Journal of Mathematics and Statistics 4 (2): 124-129, 2008
ISSN 1549-3644
© 2008 Science Publications

A New Partially Blind Signature Based on Factoring and Discrete Logarithms

N.M.F. Tahat, S.M.A. Shatnawi and E.S. Ismail
School of Mathematical Sciences, National University of Malaysia
43600 UKM Bangi Selangor, Malaysia

Abstract: Partially blind signatures played an important role in many electronic commerce applications. Many existing partially blind signature scheme based on a single hard problem but not secure. In this study, we propose a secure partially blind signature scheme based on factoring and discrete logarithms and show that the proposed scheme satisfies the partial blindness, randomization, unlinkability and unforgeability properties. We also analyse the computation cost of the proposed scheme.

Key words: Cryptology, cryptography, partially blind signature, factoring, discrete logarithms

INTRODUCTION

The blind signature technique was first introduced by Chaum[3] to protect the right of an individual's privacy. It is a special form of digital signature. Creating blind signature for a message involves two parties, which we call the signer and a group of signature requesters.

The requester requests the signer to sign on a blinded data. It means the signer does not know the content of the message. The requester then unblinds the signed message from the signed blinded data. The signer's signature on the message can be verified by checking if the corresponding public verification formula with the signature-message pair as parameter is true. In a secure blind signature scheme, the signer is unable to link (trace) this signed message to the previous signing process instance. This property is usually referred to as the unlinkability property. Due to the unlinkability (blindness) property, blind signature techniques have been widely used in the anonymous electronic cash (e-cash) and anonymous voting systems. In the e-cash system, since the e-cash may easily be duplicated, hence to prevent double spending, the bank has to record all spent e-cash to check whether a specified e-cash has been spent or not by searching the database. However, the database kept by the bank may grow unlimitedly. In order to prevent the bank's database from growing unlimitedly, the techniques of partially blind signatures were proposed in Abe and Fujisaki [1], Abe and Okamoto[2] and Fan and Lei[4].

In the partially blind signature scheme, the signer can impose the common information, for example, the date information on the signature so that the verifier needs the message, the common information, and the signature to check the validity of this signature. This common information is a pre-defined format negotiated and agreed by all requesters and the signer. By, using RSA, Abe and Fujisaki[1] proposed the partially blind signature scheme of which the signer (the bank) assures that the signed blind signature (e-cash) contains the agreed common information such as the date information. By embedding an expiration date into each e-cash, the bank only has to keep the existing cash in the database to prevent doublespending. Those expired e-cash recorded in the database can be removed. This technique can be used for dealing with the unlimited growth problem of the bank's database in the e-cash system. This partial blindness preserves the unlinkability property of the blind signature and it also embeds the common information on the blind signature. However, in most of the blind signature schemes, there are several modular exponentiations and inverse computations needed by the signature requesters and the signer. Later, based on Quadratic Residue (QR) theory, Fan and Lei[4] proposed the partially blind signature scheme, and there is no modular exponentiation and inverse computations performed by the signature requesters.

Moreover, there are only several modular additions and multiplications required for a requester to obtain and verify a signature in their protocol. Comparing with the blind signature schemes proposed in the literatures, Fan and Lei's scheme[4] reduces the amount of computations for the signature requesters or users by nearly 98% under a 1024-bit modulus, but it does not

Corresponding Author: N.M.F. Tahat, School of Mathematical Sciences, National University of Malaysia,
43600 UKM Bangi Selangor, Malaysia

decrease the computation load for the signer. So their scheme is especially suitable for mobile signature requesters and smart-card users. However, in 2002, Hwang, Lee and Lai[6] showed that Fan-Lei's[4] scheme could not meet the untraceability property of a blind signature. Recently, Huang and Chang[5] proposed a new design of efficient partially blind signature based on discrete logarithm and the Chinese Remainder, but Zhang and Chen[7] show that Huang and Chang partially blind signature scheme is not secure. However, all developed partially blind signature schemes in the literature are based on a single hard problem like factoring, discrete logarithm or elliptic curve discrete logarithm problem. In the future, if one finds a solution of one of these problems, the related partially blind signature will be no longer secure. Thus, in this study we propose a secure partially blind signature scheme based on discrete logarithms and factoring problem plus our scheme maintains the amount of computations for both the signature requester and the signer.

Preliminaries: Throughout the article, we need the following tools to describe our new partially blind signature scheme and to discuss its security analysis and efficiency performances: A cryptographic hash function h (.), that maps any arbitrary length of input and output a t-bit length and assume t = 128. A large number prime p and n (a factor of p-1) is the product of two safe prime (which contains no small prime divisors). A phi-Euler function, $\phi(n)$. 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 gcd (a,b) be the greatest common divisor of a and b.

MATERIALS AND METHODS

We now propose an efficient and secure partially blind signature for both parties of the signer and the requester to obtain a signature. There are two types of participants, a signer and a signature requester A in a partially blind signature scheme. We give a process of their interactions of the scheme:

- Suppose a requester would request a partially blind signature from the signer. In this case, the requester will notify the signer
- Then, the requester provides the blinded data/message and the common information and sends them to the signer. For this stage, the signer will decide on this common information
- If the signer agrees on this common information, then he signs the blinded data with this common information embedded on the signature
- For the partial blindness property, the requester derives the signature from the signed data, but he cannot remove or change the embedded common information. So the agreed common information should be genuinely shared among the requester, the signer and the verifiers

The proposed partially blind signature scheme consists of four phases: (1) initialization, (2) requesting, (3) signing, and (4) extraction. The signer publishes the necessary information in the initialization. In the requesting phase, a requester submits the blinded data and the common information to the signer. In the signing phase, the signer signs the blinded data with this common information imposed on it and then sends the result back to the requester. Finally, the requester extracts the signature from the signed data in the extraction phase. The details of the proposed partially blind signature scheme are described as follows.

The above process of partially blind signature is taken from Huang and Chang [5].

Initialization: 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.

Requesting: Suppose requester A wants to obtain a signature on message, h(m). Firstly, he must notify the signer and then:

- A signer selects an integer r<n such that gcd (r,n) = 1 and compute $\hat{z} = g^{r} (\mathrm{mod}\, p)$.
- Then the signer checks that gcd $(\hat{z}, n) = 1$. If this not the case, he/she goes back to select another integer r. Otherwise, he/she sends $\hat{z}$ to the requester A.
- After receiving $\hat{z}$, requester A checks that $\gcd(\hat{z}, n) \equiv 1$ and prepares the common information a, according to a pre-defined format. Then the value "a" is a common input of both the requester A and the signer.
- The requester A also randomly select two blinding factors $u \in z^*_n, v \in z_n$ and compute $z = \hat{z}^u g^V$ (modp) and checks whether gcd (z, n) = 1. If this is not case, he/she goes back to selects another blinding factor. Other wise, he/she compute $\sigma = u^{-1} h(m) \hat{z} z^{-1}$ (modn) and then send (σ, a) to the signer:

Signing and Extraction: The signer signs blindly the message h(m) as follows

- The signer computes and sends $\hat{s} = (\sigma x a + \hat{z} r)\ (\text{mod} n)$ to the requester A
- The requester A computes and sends $s \equiv (\hat{s} z \hat{z}^{-1} u + vz)(\hat{s}^{-1})^e (\text{mod} p)$ to the signer
- The signer computes and sends $\hat{\gamma} \equiv s^d\ (\text{mod} p\ )$ to the requester A
- The requester A computes $\gamma \equiv \hat{\gamma} \hat{s}\ \ (\text{mod} p\ )$

Then the signature is given by (a,z,γ).

The following theorem shows that if a signature (a,z,γ) of a message m is produced by the proposed partially blind signature scheme, then it satisfies $g^{\gamma^e} \equiv y^{h(m)a} z^z$ (mod p).

Theorem: If (a, z, γ) is a signature of the message m produced by a proposed new partially blind signature scheme, then $g^{\gamma^e} \equiv y^{h(m)a} z^z$ (mod p).

Proof: We have to show that the pair of signature (a,z,γ) satisfies:

$$\gamma^e(\text{mod} n) \equiv (\hat{\gamma}\hat{s})^e \equiv \left(\gamma^d \hat{s}\right)^e \equiv s\hat{s}^e \equiv$$
$$\left(u\hat{s}z\hat{z}^{-1} + vz\right)\left(\hat{s}^{-1}\right)^e \hat{s}^e \equiv u\left(\sigma x a + \hat{z} r\right)$$
$$z\hat{z}^{-1} + vz(\text{mod} n) \equiv uz\hat{z}^{-1}$$
$$\left(\left(u^{-1}h\left(m\right)\hat{z}z^{-1}\right)x a + \hat{z} r\right) + vz \equiv$$
$$h\left(m\right)x a + uzr + vz(\text{mod} n)$$

and thus:

$$g^{\gamma^e} \equiv g^{h(m)x a + uzr + vz} \equiv \left(g^x\right)^{h(m)a} \left(g^{ur+v}\right)^z \equiv$$
$$y^{h(m)a} \left(\hat{z}^u g^v\right)^z \equiv y^{h(m)a} z^z\ (\text{mod}\ p)$$

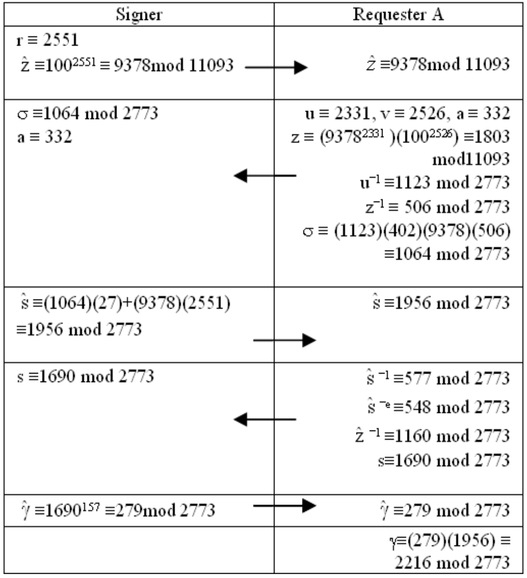
which means that (a, z, γ) is a valid signature of m.

So, our proposed protocol provides a partially blind signature scheme.

Example: Let a signer wishes to sign a hashed message h (m) = 402 such that only an intended can validate the resulting signature.

The scheme's set up is done by a signer p′ = 47, q′ = 59, n = p′q′ = 2773, p = 11093, ϕ(n) = (p′-1) (q′-1) = 2668, e = 17, $d \equiv e^{-1} \equiv 17^{-1} \equiv 157$ (mod 2668), $x = 27$, $g = 100$, $y \equiv 100^{27}$ (mod 11093) ≡ 10350 (mod 11093), and the common information a = 332.

Now we show how to obtain a partially blind signature using the above example. We describe it using a Fig. 1.



Signer		Requester A
$r \equiv 2551$ $\hat{z} \equiv 100^{2551} \equiv 9378 \text{mod}\ 11093$	$\longrightarrow$	$\hat{z} \equiv 9378 \text{mod}\ 11093$
$\sigma \equiv 1064 \text{ mod } 2773$ $a \equiv 332$	$\longleftarrow$	$u \equiv 2331, v \equiv 2526, a \equiv 332$ $z \equiv (9378^{2331})(100^{2526}) \equiv 1803$ mod11093 $u^{-1} \equiv 1123 \text{ mod } 2773$ $z^{-1} \equiv 506 \text{ mod } 2773$ $\sigma \equiv (1123)(402)(9378)(506)$ $\equiv 1064 \text{ mod } 2773$
$\hat{s} \equiv (1064)(27)+(9378)(2551)$ $\equiv 1956 \text{ mod } 2773$	$\longrightarrow$	$\hat{s} \equiv 1956 \text{ mod } 2773$
$s \equiv 1690 \text{ mod } 2773$	$\longleftarrow$	$\hat{s}^{-1} \equiv 577 \text{ mod } 2773$ $\hat{s}^{-e} \equiv 548 \text{ mod } 2773$ $\hat{z}^{-1} \equiv 1160 \text{ mod } 2773$ $s \equiv 1690 \text{ mod } 2773$
$\hat{\gamma} \equiv 1690^{157} \equiv 279 \text{mod}\ 2773$	$\longrightarrow$	$\hat{\gamma} \equiv 279 \text{ mod } 2773$
		$\gamma \equiv (279)(1956) \equiv$ $2216 \text{ mod } 2773$

Fig. 1: Interactions Between the Requester A and the Signer

Now the recipient obtains a signature given as $(a, z, \gamma) = (332, 1803, 2216)$. Next, the recipient accepts this signature as valid because:

$$g^{\gamma^e} \equiv 100^{2216^{17}} \equiv 100^{2685} \equiv 5531 \text{ mod } 11093$$
$$y^{h(m)a} k^k \equiv 10350^{402 \times 332} \times 1803^{1803} \equiv 5531 \text{ mod } 11093.$$

RESULTS

In this study, we give our results in terms of security analysis and efficiency performance of our proposed partially blind signature scheme.

Security: In this study, we discuss some security properties of our partially blind signature scheme. A secure partially blind signature scheme should satisfy the following requirements and we show that our proposed scheme satisfied the requirements.

a) Partial blindness: It allows a user to acquire a signature on a message without revealing anything about the message to the signer. Blindness property 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.

b) Randomization: The signer had better inject 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.

c) Unlinkability: In a secure blind signature scheme, it is computationally infeasible for the signer to link asignatureshown for verification to the instance of the signing protocol that produced that signature. This property is usually referred to as the unlinkability property.

d) Unforgeability: It means that only the signer can generate the valid signatures.

Partial blindness: The partial blindness property of all signature issued by the signer contain a clear common information a according to the predefined format negotiated and agreed by all the requester and the signer and the requester is unable to change or remove the embedded information a while keeping the verification of signature successful. In the proposed scheme, the requester A has to submit the common information a and the blinded data σ to the signer and then the signer computes and sends $\hat{s} = \sigma x a + \hat{z} r \pmod{n}$ to the requester A. If the requester A can successfully change or remove this common information a from the corresponding signature(a, z, γ), then he or she computes $\hat{s} = (\sigma x a + \hat{z} r)$ mod n. However, it is difficult to derive the secret key x. Also the requester A has to submit the blinded data s to the signer then the signer computes and sends $\hat{\gamma}$ to the requester. The requester A cannot change or remove $\hat{\gamma} \equiv s^d \pmod{n}$ because it is difficult to derive the secret key d. Hence, in the proposed scheme, the requester A cannot change or remove the a and $\hat{\gamma}$ and from the corresponding signature (a, z, γ) 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 r before signing it in the signing phase. In the requesting phase, the signer select an integer r such that $\hat{z} = g^r \bmod p$ and submit $\hat{z}$ to the requester. Then the requester A sends σ to the signer and the signer returns $\hat{s} = (\sigma x a + \hat{z} r) \bmod n$ to the requester A. If the requester A tries to remove r from $\hat{s} = \sigma x a + \hat{z} r$ mod n, then he has to derive x from $y = g^X$ mod p. However, it is difficult to determine x because that the derivation is discrete-log problem. Hence, in the proposed scheme, the requester A cannot remove the random r from the corresponding signature (a, z, γ) of message m.

Unlinkability: For every instance, numbered i, of the protocol in study, the signer can record the transmitted messages (σ_i, s_i) between the requester A and the signer during the instance i of the protocol. The pair (σ_i, s_i) is usually referred to as the *view* of the signer to the instance i of the protocol. Thus, we have the following theorem:

Theorem: Giving a signature (a, z, γ) produced by the proposed scheme, the signer can derive (u_i', v_i') for every(σ_i, s_i) such that:

$$\sigma_i \equiv (u_i')^{-1} h(m) \hat{z} z^{-1} \bmod n \text{ and}$$
$$s_i \equiv (\hat{s} z \hat{z}^{-1} u_i' + v_i' z)(\hat{s}^{-1})^e \bmod n$$

Proof: If $\sigma_i \equiv (u_i')^{-1} h(m) \hat{z} z^{-1} \bmod n$, we have that:

- $u_i' \sigma_i \equiv h(m) \hat{z} z^{-1} \bmod n$
- $u_i' \equiv \sigma^{-1} h(m) \hat{z} z^{-1} \bmod n$

If $s_i \equiv (\hat{s} z \hat{z}^{-1} u_i' + v_i' z)(\hat{s}^{-1})^e \bmod n$, then we have the following derivations:

- $s_i \hat{s}^e \equiv (\hat{s} z \hat{z}^{-1} u_i' + v_i' z) \bmod n$
- $v_i' z \equiv (s_i \hat{s}^e - \hat{s} z \hat{z}^{-1} u_i') \bmod n$
- $v_i' \equiv (s_i \hat{s}^e - \hat{s} z \hat{z}^{-1} u_i') z^{-1} \bmod n$
- $v_i' \equiv (s_i \hat{s}^e z^{-1} - \hat{s} \hat{z}^{-1} u_i') \bmod n$

According to the above derivations, the signer can derive u_i', v_i' for every record (σ_i, s_i). Hence, giving a signature (a, z, γ) produced by the proposed scheme, the signer can always derive the two blinding factors (σ_i, s_i) for every transmitted record (σ_i, s_i).

This implies that the signer is unable to find the link between the signature and its corresponding signing process instance. So, our scheme can achieve the unlinkability property.

Unforgability: The intruder may try to derive some forged signatures by using different ways. We will show:

Attack 1: Intruder tries to derive the signature (a, z, γ) for a given message m by letting one integer fixed or two and finding the other one. For example, intruder selects z and tries to figure out the value of γ,a to satisfy $g^{\gamma e} \equiv y^{h(m)a} z^{z}$ mod p and vise-versa. To do this, intruder first chooses at random an integers z and assume that DL is breakable then he/she knows a and γ^{e} then computes $\alpha \equiv y^{h(M)a} z^{z} \pmod{p}$. Finally he/she solves $\alpha \equiv g^{\gamma e} \pmod{p}$ for y. He can only find y if both FAC and DL are breakable. Then he/she knows γ^{e} but still does not know y because he/she learns nothing about d Now assume that FAC is breakable and the intruder selects z, a. Then he/she knows d but still does not knows γ^{e} (DL). Intruder may proceed this attack by selecting an integer γ, a and tries to figure out the value of z. He/she then compute $\lambda \equiv g^{\gamma e} y^{-h(M)a} \pmod{p}$. Finally he/she solves $\lambda \equiv z^{z} \pmod{p}$ for z. This is the worst case, because even if he/she can solve FAC and DL, the value of z is still hard to find except for try error but it is time consuming.

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/she does not know d hence cannot compute $\hat{\gamma} = s^{d}$ (mod n) and then cannot compute $\gamma = \hat{\gamma}\hat{s} \bmod n$ and fails to produce the signature (a, z, γ).

Attack 3: It is assumed that intruder is able to solve FAC problem. That means, he knows the prime factorization of n i.e.p' and q' and can find the number d. However, he/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/she cannot compute $\gamma = \hat{\gamma}\hat{s}$ mod n. Thus fails to produce the signature (a, z, γ).

Attack 4: Intruder may also try collecting t valid signature (a_j, z_j, γ_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:

$$\gamma_1^{e} \equiv h(m_1)xa_1 + z_1 r_1 \pmod{n}$$

$$\gamma_2^{e} \equiv h(m_2)xa_2 + z_2 r_2 \pmod{n}$$

$$\vdots$$

$$\gamma_t^{e} \equiv h(m_t)xa_t + z_t r_t \pmod{n}$$

In the above t equations, there are (t+1) variables i.e., x and r_j where j = 1,2,…,t which are not known by the intruder. Hence, x stays hard to detect because intruder can generate infinite solution of the above system of equations but cannot figure out which one is correct. In addition, intruder wishes to obtain secret keys (x, d) using all information that available from system. In this case, intruder needs to solve or calculate y = g^{x} mod p and e^{-1} mod $\phi(n)$ which are clearly infeasible the difficulty of solving DL and FAC.

Table 1: The computation costs of the proposed partially blind signature scheme

Type of operations	Performed by requester A	Performed by signer
Number of modular multiplications	9	3
Number of hashing operations	2	0
Number of random-number generations	2	1
Number of inverse computations	4	0
Number of modular exponentiation	3	2
Number of n*th*-root computations	0	0

Performance: Next, we investigate the performance of our scheme in 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.

In the proposed scheme, no root, hashing operation and inverse computations in Z_n^{*} are performed by the signer. There are three modular exponentiations, ten modular multiplications, two hashing operations and twice of random number generation performed by the requester A.

There are two modular exponentiations, three modular multiplications and once random number generation performed by the signer to issue a signature.

DISCUSSION

So far in the literature, the developed partially blind signature schemes are based on a single problem. If an enemy can find a solution of this single problem then he or she can break the scheme. These includes the scheme of Abe and Fujisaki[1] , Abe and Okamoto[2] , Fan and Lei[4], Hwang, Lee and Lai[6] and Zhang and Chen[7] .

This problem is avoided in our scheme, since the proposed partially blind signature is based on two multiple hard problems; namely factoring and discrete logarithm problems. Thus it provides a longer security than that partially blind signature schemes based on a single problem. This is because it is very unlikely for enemies to solve the two problems simultaneously. If one of the problems can be solved, the intruder still has to solve the other problem in order to break our new scheme. Next, our scheme also satisfies the four important requirements to guarantee the security of the scheme namely; partial blindness, randomization, unlinkability and unforgeability. The randomization property avoids intruder in gaining some valuable hints or ideas to break the scheme. The property of unlinkability prevents intruder from obtaining added information from the previous blind signature. The last requirement, unforgeability confirms that the intruder will have no chance in getting any secret numbers or information.

The efficiency performance reveals that the modular multiplication operation dominates our scheme. However this operation does not interrupt the process of the scheme since it can always speeded up. Note that the other operations; modular exponentiation, hashing and inverse computations involve only minimal operations. Our performance analysis also maintains the performances of schemes of Abe and Fujisaki[1] , Abe and Okamoto[2] , Fan and Lei[4], Hwang, Lee and Lai[6] and Zhang and Chen[7] . This means, no significant difference were found in performance analysis of our scheme (using Table 1) when compared with other schemes.

CONCLUSIONS

In this study, we presented a new partially blind signature based two hard problems namely; factoring and discrete logarithms. The scheme based on two problems provides higher level security than scheme that based on a single 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.

ACKNOWLEDGMENT

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

REFERENCES

1. Abe, M. and E. Fujisaki, 1996. How to date blind signatures. Lecture Notes in Computer Science, 1163. Springer-Verlag, pp: 244-251. ISBN: 978-3-540-61872-0. www.springerlink.com/index/5g4633570832g73k.pdf.
2. Abe, M. and T. Okamoto, 2000. Provably Secure Partially Blind Signatures. Lecture Notes in Computer Science, 1880. Spring-Verlag, pp: 271-286. ISBN: 978-3-540-67907-3. www.iacr.org/archive/crypto2000/18800272/18800272.pdf.
3. Chaum, D., 1982. Blind signature for untraceable payments. Advances in Cryptology, Proceedings of CRYPTO '82. Plenum Press, New York, pp: 199-203. http://www.informatik.unitrier.de/~ley/db/indices/a-tree/c/Chaum:David.html.
4. Fan, C.I. and C.L. Lei, 1998. Low-computation partially blind signatures for electronic cash. IEICE Trans. Fundam, 81: 818-824. http://search.ieice.org/bin/summary.php?id=e81-a_5_818&category=A&lang=&year=1998.
5. Hui-Feng Huang and Chin-Chen Chang, 2004. A new design of efficient partially blind signature scheme. J. Syst. Software, 73: 397-403. doi:10.1016/S0164-1212(03)00237-1.
6. Hwang, M.S., C.C. Lee and Y.C. Lai, 2002. Traceability on low computation partially blind signatures for electronic cash. IEICE Trans. Fundam, 85: 1181-1182. http://search.ieice.org/bin/summary.php?id=e85-a_5_1181&category=A&lang=&year=2002&auth=1.
7. Fangguo Zhang and Xiaofeng Chen, 2005. Cryptanalysis of Huang-Chang partially blind signature scheme. J. Syst. Software, 76: 323-325. doi: 10.1016/j.jss.2004.07.249.