ELSEVIER

Computer Communications 23 (2000) 1677–1680

computer communications

www.elsevier.com/locate/comcom

Randomization enhanced Chaum's blind signature scheme

Chun-I Fan[a,1], Wei-Kuei Chen[b,*], Yi-Shung Yeh[b]

[a]*Telecommunication Laboratories, Chunghwa Telecom Co., Ltd., TT5081, 12, Lane 551, Min-Tsu Road Sec. 5, Yang-Mei, Taoyuan 326, Taiwan, ROC*
[b]*Department of Computer Science and Information Engineering, National Chiao Tung University, Hsin Chu 300, Taiwan, ROC*

Abstract

At Crypto'99, Dr Coron, Naccache, and Stern presented a signature forgery strategy of the RSA digital signature scheme. The attack is valid on Chaum's blind signature scheme, which has been applied to many practical applications such as electronic cash and voting. In this paper we propose a method to inject a randomizing factor into a message when it is signed by the signer in Chaum's blind signature scheme such that attackers cannot obtain the signer's signatures of the special form for the attack.

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

1. Introduction

The RSA cryptosystem [18] is one of the widely used techniques in encryption/decryption algorithms or digital signatures. In a secure digital signature scheme, the signature is the proof of the signer, and no one else can deliberately sign the message. This property is usually referred to as the *unforgeability* property. Based on the RSA cryptosystem, Dr Chaum proposed the first blind signature scheme in 1982 [4] to achieve the *unlinkability* property. Two parties, a signer and a group of users, participate in a blind signature protocol. The protocol is briefly described below. First, a user blinds a message by performing a blinding process on it. Secondly, the user submits the blinded message to the signer to request the signature on the blinded message. Thirdly, the signer signs the blinded message by using its signing function, and then sends the signing result back to the user. Finally, the user unblinds the signing results by performing an unblinding operation to obtain the signer's signature on his chosen message. 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, it is computationally infeasible for the signer to link a signature shown for verification to the instance of the signing protocol that produced that signature. This property is usually referred to as the unlinkability property [3,4,9,13,15,16]. Due to the unlinkability and unforgeability properties, the techniques of blind signatures have been widely used in many advanced electronic communication services where anonymity is indispensable, such as anonymous electronic voting [1,6,10,19] and untraceable electronic cash systems [2,3,5,9,13,14].

Dr Coron, Naccache, and Stern proposed a signature forgery of the RSA digital signatures at Crypto'99 [7]. This is a kind of chosen-message attack [11]. The attack described in [7] is a sophisticated variant of Desmedt–Odlyzko's method [8] where the attacker obtains the signatures of $m_1, m_2, \ldots, m_{\tau-1}$ and forges the signature of an m_τ that was never submitted to the signer. Let f be a redundancy function and alternatively denote one-way hash function, ISO 9796-2, PKCS #1 v2.0, ANSI X9.31, SSL-3.02 or an ISO 9796-1 variant [7]. Dr Coron, Naccache, and Stern assume that all messages are padded by f before being signed. Before interacting with the signer, the attacker selects τ smooth $f(m_i)$ values and expresses $f(m_\tau)$ as a multiplicative combination of the padded strings $f(m_1), \ldots, f(m_{\tau-1})$. The signature of m_τ is then forged by using the homomorphic property of RSA. By obtaining signatures on enough messages of a certain form from a legitimate signer, the attacker can forge signatures on additional messages without the help of the signer. Since these messages have to be of a special form, the signer can detect them before signing and then refuse to sign them. Thus the attack does not really affect the security of the RSA digital signatures. However, in Chaum's blind signature scheme, which is based on the typical RSA digital signatures, since the plain text messages are blinded by users in advance, the

* Corresponding author. P.O. Box 343, Chung Li, Taiwan 320. Tel.: +886-3-402-9538; fax: +886-3-402-9539.

E-mail addresses: chunifan@ms35.hinet.net (C.-I. Fan), weikchen@ms31.hinet.net (W.-K. Chen).

[1] Tel.: +886-3-424-5081; fax: +886-3-424-4920.

0140-3664/00/$ - see front matter
PII: S0140-3664(00)00254-1

signer cannot know the format or the content of the plain text messages when signing them. If the users do not follow some encoding rule specified by the signer to prepare their plain text messages, the signer cannot detect them out when signing. Hence, the attackers can obtain the signer's signatures of the messages that are of the special form of the attack [7] or depend on previously obtained signatures for other chosen-message attacks [11]. It turns out that the chosen-message attacks [7,11] are valid on Chaum's blind signature scheme.

RSA encryption/decryption and digital signature schemes have been widely used in many computer and information systems. Furthermore, many practical cryptographic techniques based on RSA cryptosystems have been proposed in the literature. Chaum's blind signature is one of the popular techniques based on RSA scheme since it can be applied to payment protocols in electronic commerce and anonymous electronic voting systems; it is urgent to enhance the security of Chaum's scheme for the quality of these advanced communication services. In this paper we propose a method to enhance the randomization of Chaum's blind signature scheme such that attackers cannot predict what the signer exactly signs to avoid threats from chosen-message attacks.

The rest of this paper is organized as follows. In Section 2, we review Chaum's blind signature scheme. A randomization enhanced version of Chaum's scheme is presented in Section 3. In Section 4, we discuss the security of the proposed scheme. Finally, we make a conclusion of this paper in Section 5.

2. Chaum's blind signature scheme

In Chaum's blind signature scheme, there are two kinds of participants, a signer and a group of users. Users request signatures from the signer and the signer computes and issues blind signatures to the users. The blind signature scheme is described as follows.

1. *Initializing.* Initially, the singer 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 large 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 [12].
2. *Blinding.* A user chooses a message m and randomly selects an integer τ 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 signer's signature on m.
5. *Verifying.* The signature–message pair (s, m) can be verified by checking if $s^e \equiv H(m) \pmod{n}$.

3. Randomization enhanced Chaum's scheme

In this section we present a method to inject a randomizing factor into every message when it is signed by the signer in Chaum's blind signature scheme, and users cannot eliminate these randomizing factors embedded in the signatures obtained from the signer. The details of the proposed scheme are described as follows.

1. *Initializing.* According to the key generation protocol of Chaum's blind signature scheme shown in Section 2, the public and private keys of the signer are (e, n) and (p, q, d), respectively. H is a public one-way hash function such as SHA-1.
2. *Blinding.* To request a signature of a message m, a 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 $\beta = (b^e(u - x) \bmod n)$. Finally, the user submits the integer β to the signer.
3. *Signing.* After receiving β, the signer computes $t = ((\alpha(x^2 + 1)\beta^{-2})^d \bmod n)$. 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

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

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

4. Discussions

In this section we examine the correctness and security of the proposed scheme presented in Section 3. 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 scheme of Section 3, then*

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

4.1. Randomization

In the proposed scheme, the attackers can choose m but they cannot choose (c, m) on which a signature will be

calculated due to the randomizing factor x. Theorem 2 shows that the randomizing factor x cannot be removed from the signature by the user.

Theorem 2. *In the signing phase of the blind signature protocol in Section 3, it is computationally infeasible for a user to obtain an integer t' from the signer such that $t' \equiv \alpha^d \pmod n$ where α is chosen by the user in the blinding phase.*

Proof. In the blinding phase of the proposed scheme in Section 3, a user chooses and submits the integer α to the signer, and then the user receives the integer x from the signer. If the user tries to select an integer β' such that $\alpha(x^2+1)\beta'^{-2} \equiv \alpha \pmod n$, and in the signing phase, obtains t' from the signer such that $t' \equiv \alpha^d \pmod n$, then he has to form β' such that $\beta'^2 \equiv (x^2+1) \pmod n$. Since x is randomly chosen by the signer and computing a square root of an integer in Z_n^* is intractable without the factorization of n [17], it is computationally infeasible for the user to obtain t' from the signer such that $t' \equiv \alpha^d \pmod n$ in the signing phase of the proposed protocol. ■

In addition, given (s, v, y) with $s^e \equiv (v^2+y^2) \pmod n$, it is intractable to compute a square root c of (v^2+y^2-1) in Z_n^* such that $s^e \equiv (c^2+1) \pmod n$ without the factorization of n [17], and deriving an integer s' such that $(s')^e \equiv ((y^{-1}v)^2+1) \pmod n$ depends on the security of [18] since $s' = (y^{-2e^{-1}} s \bmod n)$.

4.2. Unlinkability

For every instance, numbered i, of the protocol in Section 3, the signer can record the transmitted messages (α_i, β_i, x_i) between the user and the signer during the instance i of the protocol. The triple (α_i, β_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 3. *Given a triple*(c, m, s) *produced by the scheme of* Section 3, *the signer can derive b_i', r_i' and u_i' for every (α_i, β_i, x_i) such that*

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

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

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

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

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

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

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

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

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

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

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

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

According to the above derivations, the signer can derive $b_i{}'$, $r_i{}'$ and $u_i{}'$ for every recorded (α_i, β_i, x_i). ■

Hence, given a triple (c, m, s) produced by the protocol of Section 3, the signer can always derive the three blinding factors $b_i{}'$, $r_i{}'$ and $u_i{}'$ for every view (α_i, β_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 signature produced by that protocol.

5. Conclusions

If an attacker obtains signatures on enough messages of the certain form shown in [7] from a legitimate signer, he can forge signatures in Chaum's blind signature; the proposed randomization enhanced Chaum's scheme makes it computationally infeasible for the attacker to obtain signatures of the certain form for the attack [7], but it requires additional communication and computation overhead, such as two additional ways of communication, a signature–message triple instead of a tuple, three additional random number generations, an extra inverse and exponentiation computations.

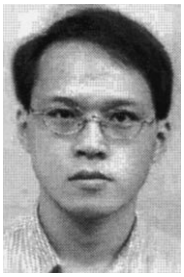
Acknowledgements

We would like to thank the anonymous referees of this paper for their valuable comments.

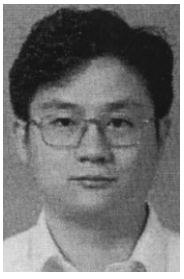
References

[1] C.A. Boyd, A new multiple key cipher and an improved voting scheme. Advances in Cryptology — EUROCRYPT'94, LNCS 434, Springer, 1990, pp. 617–625.
[2] S. Brands, Untraceable off-line cash in wallets with observers.

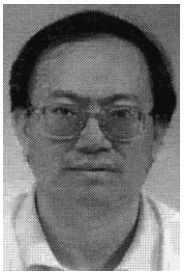
Advances in Cryptology — CRYPTO'93, LNCS 773, Springer, 1993, pp. 302–318.
[3] J. Camenisch, J.M. Piveteau, M. Stadler, An efficient fair payment system protecting privacy. Proceedings of ESORICS'94, LNCS 875, Springer, 1994, pp. 207–215.
[4] D. Chaum, Blind signatures for untraceable payments. Advances in Cryptology — CRYPTO'82, Plenum, 1983.
[5] D. Chaum, A. Fiat, M. Naor, Untraceable electronic cash. Advances in Cryptology — CRYPTO'88, LNCS 403, Springer, 1990, pp. 319–327.
[6] J.D. Cohen, M.J. Fisher, A robust and verifiable cryptographically secure election scheme. Proceedings of the 26th IEEE Symposium on Foundations of Computer Science, IEEE, 1985, pp. 372–382.
[7] J.S. Coron, D. Naccache, J.P. Stern, On the security of RSA padding. Advances in Cryptology — CRYPTO'99, LNCS 1666, Springer, 1999, pp. 1–18.
[8] Y. Desmedt, A. Odlyzko, A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes. Advances in Cryptology — CRYPTO'85, LNCS 218, Springer, 1994, pp. 318–328.
[9] N. Ferguson, Single term off-line coins. Advances in Cryptology — EUROCRYPT'93, LNCS 765, Springer, 1994, pp. 318–328.
[10] A. Fujioka, T. Okamoto, K. Ohta, A practical secret voting scheme for large scale elections. Advances in Cryptology — AUSCRYPT'92, LNCS 718, Springer, 1992, pp. 244–251.
[11] S. Goldwasser, S. Micali, R.L. Rivest, A digital signature scheme secure against adaptive chosen-message attacks, Technical Report, MIT Lab., Computer Science, Cambridge, Mass., March, 1995.
[12] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.
[13] T. Okamoto, K. Ohta, Universal electronic cash. Advances in Cryptology — CRYPTO'91, LNCS 576, Springer, 1992, pp. 324–337.
[14] B. Pfitzmann, M. Waidner, Strong loss tolerance of electronic coin systems, ACM Transactions on Computer Systems 15 (2) (1999) 194–213.
[15] D. Pointcheval, J. Stern, Provably secure blind signature schemes. Advances in Cryptology — ASIACRYPT'96, LNCS 1163, Springer, 1996, pp. 252–265.
[16] D. Pointcheval, J. Stern, New blind signatures equivalent to factorization. Proceedings of the 4th ACM Conference on Computer and Communication Safety, 1997, pp. 92–99.
[17] M.O. Rabin, Digitalized signatures and public-key functions as intractable as factorization, Technical Report, MIT/LCS/TR212, MIT Lab., Computer Science, Cambridge, Mass., Jan. 1979.
[18] R.L. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (2) (1978) 120–126.
[19] K. Sako, Electronic voting schemes allowing open objection to the tally , IEICE Transactions onFundamentals E77-A (1) (1994) 24–33.



Chun-I Fan was born in Tainan, Taiwan on October 15, 1967. He received his PhD degree in Electrical Engineering from National Taiwan University in 1998. In 1999, he joined the telecommunication laboratories of Chunghwa Telecom Co. Ltd., Taiwan, ROC. His current research interests include electronic cash, electronic voting, information security, and cryptographic protocols in distributed environments.



We-Kuei Chen was born in Taichung, Taiwan on February 13, 1968. He received the BS and Master degrees in the Department of CS and IE, National Chiao-Tung University in 1991 and 1993, respectively. He is working towards the PhD degree in the Department of CS and IE, National Chiao-Tung University now. His current research interests include electronic cash, electronic voting, and data security.



Yi-Shiung Yeh. Education. Sep. 1981–Dec 1985 PhD in Computer Science, Department of EE and CS, University Of Wisconsin-Milwaukee. Sep. 1978–June 1980 MS in Computer Science, Department of EE and CS, University Of Wisconsin-Milwaukee.
Professional background. Aug. 1988 to the present: Associate Professor, Institute of CS and IE, National Chiao-Tung University. Jul. 1986–Aug. 1988 Assistant Professor, Department of Computer and Information Science, Fordham University. Jul. 1984–Dec. 1984 Doctorate Intern, Johnson Controls, Inc. Aug. 1980–Oct. 1981 System Programmer, System Support Div., Milwaukee County Gov.
Research interest. Data security and Privacy, Information and Coding Theory, Game Theory, Reliability and Performance.