A Provably Secure Scheme for
Restrictive Partially Blind Signatures

Fuw-Yi Yang and Jinn-Ke Jan*

Institute of Applied Mathematics, National Chung Hsing University,

Taichung 402, Taiwan, R.O.C., yangfy@ms7.hinet.net

*Institute of Computer Science, National Chung Hsing University,

Taichung 402, Taiwan, R.O.C., jkjan@cs.nchu.edu.tw

Abstract

A secure scheme of restrictive partially blind signature was presented. The proposed scheme has several advantages over the previous scheme: 1. The scheme is provable secure against the one-more signature forgery under the adaptively parallel attack. 2. The issued signatures can be of polynomial number whereas the previous work allows only logarithmic number. 3. The scheme is more efficient than previous scheme in both communicational and computational complexities.

Key words:

Blind signature, partially blind signature, and restrictive blind signature.

1. Introduction

Blind signature schemes [1] allow users to blind the messages being signed and reshape the outside of signatures such that the signer cannot link the signatures and the users. It is a useful building block in applications where anonymity is one of the most significant considerations, such as electronic cash and electronic voting systems.

But it may not be a good idea to blind everything in every application. Considering the settings for electronic cash schemes, a database is required to store the deposited coins so as to detect double spending. In the area of electronic cash systems based on the blind signature scheme, the coins are usually the blind signatures issued from the banks. Therefore, the database will grow unlimitedly if no explicitly expiring date is specified. In addition, the banks usually issue coins of different denominations in order to allow exact payments. Clearly inscribing the value of each coin is required.

The scheme of partially blind signature helps a lot to solve the aforementioned problems. A scheme based on the RSA assumption was firstly introduced in [2]. The scheme allows the blind signatures to explicitly contain some information that the two sides have agreed on. Therefore, the pieces of common agreed information can enclose the expiring date, the denominational data and other useful message. Based on the hardness of solving discrete logarithms, the scheme in [3] is a secure scheme as long as the issued blind signatures are logarithmic number.

Several researchers have proposed schemes of restrictive blind signature [4-6], which require that the structure of messages being signed must obey some predetermined rules. By the enforced restrictive property, the signer is assured that the withdrawer's identity was embedded in the blind signatures whenever the coins are withdrawn from the banks. The embedding of useful message in the blind signatures enables the banks to detect and reveal the identity that doubly spends the coins.

Combining the schemes of partially blind signature [3] and restrictive blind signature [4-6], a scheme of restrictive partially blind signature was proposed in [7]. Like the scheme in [3], it is secure only up to logarithmic number of issued blind signatures. Although the schemes in [3, 7] are possible to be secure in polynomial number of published signatures by incorporating the more complex three-party signature protocol [8], the final scheme will result in more expensive computations.

This paper proposes a secure restrictive blind signature scheme based on the intractability of the ROS-problem [9-10] and the hardness of the discrete logarithm problem. The scheme is secure up to polynomial number of issued blind signatures and it is more efficient than the scheme in [7]. The promotion of the efficiency and circulated signatures would be valuable, because the time complexity and system requirements are reduced.

The organization of this paper is as follows. Section 2 describes notations used in the paper. Section 3 presents a new scheme and discusses the properties of restrictive nature and blindness. In Section 4, the scheme's security is investigated and proved. Section 5 makes comparisons with the scheme in [7] in terms of computational and communicational cost. Finally, Section 6 concludes the paper.

2. Notations

Let G be an arbitrary group with prime order q. g and g_1 are generators of G, where $log_g^{g_1}$ is unknown to everybody. M is an arbitrary message space. $a||b$ denotes a concatenation of strings a and b. $a \in_R G$ denotes a is randomly selected from the set G. $H(.)$ is a collision-resistant hash function defined as $H(.): \{0, 1\}^* \rightarrow Z_q^*$, where Z_q^* is the multiplicative group of integers modulo q.

3. The proposed scheme

Assume that the user U has registered at the signer's system with identity $ID_u = g^{x_u} \in G$. Suppose that the user U wants to get a restrictive partially blind signature on a message $m \in M$. Then, the signer would use his secret key x to impose $(ID_u g_1)^x$ on the resulting signature. This is helpful to extract the user who requested the signature, if the signature is used maliciously [6]. Also, assume that the signer S and U have agreed on the common information $info \in M$. Let $x_1, x_2 \in_R Z_q$ be the signer's secret keys and the corresponding public keys are $y_1 = g^{x_1}$ and $y_2 = g^{x_2}$, where y_1 and $y_2 \in G$.

1. S chooses $w \in_R Z_q$, computes $r = g^w$, $r_u = (ID_u g_1)^w$, $z = H(info)$, $y_u = (ID_u g_1)^{x_1+zx_2}$. These three elements r, r_u, and y_u are members of the group G. S sends them to the user U.
2. In order to blind the signer's view, U chooses u, v, $\alpha \in_R Z_q$ and computes $z = H(info)$, $r' = rg^u(y_1 y_2^z)^v$, $ID'_u = (ID_u g_1)^\alpha$, $r'_u = (r_u)^\alpha (ID'_u)^u (y'_u)^v$, and $y'_u = (y_u)^\alpha$. U computes $c' = H(g \| g_1 \| y_1 \| y_2 \| m \| info \| ID'_u \| y'_u \| r' \| r'_u)$ and sends the challenge $c = c' + v \in Z_q$ to S.
3. S computes $s = w + c\,(x_1 + z\,x_2) \in Z_q$ and sends s to U.
4. U computes $s' = s + u \in Z_q$. U accepts $(m, info, ID'_u, y'_u, c', s')$ as a valid signature if $c' = H(g \| g_1 \| y_1 \| y_2 \| m \| info \| ID'_u \| y'_u \| g^{s'}(y_1 y_2^z)^{-c'} \| (ID'_u)^{s'} (y'_u)^{-c'})$, otherwise rejects.

Restrictive: The representation of ID_u, with respect to the generator tuple (g, g_1) is $(x_u, 1)$. After finishing the protocol, the representation of ID'_u with respect to the same generator tuple is $(\alpha x_u, \alpha)$. Let $I_1(a_1, a_2) = a_1 / a_2 = x_u \bmod q$ be a function on the representation of ID_u and $I_2(a_1, a_2) = a_1 / a_2 = \alpha x_u / \alpha = x_u \bmod q$ be a function on the representation of ID'_u. Thus, we have found the blinding-invariant functions [6] for the proposed scheme, *i.e.* $I_1(a_1, a_2)$ and $I_2(a_1, a_2)$. The equal of $I_1(a_1, a_2)$ and $I_2(a_1, a_2)$ indicates that whatever the user can blind the message ID_u, he cannot blind its internal structure. Therefore, our scheme possesses the restrictive nature.

Blindness: Let $(info, ID_u, y_u, r_u, r, c, s)$ denote the signer's view and the user have obtained a valid signature on m, *i.e.* the tuple $(m, info, ID'_u, y'_u, c', s')$. Also assume that the signer cannot distinguish the signatures by analyzing the signer cannot distinguish the signatures by analyzing the information *info*. The property of blindness requires that the signer's view is independent of the user's signature.

Lemma 1 below proves the blindness of the proposed scheme.

Lemma 1. The tuple $(m, info, ID^{'}_{u}, y^{'}_{u}, c', s')$ is a partially blind signature.

Proof. The signer and user have negotiated the common information *info* before they are engaged in the signing steps, and the signer has no idea about the message *m*, therefore the signer partially knows the context *(m, info)*. There exists a unique triple (u, v, α) for every valid signature, *i.e.* $u = s' – s$, $v = c - c'$, and $\alpha = log_{ID_u}^{ID'_u} = log_{y_u}^{y'_u}$. The existence of unique triple (u, v, α) proves the property of blindness, since the user chooses them randomly from Z_q, the field of integers modulo *q*.

4. Securities

The security of a practically scheme for blind signature has been suggested should be resistant to the attack of one-more signature forgery [11-13]. This level of security requires that after *l* interactions with the signer, the adversary construct $(l + 1)$ signatures with negligible probability, if the adversary does not know the signer's secret key.

In this section, we will prove that our scheme is secure against this attack even under the novel parallel attack as illustrated in [9]. Our proof of security is based on the ROS-problem, Random Oracle Model (ROM), Generic Group Model (GM) [14-15], and the hardness of discrete logarithm problem.

The ROS-problem is to find an over-determined solvable system of linear equations modulo *q*, where the right-hand side is random inhomogeneities. The ROS-problem is related to a NP-complete problem [10]. If solving the ROS-problem is feasible, then the schemes of Schnorr signature [16] and Okamoto-Schnorr signature [11-12,17] are breakable to the attack of one-more forgery as shown in [9]. Hence, it is reasonable to add the assumption of intractability of the ROS-problem in the proof of security.

For easy reading, we introduce some terminology of GM; further details please refer to [9, 14-15, 18-20]. In the GM, the manipulations on group elements are not dependent on its representation. A generic step for group element is multivariate exponentiations, *i.e.*

$$Z_q^d \times G^d \rightarrow G,\ (b_1,\ldots,b_d,\ g_1,\ldots,\ g_d) \mapsto \prod_{i=1}^{d} g_i^{b_i}\ ,$$

where $d \geq 0$. Queries to the hash oracle and interactions with the signer are also generic step. A generic non-interactive generic algorithm is a sequence of t generic steps: Giving t' group elements $f_1,\ldots,f_{t'}$, computes the set of t - t' group elements $\{f_i \mid f_i = \prod_{j=1}^{i-1} f_j^{b_j}\ ,\ i = t' + 1,\ldots,t\}$, where non-group elements $b_1,\ldots,b_{i-1} \in Z_q$ depend arbitrarily on i and the set of the previous collision of group elements.

A generic adversary is an adversary in the model of ROM + GM. Assume that a generic adversary A is given the public parameters: the group G of prime order q, generator g of G, signer's public keys (y_1, y_2), and an oracle for $H(.)$. Also assume the adversary A has performed t generic steps including l times of signer interactions, *i.e.* the adversary A can construct at least l valid signatures. We want to prove that A cannot have probability of success better than $(\,^{t}_{2}) / q$, if A conduct a parallel attack to produce $l + 1$ valid signatures, *i.e.* the one-more signature forgery under the adaptively parallel attack.

Since the adversary A has conducted t generic steps including l interactions with the signer. Hence, the signer has generated the set of tuples $\{(w_i,\ s_i,\ g_i) \mid g_i = g^{w_i} \in G,\ w_i \in_R Z_q,\ s_i = w_i + c_i\,(x_1 + z_i\,x_2) \in Z_q,\ z_i = H(info_i),$ c_i is the i_{th} challenge of adversary A , $i = 1, 2,\ldots l\}$. For simplifying the discussions and notations, the tuples do not include the group elements ID_u, g_1, r_u and y_u. But, the omission will have no effect on the final result. Also assume the adversary A has produced some t' elements of G and queried t'' times to the hash oracle, where $t = t' + t''$. Let $f = \{f_1 = g, f_2 = y_1, f_3 = y_2, f_4,\ldots,f_{t'} \in G\}$ be the set of t' elements generated by A, where

$$f_i = g^{a_{i,-2}}\ y_1^{a_{i,-1}}\ y_2^{a_{i,0}}\ \ \Pi_{j=1}^{l} g_j^{a_{i,j}}$$

for $i = 1, 2,\ldots, t'$. For example, the exponents of group element f_1 are $a_{1,-2} = 1$, $a_{1,-1} = a_{1,0} = \ldots = a_{1,l} = 0$. Obviously, the adversary chooses exponents $a_{i,j} \in Z_q$ depending arbitrarily on the previously computed non-group data and collided group elements such that f_i is dependent on $f_{i-1}, f_{i-2},\ldots, f_1$.

In the following probabilistic analysis, the probability space consists of $H(.)$, y_1, y_2, and the signer's random coins w.

Lemma 2. The probability of triple collisions among the group elements $f_1, f_2,\ldots, f_{t'}$ is at most $\binom{t'}{3} / q^2$.

Proof. Let us define the discrete random variables X_{ijk} for $1 \le i < j < k \le t'$ as follow: $X_{ijk} = 1$ if collision occurs, i.e. $f_i = f_j = f_k$, but otherwise $X_{ijk} = 0$. The probability that $f_i = f_j = f_k$ is $1/q^2$, thus the expectation value of the discrete random variable is $E[X_{ijk}] = 1*(1/q^2) + 0*(1 - 1/q^2) = 1/q^2$. The expected number of collided triplets is just the sum of the expectations, that is, $\Sigma_{i=3}^{t'}\Sigma_{j=2}^{i-1}\Sigma_{k=1}^{j-1}E[\,X_{ijk}\,] = \binom{t'}{3}/q^2$. Since the trivial collisions (collision that is independent of the secret data) contribute no information to solve the secret data, we ignore the probability of trivial collisions. Thus, we have proved Lemma 2.

Lemma 3. If there occurs non-trivial triple collisions, then the secret data, i.e. $(x_1, x_2, w_1, \ldots, w_l)$, are solvable with overwhelming probability.

Proof. Assume the non-trivial collision triplet is $f_i = f_j = f_k$, we have $log_g^{f_i} = log_g^{f_j} = log_g^{f_k}$, where

$$log_g^{f_i} = a_{i,-2} + a_{i,-1} x_1 + a_{i,0} x_2 + \sum_{e=1}^{l} a_{i,e} w_e \ ,$$

$$log_g^{f_j} = a_{j,-2} + a_{j,-1} x_1 + a_{j,0} x_2 + \sum_{e=1}^{l} a_{j,e} w_e \text{ and}$$

$$log_g^{f_k} = a_{k,-2} + a_{k,-1} x_1 + a_{k,0} x_2 + \sum_{e=1}^{l} a_{k,e} k_e \ .$$

Combining these equations, we have

$$x_1 = b_{1,0} + \sum_{e=1}^{l} b_{1,e} w_e \text{ and}$$

$$x_2 = b_{2,0} + \sum_{e=1}^{l} b_{2,e} w_e \ .$$

Interacting with the signer l times, the adversary A has l linear polynomials $s_i = w_i + c_i (x_1 + a_i x_2)$ in $Z_q[x_1, x_2, w_1,\ldots, w_l]$, *i.e.* $x_1, x_2, w_1,\ldots, w_l$ are indeterminate variables over Z_q. For each polynomial, the variable x_1 and x_2 are replaced with $x_1 = b_{1,0} + \sum_{e=1}^{l} b_{1,e} w_e$ and $x_2 = b_{2,0} + \sum_{e=1}^{l} b_{2,e} w_e$. Thus, A has l linear polynomials in $Z_q[w_1,\ldots, w_l]$. Because the adversary chooses exponents $a_{i,j} \in Z_q$ depending arbitrarily on the previously computed non-group data, the l linear polynomials in $Z_q[w_1,\ldots, w_l]$ are solvable with overwhelming probability.

Lemma 4. The probability of two pair collisions among the group elements $f_1, f_2,\ldots, f_{t'}$ are at most $(\binom{t'}{2}/q)^2$.

Proof. By the same method for triple collisions, this Lemma is proved.

Lemma 5. If there occurs two non-trivial pair collisions, then the secret data, i.e. $(x_1, x_2, w_1, \ldots, w_l)$, are solvable with overwhelming probability.

Proof. By the same method for non-trivial triple collisions, this Lemma is proved.

Lemma 6. (The generic parallel attack) From the l interactions with the signer, the adversary A obtains $(l + 1)$ signatures with probability not better than $1 / q$, except he can solve ROS-problem or there exists group collisions or hash collisions.

Proof. Let the set of tuples $\{(w_j, g_j, c_j, s_j)| \; w_j \in_R Z_q, \; g_j = g^{w_j} \in G, \; j = 1,...,l\}$ describe the interactions. The signer sends g_j to the adversary A and responds $s_j = w_j + c_j (x_1 + z_j x_2)$ to A when receiving the challenge c_j, where $z_j = H(info_j)$. Suppose that the adversary A is able to constructs $l + 1$ different valid signatures $(m_i, info_i, c'_i, s'_i)$, $i = 1,..., l+1$. Then, $c'_i = H(g|| \; g_1|| \; y_1|| \; y_2|| \; m_i|| \; info_i|| \; g^{s'_i} (y_1 y_2^{z_i})^{-c'_i})$. (The discussion on ID_u and y_u was omitted. It could be done in a similar way.)

Because the adversary has generated t' distinct group elements, he obtained the set $f = \{f_1 = g, f_2 = y_1, f_3 = y_2, f_4,...f_{t'} \in G\}$ of group elements. In addition, he has queried t'' times to the hash oracle, *i.e.* $c_k = H(g|| \; g_1|| \; y_1|| \; y_2|| \; m_k|| \; info_k|| \; f_k)$ for $k = 1,...,t''$ and $f_k \in f$. Therefore, there is a mapping for $i = 1,..., l+1$ such that $g^{s'_i} (y_1 y_2^{z_i})^{-c'_i} = f_{ki} \in f$ and $f_k = f_{ki}$ for some $k \in \{1,..., t''\}$. Thus, A has the following equations.

$$g^{s'_i} (y_1 y_2^{z_i})^{-c'_i} = g^{s'_i - c'_i x_1 - c'_i z_i x_2} \tag{1}$$

$$f_{ki} = g^{a_{ki,-2} + a_{ki,-1} x_1 + a_{ki,0} x_2 + \sum_{j=1}^{l} a_{ki,j} w_j} \tag{2}$$

$$= g^{a_{ki,-2} + a_{ki,-1} x_1 + a_{ki,0} x_2 + \sum_{j=1}^{l} a_{ki,j} (s_j - c_j x_1 - c_j z_j x_2)}$$

From equations (1) and (2), we deduce the equation below.

$$s'_i = a_{ki,-2} + \Sigma_{j=1}^{l} a_{ki,j} s_j + (c'_i + a_{ki,-1} - \Sigma_{j=1}^{l} a_{ki,j} c_j) \, x_1 + \tag{3}$$

$$(c'_i z_i + a_{ki,0} - \Sigma_{j=1}^{l} a_{ki,j} c_j z_j) \, x_2$$

Since $x_1$and x_2 are signer's secret key, the adversary can successfully compute s'_i if he can set the coefficient of x_1 and x_2 to zero, i.e. $(c'_i + a_{ki,-1} - \Sigma_{j=1}^{l} a_{ki,j} c_j) = (c'_i z_i + a_{ki,0} - \Sigma_{j=1}^{l} a_{ki,j} c_j z_j) = 0$. This implies the adversary can find $c_1, c_2,..., c_l$ so as to zero the coefficient of x_1 and x_2 in equation (3). Thus, the adversary solves the unknown variables $c_1, c_2, \ldots, c_l$ from the following t'' linear equations modulo q with random inhomogeneities in right hand-side, *i.e.* solve (4) or (5).

$c_k = -a_{k,-1} + \sum_{j=1}^{l} a_{k,j} c_j = H(g|| g_1|| y_1|| y_2|| m_k|| info_k|| f_k)$, for $k=1,\ldots,t''$ and $f_k \in f$. (4)

$c_k = (-a_{k,0} + \sum_{j=1}^{l} a_{k,j} c_j)(z_k)^{-1} = H(g|| g_1|| y_1|| y_2|| m_k|| info_k|| f_k)$. (5)

The suggestion of solving (4) or (5) contradicts the assumption that the ROS-problem is hard. Thus, even under the parallel attack, the adversary cannot have probability of success better than $1 / q$ (the probability of guessing the challenges), if there are no collisions of group elements and hash values.

Theorem 7. From the l interactions with the signer, the adversary A obtains $(l + 1)$ signatures with probability not better than $1/q+ (\binom{t'}{2}/q)^2 +\binom{t'}{3}/q^2 +\binom{t''}{2}/q \le \binom{t}{2}/q$.

Proof. The adversary can achieve his goal by:

1. Collisions of group elements,
2. Parallel attack, and
3. Collisions of hash values.

By Lemma 2-5, the probability of the first case is at most $(\binom{t'}{2}/q)^2 +\binom{t'}{3}/q^2$. By Lemma 6, the probability of the second case is at most $1/q$.

Considering the third case, *i.e.* $(m_k, info_k, c'_i, s'_i)$ is a valid signature and $c'_i = c_{ki} = H(g|| g_1|| y_1|| y_2|| m_k|| info_k|| f_{ki}) = c_{kj} =H(g|| g_1|| y_1|| y_2|| m_k|| info_k|| f_{kj})$, where $ki, kj \in \{1,\ldots, t''\}$, $ki \neq kj$ and $f_{ki} \neq f_{kj}$. From equations (4) and (5), we have $a_{ki,b} = a_{kj,b}$ for $b = -1, 0,\ldots, l$. Thus, from equation (3), the adversary can compute $s'_j = (s'_i - a'_{i,-2}) + a'_{j,-2}$ without knowing the signer's secret keys. The tuple $(m_k, info_k, c'_j, s'_j)$ is the $(l + 1)_{th}$ signature, where $c'_j = c'_i$. The probability of the third case is at most $\binom{t''}{2}/q$, by a similar analysis to Lemma 2. Therefore, combining the three cases, we have completed the proof.

5. Performances

Table 1 displays the comparisons of the proposed scheme and the scheme in [7]. In estimating the computational complexity, we count only the modular operations of exponentiation. As shown in Table 1, the computational cost for signer, user and verifier are all reduced. In addition, the proposed scheme has smaller message size than the one in scheme [7].

Table 1: The comparisons of proposed scheme and scheme [7]

	Proposed scheme	Scheme [7]
Signer's computations	*3*	*5*
User's computations	*13*	*17*
Verifier's computations	*5*	*6*
Signature size	$2*\|M\| + 2*\|p\| + 2*\|q\|$	$2*\|M\| + 2*\|p\| + 4*\|q\|$

6. Conclusions

We have proposed a secure scheme for restrictive partially blind signatures. The proposed scheme is secure up to polynomial number of circulated signatures. The computational cost for the signer and the user are drastically decreased. The relief of computing is valuable, since the signer would be the bottleneck in the environment of electronic cash. The extension of issued signatures enhances the security of application system.

References

[1] D. Chaum, "Blind signatures for untraceable payments," *Advances in Cryptology-CRYPTO'82*, pp. 199-203, 1983.

[2] M. Abe and E. Fujisaki, "How to date blind signatures," *Advances in Cryptology-ASIACRYPT'96*, LNCS 1163, pp. 244-251, 1996.

[3] M. Abe and T. Okamoto, "Provably secure partially blind signatures," *Advances in Cryptology-CRYPTO'00*, LNCS 1880, pp. 271-286, 2000.

[4] D. Chaum and T. Pryds Pedersen, "Wallet databases with observers," *Advances in Cryptology-CRYPTO'92*, LNCS 740, pp. 89-105, 1992.

[5] S. Brands, "An efficient off-line electronic cash system based on the representation problem," *CWI Technical Report CS-R9323,* Centrum voor Wiskunde en Informatica (CWI), 1993.

[6] S. Brands, "Untraceable off-line cash in wallets with observers," *Advances in Cryptology-CRYPTO'93*, LNCS 773, pp. 302-318, 1993.

[7] G. Maitland and C. Boyd, "A provably secure restrictive partially blind signature scheme," *PKC 2002*, LNCS 2274, pp. 99-114, 2002.

[8] D. Pointcheval, "Strengthened security for blind digital signatures," *Advances in Cryptology-EUROCRYPT'98*, LNCS 1403, pp. 391-405, 1998.

[9] C. P. Schnorr, "Security of blind discrete log signatures against interactive attacks," *ICICS 2001,* LNCS 1880, pp. 1-12, 2001.

[10] J. Hastad, "Some optimal inapproximability results," *Proceedings of ACM Symposium on Theory of Computing 1997*, pp. 1-10, 1997.

[11] D. Pointcheval and J. Stern, "Provably secure blind signature schemes," *Advances in Cryptology-ASIACRYPT'96*, LNCS 1163, pp. 252-265, 1996.

[12] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, Vol. 13, N0. 3, pp. 361-396, 2000.

[13] A. Juels, M. Luby and R. Ostrovsky, "Security of blind digital signatures," *Advances in Cryptology-CRYPTO'97*, LNCS 1294, pp. 150-164, 1997.

[14] V. I. Nechaev, "Complexity of a determinate algorithm for the discrete

logarithm," *Math.* Notes 55, pp. 165-172, 1994.

[15] V. Shoup, "Lower bounds for discrete logarithms and related problems," *Advances in Cryptology-EUROCRYPT'97*, LNCS 1233, pp. 256-266, 1997.

[16] C. P. Schnorr, "Efficient signature generation for smart cards," *Journal of Cryptology,* Vol. 4, pp. 161-174, 1991.

[17] T. Okamoto, "Provably secure identification schemes and corresponding signature schemes," *Advances in Cryptology-CRYPTO'92*, LNCS 740, pp. 31-53, 1992.

[18] C. P. Schnorr, "Small generic hardcore subsets for the discrete logarithm: short secret DL-Keys," *Information and Processing Letters,* Vol. 79, pp. 93-98, 2001.

[19] C. P. Schnorr and M. Jakobsson, "Security of signed ElGamal Encryption," *Advances in Cryptology-ASIACRYPT 2000*, LNCS 1976, pp. 73-89, 2000.

[20] M. Fischlin, "A note on security proofs in the generic model," *Advances in Cryptology-ASIACRYPT 2000*, LNCS 1976, pp. 458-469, 2000.