and dl are breakable.

Attack 2: It is assumed that intruder is able to solve dl problem. In this case, intruder knows x and can generate or calculate the numbers $\hat{s}$ and s. Unfortunately, he or she does not know d hence cannot compute $\hat{u} \equiv s^d \pmod{n}$ and then cannot compute $u \equiv \hat{u}\hat{s} \pmod{n}$ and fails to produce the signature (k, u).

Attack 3: It is assumed that intruder is able to solve the fac problem. That means, he knows the prime factorization of n and can find the number d. However, he or she cannot compute $\hat{s}$ since no information is available for x, hence cannot compute s because it is dependent on $\hat{s}$, then he or she cannot compute $u \equiv \hat{u}\hat{s} \pmod{n}$. Thus fails to produce the signature (k, u).

Attack 4: Intruder may also try collecting t valid signatures (k_j, u_j) on message m_j where $j = 1, 2, ..., t$ and attempts to find secret keys and number of the signature scheme. In this case, intruder has t equations given as follows:

$$\begin{aligned} u_1^e &\equiv h(m_1)x + k_1 r_1 \pmod{n} \\ u_2^e &\equiv h(m_2)x + k_2 r_2 \pmod{n} \\ &\vdots \\ u_t^e &\equiv h(m_t)x + k_t r_t \pmod{n}. \end{aligned}$$

In the above t equations, there are $t+1$ variables, x and r_j which are not known by the intruder. Hence, x stays hard to detect because intruder can generate infinite solutions of the above system of equations but cannot figure out which one is correct.

EFFICIENCY PERFORMANCE

Next, we investigate the performance of our scheme in the number of modular multiplication, number of hashing operation, number of random-number generation, number of inverse computations and number of modular exponentiation. The computation costs of the proposed scheme are summarized in Table 1.

TABLE 1*: The computation costs of the proposed blind signature scheme*

Type of Operations	Performed by the signature-requester	Performed by the signer
Modular multiplication	11	2
Hashing operation	3	1
Random-number generation	2	1
Inverse computations	4	0
Modular exponentiation	7	2
nth-root computations	0	0

.

In the proposed scheme, no root and inverse computations in Z_n^* are performed by the signer. There are seven modular exponentiations, eleven modular multiplications, three hashing operations and twice of random number generation performed by the recipient to obtain and verify a signature. There are two modular exponentiations, two modular multiplications, one hashing operation and once random number generation performed by the signer to issue a signature.

CONCLUSIONS

In this paper, we presented a new blind signature scheme based on factoring and discrete logarithms. The scheme based on two hard problems provides longer and higher level security than scheme that based on a single hard problem. The proposed scheme requires minimal operation in signing and verifying and thus makes it very efficient. Some possible attacks have also been considered and we showed that the scheme secure from those attacks.

ACKNOWLEDGEMENT

The first author acknowledges the financial support received from the Malaysian Ministry of Higher Education under the FRGS Grant UKM-ST-02-FRGS0004-2006.

REFERENCES

Camenish, J. L., Priveteau, J-M. and Stadler, M. A. 1994. Blind signature based on the discrete logarithm problem. *Advances in Cryptology (Eurocrypt '94),* LNCS 950, Springer-Verlag, 428-432.

Chaum, D. 1983. Blind signature system. *Advances in Cryptology (Crypto'83)*, Plenum, New York, 153.

Chaum, D., Fiat, A. and Noar, M.1988. Untraceable electronic cash. *Advances in Cryptology (Crypto'88)*, LNCS 403, Springer-Verlag, 319-327.

Chaum, D. 1989. Privacy protected payment, smart card 2000. *Elsevier Science Publishers B.V. (North-Holland)*, 69-93.

Chaum, D., den Boer, B., Van Heyst., E., Mjolsnes, S. and Steenbeek, A. 1989. Efficient offline electronic checks. *Advances in Cryptology (Eurocrypt '89),* LNCS 434, Springer-Verlag, 294-301.

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

Okamato, T. and Ohta, K. 1991. Universal Electronic Cash. *Advances in Cryptology (Crypto'91),* LNCS 576, Springer-Verlag, 324-337.