用戶端高效率之隨機化 Chaum 盲簽章機制

User Efficient Randomized Chaum's Blind Signatures

范俊逸 Chun-I Fan
中華電信公司 電信研究所
桃園縣楊梅鎮民族路五段 551 **巷** 12 **號**
Telecommunication Laboratories
Chunghwa Telecom Co., Ltd.
12, Lane 551, Min-Tsu Road Sec. 5
Yang-Mei, Taoyuan, Taiwan 326, R.O.C.
TEL: +886-3-424-5081
FAX: +886-3-424-4147
E-mail: chunifan@ms35.hinet.net

陳維魁 Wei-Kuei Chen
清雲技術學院 資訊管理系
桃園縣中壢市健行路 229 **號**
Ching-Yun Institute of Technology
Department of Information Management
229, Chien-Hsin Road, Chung-Li, Taiwan 320
TEL: +886-3-458-1196
FAX: +886-3-402-9539
E-mail: weikchen@ms31.hinet.net

摘要

本論文提出一個新型的隨機化 Chaum **盲簽章機制，減輕了用戶的計算負擔，以適合於計算能力受限的用戶環境，例如智慧卡使用者與行動通訊用戶。和原始的機制相比，用戶端的計算量降低了** 40%**；而如果使用了較短的公開金鑰，例如** $e = 3$**，則可降低用戶端的計算量達** 95%**以上。另外，本論文也檢驗了此盲簽章機制之隨機化與不可連結等特性。**

關鍵字：盲簽章、電子現金、電子投票、密碼學

Abstract

This manuscript presents a new randomized Chaum's blind signature scheme to reduce users' computation loads for the situations where their computation capabilities are limited such as smart-card customers and mobile clients. Comparing with the original scheme, the computations required for users are reduced by about 40% in general and more than 95% if we take a short key $e = 3$. In addition, the randomization and unlinkability of the proposed scheme are examined.

Keywords: Blind signatures, Electronic cash, Electronic voting, Cryptography

1 Introduction

The concept of blind signatures was first introduced by Chaum [2] to prevent digital signatures from being forged and to protect the privacy of users. Based on the RSA cryptosystem, Chaum proposed the first blind signature scheme to achieve the unlinkability property [2]. By means of the techniques of blind signatures, many anonymous electronic voting protocols [1, 5, 11] and untraceable electronic cash systems [3, 10, 14, 15] have been proposed.

In general, two kinds of roles, a signer and a group of users, participate in a blind signature protocol. A user blinds a message by performing an encryption-like process (or a blinding process) on the message, and then submits the blinded message to the signer to request the signer's signature on the blinded message. The signer signs on the blinded message by using its signing

function, and then sends the signing result back to the user. Finally, the user unblinds the signing result to obtain the exact signature on the message by performing a decryption-like operation (or an unblinding operation) on the signing result he receives. The signature on the message can be verified by checking whether the corresponding public verification formula with the signature-message pair as parameters is true or not. In a secure blind signature scheme, it is computationally infeasible for the signer to derive the link between a signature and the instance of the signing protocol which produces the blinded form of that signature. This is usually referred to as the unlinkability or blindness property.

In [9], a modified Chaum's blind signature scheme was proposed to enhance the randomization of the signatures against the chosen-text attacks of [6] by injecting randomization factors into the signatures. However, the randomization factors can be removed from the signatures by the users such that the randomization is lost. This manuscript presents a method to repair the weakness and the improved scheme is more user efficient than that of [9].

2 Related Works

In this section, we review Chaum's blind signature scheme [2] and Fan-Chen-Yeh blind signature scheme [9].

2.1 Chaum's Blind Signature Scheme

Chaum's blind signature scheme contains five stages, initializing, blinding, signing, unblinding, and verifying. In the initializing stage, the signer publishes the necessary information such as the public keys. The stage can be pre-performed just once. To request the signature on a message, the user blinds the message and submits the blinded message to the signer in the blinding stage. In the signing stage, the signer signs on the blinded message and sends the signing result back to the user. After receiving the signing result, the user performs the unblinding operation on it to obtain the exact signature on the message in the unbinding stage. Finally, the signature is verified in the verifying stage. The protocol is described below.

(1) Initializing. Initially, the signer randomly selects two distinct large primes p and q, and then computes $n = pq$ and $\phi(n) = (p-1)(q-1)$. The signer chooses two integers e and d at random such that $ed \equiv 1 \pmod{\phi(n)}$. Then, it publishes (e, n) and a one-way hash function H such as SHA-1 [13].

(2) Blinding. A user chooses a message m and randomly selects an integer r in Z_n^* which is the set of all positive integers less than and relatively prime to n. The user computes and submits the integer $\alpha = (r^e H(m) \bmod n)$ to the signer.

(3) Signing. After receiving α, the signer computes and sends the integer $t = (\alpha^d \bmod n)$ to the user.

(4) Unblinding. After receiving t, the user performs the unblinding process to obtain $s = (r^{-1}t \bmod n)$. The integer s is the signature on m.

(5) Verifying. The signature-message pair (s, m) can be verified by checking if $s^e \equiv H(m) \pmod{n}$.

Given (s, m), the signer cannot derive the link between (s, m) and α due to the blinding factor r. This is the unlinkability or blindness property.

2.2 Fan-Chen-Yeh Blind Signature Scheme

Fan-Chen-Yeh blind signature scheme [9] is a variant of Chaum's scheme with an injected randomization factor for each issued signature. The scheme is described below.

(1) Initializing. According to the key generation of Chaum's blind signature scheme shown in section 2.1, the public and private keys of the signer are (e, n) and (p, q, d), respectively. Let H be a public one-

way hash function.

(2) Blinding. To request a signature on a message m, the user randomly chooses an integer r in Z_n^* and a positive integer u less than n, and then computes and submits the integer $\alpha = (r^e H(m)(u^2+1) \bmod n)$ to the signer. After receiving α, the signer randomly selects a positive integer x less than n and sends it to the user. After receiving x, the user randomly chooses an integer b in Z_n^*, and then computes $b = (b^e(u-x) \bmod n)$. Finally, the user submits the integer b to the signer.

(3) Signing. After receiving b, the signer computes $t = ((\alpha (x^2+1)b^{-2})^d \bmod n)$, and then the signer sends t to the user. The integer x is said to be the randomizing factor.

(4) Unblinding. After receiving t, the user computes

$$\begin{cases} c = (ux+1)(u-x)^{-1} \bmod n \text{ and} \\ s = r^{-1} b^2 t \bmod n. \end{cases}$$

(5) Verifying. The integer s is the signature on the tuple (c, m). To verify (c, m, s), one can examine if $s^e \equiv H(m)(c^2+1) \pmod n$.

However, the randomization factor x can be removed by the user. In the blinding stage, the user forms $b = ((x^2+1)^{\frac{qe+1}{2}} \bmod n)$ with an arbitrary odd number q such as $q = 1$, and sends b to the signer. After receiving b, the signer computes $t \equiv (\alpha(x^2+1)b^{-2})^d \equiv (\alpha (x^2+1)(x^2+1)^{-\theta e-1})^d \equiv (x^2+1)^{-\theta}\alpha^d \pmod n$, and sends t to the user. After receiving t, the user computes $((x^2+1)^q t \bmod n)$ to obtain $(\alpha^d \bmod n)$ which does not contain the randomization factor x.

3 User Efficient Randomized Chaum's Blind Signature Scheme

In this section we present a randomized Chaum's blind signature scheme to repair the weakness of the randomization in [9] and make it efficient for the users to request and verify the signatures. The details of the proposed scheme are described as follows.

(1) Initializing. Initially, the signer randomly selects two distinct large primes p and q such that $p \equiv q \equiv 3 \pmod 4$, and then computes $n = pq$ and $\phi(n) = (p-1)(q-1)$. The signer chooses two integers e and d at random such that $ed \equiv 1 \pmod{\phi(n)}$. Then, it publishes (e, n) and a one-way hash function H.

(2) Blinding. To request a signature on a message m, the user randomly chooses two integers r, v in Z_n^* and a positive integer u less than n, and then computes and submits the integer $\alpha = (r^{2e} H(m)(u^2+1) \bmod n)$ to the signer. After receiving α, the signer randomly selects a positive integer x less than n such that $(\alpha(x^2+1) \bmod n)$ is a quadratic residue (QR)[1] in Z_n^*, and then sends x to the user. After receiving x, the user computes $b = (rv \bmod n)$, $\delta = (b^e \bmod n)$, and $\beta = (\delta(u-x) \bmod n)$. Finally, the user submits the integer β to the signer.

(3) Signing. After receiving β, the signer computes $\lambda = (b^{-1} \bmod n)$ and a square root t of $((\alpha(x^2+1)\lambda^2)^d \bmod n)$ in Z_n^* such that $t^2 \equiv (\alpha(x^2+1)\lambda^2)^d \pmod n$. The signer sends t and λ to the user. The integer x is the randomizing factor.

(4) Unblinding. After receiving (t, λ), the user computes

$$\begin{cases} c = dl\,(ux+1) \bmod n \text{ and} \\ s = tv \bmod n \end{cases}$$

(5) Verifying. The integer s is the signature on the tuple (c, m). To verify (c, m, s), one can examine if $s^{2e} \equiv H(m)(c^2+1) \pmod n$.

[1] Under a modulus n, w is a quadratic residue (QR) in Z_n^* if and only if there exists an integer y in Z_n^* such that $y^2 \equiv w \pmod n$. Given w and n, it is intractable to compute the square root y of w in Z_n^* if n contains large prime factors and the factorization of n is unknown [19].

4 Discussions

In this section we examine the correctness and security of the proposed scheme. First, from the protocol of section 3, we have the following theorem to ensure the correctness of the protocol.

Theorem 1. If a triple (c, m, s) is produced by the proposed scheme, then

$$s^{2e} \equiv H(m)(c^2+1) \pmod{n}$$

Proof. By the Chinese remainder theorem [21], an integer w in Z_n^* can be represented by $< w_1, w_2 >$ where $w_1 = (w \bmod p_1)$ and $w_2 = (w \bmod p_2)$. For convenience, $< w_1, w_2 >$ is denoted by $< w >$ sometimes. For each $< k >$ = $<k_1, k_2>$ and $< w >$ = $< w_1, w_2 >$ in Z_n^*, $< kw \bmod n >$ = $< k_1 w_1 \bmod p_1, k_2 w_2 \bmod p_2>$, and $< k^{-1} \bmod n >$ = $<k_1^{-1} \bmod p_1, k_2^{-1} \bmod p_2>$. In addition, for each $< k_1, k_2>$ and $< w_1, w_2 >$ in Z_n^*, $< k_1, k_2 >$ = $< w_1, w_2 >$ if and only if $k_1 \equiv w_1 \pmod{p_1}$ and $k_2 \equiv w_2 \pmod{p_2}$.

Let $\left[\frac{q}{h}\right]$ denote the Legendre symbol g over h where h is a prime [21]. Since both ($\alpha(x^2+1) \bmod n$) and ($\lambda^2 \bmod n$) are QR's in Z_n^*,

$$\left[\frac{a(x^2+1)l^2}{p_1}\right] = \left[\frac{a(x^2+1)}{p_1}\right]\left[\frac{l^2}{p_1}\right] = 1 \cdot 1 = 1$$

and

$$\left[\frac{a(x^2+1)l^2}{p_2}\right] = \left[\frac{a(x^2+1)}{p_2}\right]\left[\frac{l^2}{p_2}\right] = 1 \cdot 1 = 1$$

Therefore, we have that ($\alpha(x^2+1)\lambda^2 \bmod n$) is a QR in Z_n^*, and

$$\begin{aligned}
&(\alpha(x^2+1)\, l^2)^d \\
&\equiv (\alpha(x^2+1)b^{-2})^d \\
&\equiv (r^{2e}H(m)(u^2+1)(x^2+1)(b^e(u-x))^{-2})^d \\
&\equiv (b^{-2e}r^{2e}H(m)(u^2+1)(x^2+1)(u-x)^{-2})^d \\
&\equiv (b^{-2e}r^{2e}H(m)((ux+1)^2+(u-x)^2)(u-x)^{-2})^d \\
&\equiv (b^{-2e}r^{2e}H(m)((ux+1)^2(u-x)^{-2}+1))^d \\
&\equiv (b^{-2e}r^{2e}H(m)(((ux+1)(u-x)^{-1})^2+1))^d \\
&\equiv (b^{-2e}r^{2e}H(m)((b^e b^{-e}(u-x)^{-1}(ux+1))^2+1))^d \\
&\equiv (b^{-2e}r^{2e}H(m)((b^e l(ux+1))^2+1))^d \\
&\equiv (b^{-2e}r^{2e}H(m)(c^2+1))^d \\
&\equiv b^{-2}r^2H(m)^d(c^2+1)^d
\end{aligned}$$

is a QR in Z_n^*, too. Because

$$\left[\frac{b^{-2}r^2}{p_1}\right] = \left[\frac{b^{-2}r^2}{p_2}\right] = 1$$

the integer ($H(m)^d(c^2+1)^d \bmod n$) also is a QR in Z_n^* and there are 4 different square roots of ($H(m)^d(c^2+1)^d \bmod n$) in Z_n^* [19]. Let $< w_1, w_2 >$ be one of the square roots of the integer ($H(m)^d(c^2+1)^d \bmod n$) in Z_n^*, then the four square roots of the integer in Z_n^* are $< \pm w_1 \bmod p_1, \pm w_2 \bmod p_2>$. Thus, the four square roots of ($b^{-2}r^2H(m)^d(c^2+1)^d \bmod n$) in Z_n^* are $< \pm b_1^{-1}r_1 w_1 \bmod p_1, \pm b_2^{-1}r_2 w_2 \bmod p_2>$. As $t^2 \equiv b^{-2}r^2H(m)^d(c^2+1)^d \pmod{n}$, t belongs to $\{< \pm b_1^{-1}r_1 w_1 \bmod p_1, \pm b_2^{-1}r_2 w_2 \bmod p_2>\}$. Since $s = (tv \bmod n) = (tbr^{-1} \bmod n)$, s is an element in $\{< \pm b_1 b_1^{-1} r_1^{-1} r_1 w_1 \bmod p_1, \pm b_2 b_2^{-1} r_2^{-1} r_2 w_2 \bmod p_2>\}$ = $< \pm w_1 \bmod p_1, \pm w_2 \bmod p_2>$. It follows that s is a square root of the integer ($H(m)^d(c^2+1)^d \bmod n$) in Z_n^*. Hence, $s^2 \equiv H(m)^d(c^2+1)^d \pmod{n}$. Thus, we have that $s^{2e} \equiv H(m)(c^2+1) \pmod{n}$.

4.1 Randomization

In the proposed scheme, the attackers can choose m but that they cannot choose (c, m) on which a signature is computed due to the randomizing factor x.

In the blinding stage, if the user forms b = $((x^2+1)^{\frac{qe+1}{2}} \bmod n)$ with an odd number q, and sends b to the signer. After receiving b, the signer computes an integer t such that $t^2 \equiv (\alpha(x^2+1)b^{-2})^d \equiv (\alpha(x^2+1)(x^2+1)^{-\theta e-1})^d \equiv (x^2+1)^{-\theta}\alpha^d \pmod{n}$, and sends t to the user. After receiving t, the user cannot derive any of the four square roots of $((x^2+1)^{-\theta} \bmod n)$ to remove x from t since q is odd and computing a square root of the integer in Z_n^* is intractable without the factorization of n [19].

Given an integer s, attackers can derive (w, y) such that $s^{2e} \equiv (w^2+y^2) \pmod{n}$ by [16] without p and q. However, it is still intractable to compute a square root c of (w^2+y^2-1) in Z_n^* such that $s^{2e} \equiv (c^2+1) \pmod{n}$ without

the factorization of n [19], and deriving an integer s' such that $(s')^{2e} \equiv ((y^{-1}w)^2+1) \pmod{n}$ depends on the security of [20] since $s' = (y^{-e^{-1}} s \bmod n)$.

4.2 Unlinkability

For each instance, numbered i, of the proposed protocol, the signer can record the transmitted messages (α_i, b_i, x_i) between the user and the signer during the instance i of the protocol. The triple (α_i, b_i, x_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 2. Given a triple (c, m, s) produced by the proposed scheme, the signer can derive b_i', r_i', and u_i' for each (α_i, b_i, x_i) such that

$$\begin{cases} c \equiv (u_i' x_i + 1)(u_i' - x_i)^{-1} \pmod{n}, \\ a_i \equiv (r_i')^{2e} H(m)((u_i')^2 + 1) \pmod{n}, \text{ and} \\ b_i \equiv (b_i')^e (u_i' - x_i) \pmod{n} \end{cases}$$

Proof. If $c \equiv (u_i' x_i+1)(u_i' - x_i)^{-1} \pmod{n}$, we have that $u_i' \equiv (cx_i+1)(c-x_i)^{-1} \pmod{n}$.

If $\alpha_i \equiv (r_i')^{2e} H(m)((u_i')^2+1) \pmod{n}$, then we have the followings,

$\alpha_i \equiv (r_i')^{2e} H(m)((cx_i+1)^2(c-x_i)^{-2}+1) \pmod{n}$

$\alpha_i \equiv (r_i')^{2e} H(m)((cx_i+1)^2+(c-x_i)^2)\ (c-x_i)^{-2} \pmod{n}$

$\alpha_i \equiv (r_i')^{2e} H(m)((c^2+1)(x_i^2+1)\ (c-x_i)^{-2} \pmod{n}$

$\alpha_i \equiv (r_i')^{2e} s^{2e} (x_i^2+1)\ (c-x_i)^{-2} \pmod{n}$

$(r_i')^{2e} \equiv \alpha_i s^{-2e}\ (x_i^2+1)^{-1}\ (c-x_i)^2 \pmod{n}$

$(r_i')^2 \equiv \alpha_i^d s^{-2}\ (x_i^2+1)^{-d}\ (c-x_i)^{2d} \pmod{n}$

Since $((\alpha_i (x_i^2+1)^{-1})^d \bmod n)$, $((s^{-1})^2 \bmod n)$, and $(((c-x_i)^d)^2 \bmod n)$ are QR's, the signer can obtain 4 different values of r_i' in Z_n^*.

If $b_i \equiv (b_i')^e (u_i' - x_i) \pmod{n}$, we have that

$b_i \equiv (b_i')^e ((cx_i+1)(c-x_i)^{-1} - x_i) \pmod{n}$

$(b_i')^e \equiv b_i ((cx_i+1)(c-x_i)^{-1} - x_i)^{-1} \pmod{n}$

$b_i' \equiv b_i^d ((cx_i+1)(c-x_i)^{-1} - x_i)^{-d} \pmod{n}$

Hence, given a triple (c, m, s) produced by the protocol, the signer can always derive the three blinding factors b_i', r_i', and u_i' for each view (α_i, b_i, x_i). It turns out that all of the signature-message triples are indistinguishable from the signer's point of view. Therefore, it is computationally infeasible for the signer to derive the link between an instance i of the protocol and the blind signature produced by that protocol.

4.3 Performance

Typically, under a modulus n, the computation time for a modular exponentiation operation is about $O(|n|)$ times that of a modular multiplication where $|n|$ denotes the bit length of n [21]. The modulus n is usually taken about 1024 bits or more in a practical implementation [13, 21]. In [4, 8], some fast modular exponentiation algorithms are proposed. In [8], it requires 0.3381|n| modular multiplications and large amount of storage, e.g. 83370 stored values for a 512-bit modulus, to perform a modular exponentiation computation. An enhanced version of [8] is introduced in [4]. However, it still requires 0.3246$|n|$ modular multiplications and large amount of storage, e.g. 36027 stored values for a 512-bit modulus, to perform a modular exponentiation computation [4]. Besides, an inverse computation in Z_n^* takes about the same time as that of a modular exponentiation computation in Z_n^*, and a hashing computation does not take longer time than that of a modular multiplication computation [21].

In the proposed blind signature scheme, 3 modular exponentiation computations are performed by a user, while 3 modular exponentiations and 2 inverse computations are required for a user in the original scheme [9]. Compared to [9], the proposed scheme reduces the amount of computations for users by about 40%. In addition, if a short public key $e = 3$ is adopted and we take a modular exponentiation computation to be 0.3246$|n|$ modular multiplications [4], the proposed method largely reduces the amount of computations for

users by more than 95% under a 1024-bit modulus since no inverse computation and modular exponentiation is needed for users in the proposed scheme.

In the proposed scheme, the signer performs 1 modular exponentiation computation, 1 square root computation, and 1 inverse computation in Z_n^*. Comparing with [9], the proposed protocol does not decrease the computation load for the signer. However, in most of the applications based on blind signatures, the signer usually possesses much more computation capabilities than a user such as the bank of an untraceable electronic cash system or the tally center of an anonymous electronic voting protocol, while the computation capabilities of the users are limited in some situations such as mobile clients and smart-card users. Hence, to guarantee the quality of these ever-growing popular communication services based on blind signatures, it is more urgent to reduce the computation load for the users than that for the signer.

5 Conclusions

We have proposed an improved randomized Chaum's blind signature scheme. The scheme greatly reduces users' computations for mobile and smart-card environments. By performing an additional square-root operation for signing, the weakness of the randomization in the original scheme has been repaired.

References

[1] Boyd, C. A., "A new multiple key ciphers and an improved voting scheme", Advances in Cryptology-EUROCRYPT'94, LNCS 434, Springer-Verlag, pp. 617-625, 1990.

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

[3] Chaum, D., Fiat, A., and Naor, M.,"Untraceable electronic cash", Advances in Cryptology-CRYPTO'88, LNCS 403, Springer-Verlag, pp. 319-327, 1990.

[4] Chen, C., Chang, C., and Yang, W., "Hybrid method for modular exponentiation with precomputation", IEE Electronics Letters, Vol. 32, No. 6, pp. 540-541, 1996.

[5] Cohen, J. D. and Fisher, M. J., "A robust and verifiable cryptographically secure election scheme", Proceedings of the 26th IEEE Symp. on Foundations of Computer Science, IEEE, pp. 372-382, 1985.

[6] Coron, J. S., Naccache, D., and Stern, J. P., "On the security of RSA padding", Advances in Cryptology-CRYPTO'99, LNCS1666, Springer-Verlag, pp. 1-18, 1999.

[7] Desmedt, Y. and Odlyzko, A., "A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes", Advances in Cryptology-CRYPTO'85, LNCS 218, Springer-Verlag, pp. 516-522, 1986.

[8] Dimitrov, V. and Cooklev, T., "Two algorithms for modular exponentiation using nonstandard arithmetics", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E78-A, No. 1, pp. 82-87, 1995.

[9] Fan, C. I., Chen, W. K., and Yeh, Y. S.," Randomization enhanced Chaum's blind signature scheme", Advances in Research and Application of Network Security, Computer Communications, Vol 23, No. 17, pp. 1677-1680, 2000.

[10]Ferguson, N., "Single term off-line coins", Advances in Cryptology-EUROCRYPT'93, LNCS 765, Springer-Verlag, pp. 318-328, 1994.

[11] Fujioka, A., Okamoto, T., and Ohta, K., "A practical secret voting scheme for large scale elections", Advances in Cryptology-AUSCRYPT'92, LNCS 718, Springer-Verlag, pp. 244-251, 1992.

[12] Goldwasser, S., Micali, S., and Rivest, R. L., "A

digital signature scheme secure against adaptive chosen-message attacks", Technical Report, MIT Lab., Computer Science,Cambridge, Mass. March, 1995.

[13] Menezes, A., van Oorschot, P., and Vanstone, S., "Handbook of Applied Cryptography", CRC Press LLC, 1997.

[14] Okamoto, T. and Ohta, K., "Universal electronic cash", Advances in Cryptology-CRYPTO'91, LNCS 576, Springer-Verlag, pp. 324-337, 1992.

[15] Pfitzmann, B. and Waidner, M., "Strong loss tolerance of electronic coin systems", ACM Transactions on Computer Systems, Vol. 15, No. 2, pp. 194-213, 1999.

[16] Pollard, J. M. and Schnorr, C. P., "An efficient solution of the congruence $x^2+ky^2 = m \pmod{n}$", IEEE Transactions on Information Theory, Vol. 33, No. 5, pp. 702-709, 1987.

[17] Pointcheval, D. and Stern, J., "Provably secure blind signature schemes", Advances in Cryptology-ASIACRYPT'96, LNCS1163, Springer-Verlag, pp. 252-265, 1996.

[18] Pointcheval, D. and Stern, J., "New blind signatures equivalent to factorization", Proceedings of the 4th ACM Conference on Computer and Communication Security, pp. 92-99, 1997.

[19] Rabin, M. O., "Digitalized signatures and public-key functions as intractable as factorization", Technical Report, MIT/LCS/TR212, MIT Lab., Computer Science, Cambridge, Mass. Jan, 1979.

[20] Rivest, R. L., Shamir, A., and Adleman, L.M., "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol. 21, No.2, pp. 120-126, 1978.

[21] Simmons, G., "Contemporary Cryptology: The Science of Information Integrity", IEEE Press, N.Y., 1992.