An Efficient Partially Blind Signature with Provable Security

CAI Yong-quan，LI Yun-long

(College of Computer Science and Technology, Beijing University of Technology Chaoyang Beijing 100022)

Abstract Partially blind signatures allow signers to include some common information (the date of issue, the value of electronic coins) negotiated by signers and users. This paper presents an efficient partially blind signatures scheme with provable security in the random oracle model. Our scheme uses a public algorithm to evolve the public keys and private keys which will be used during the partially blind signatures protocol. In such a manner the scheme has the same security as the underlying blind Okamoto-Schnorr signature without bringing out additional workload.

Key words electronic cash; electronic voting; knowledge proof signature; partially blind signature

高效的可证安全的部分盲签名

蔡永泉，李云龙

(北京工业大学计算机学院 北京 朝阳区 100022)

【摘要】部分盲签名通过在最终的签名数据中包含签名者和用户协商一致的公用信息（签名发布日期，电子货币的金额）来扩展了盲签名的概念。该文在随机预言机模型下提出了一个高效的可证安全的部分盲签名方案，该方案利用一个公开可行的算法提前计算出将要在随后的部分盲签名协议中用到的公钥和私钥，因此该方案Okamoto-Schnorr盲签名方案具有相同的安全性，并且不会造成额外的系统开销。

关 键 词 电子现金; 电子选举; 知识证明签名; 部分盲签名
中图分类号 TP309 文献标识码 A

1 Introduction

The concept of digital signatures was invented by Ref. [1], and their security was formalized by Ref. [2]. Digital signature schemes are essential for electronic commerce as they allow one to authorize digital documents that are moved across networks. Typically, a digital signature comes with not just the document body but also attributes such as “date of issue” or “valid until”, which may be controlled by the signer rather than the receiver.

Blind signature was introduced by Ref. [3], which can provide an anonymity of signed message. Since it was introduced, blind signature schemes have been used in numerous applications, most prominently in anonymous voting and anonymous e-cash, and appeared many variants[4-5]. Informally, blind signature allows a user to obtain signatures from an authority on any document, in such a way that the authority learns nothing about the message that is being signed. The most important property of blind signature differing from the other signatures is blindness, which requires that after interacting with various users, the signer is not able to link a valid message-signature pair obtained by some user, with the protocol session.

One particular shortcoming of blind signature is that, since the singer’s view of the message to be signed is completely blocked, the signer has no control over the attributes except for those bound by the public key. For instance, in a simple electronic cash system, a

Received date: 2007 – 09 – 14
收稿日期：2007 – 09 – 14
Foundation item: Supported by scientific research common program of Beijing municipal commission of education (Grant No.KM200610005001)
基金项目：北京教委科技发展计划项目(KM200610005001)
Biography: CAI Yongquan was born in 1956, received his PH.D. degree in 1998. He is a professor. His research interests include information security and cryptography. LI Yunlong wasborn in 1976. He is currently a master student. His research interests include network protocol and cryptography.
作者简介：蔡永泉(1956–)，男，教授，主要从事信息安全和密码算法等方面的研究；李云龙(1976－)，男，硕士生，主要从事计算机网络协议和密码学方面的研究.

bank issues a blind signature as an electronic coin. Since the bank cannot inscribe the value on the blindly issued coins, it has to use different public keys for different coin values. Hence the shops and customers must always carry a list of those public keys in their electronic wallet, which is typically a smart card whose memory is very limited.

The notion of partially blind signatures was introduced in[6], a partially blind signature scheme allows the signer to explicitly include common information such as the value of the e-coins in the blind signature under some agreement with the receiver. For instance, the signer can attach the date of issue to his blind signatures as an attribute. If the signer issues a huge number of signatures in a day, including the date of issue will not violate anonymity. Accordingly, the attributes of the signatures can be decided independently from those of the public key. By fixing common information to a single string, one can easily transform partially blind signature schemes into fully blind ones. However, the reverse is not that easy. One can now see that partially blind signatures are a generalized notion of blind signatures. The notion attracts a lot of attentions and has been implemented under different assumptions[7-10].

In this paper, we propose an efficient partially blind signatures with provable security in the random oracle model. The scheme is a partially blind Okamoto-Schnorr signature. The merit is that, after an efficient publicly available generation of public keys, we achieve partially blindness from blind signatures without introducing additional workload or degrading the security of the underlying schemes.

2 Preliminaries

2.1 Notations

A negligible function is a function $\varepsilon(\lambda)$ such that for all polynomials $\mathrm{poly}(\lambda)$, $1/\varepsilon(\lambda) < 1/\mathrm{poly}(\lambda)$ holds for all sufficient large λ. PPT stands for probabilistic polynomial-time. $KS\{x: y = f(x)\}(m)$ represents a knowledge signature on message m that is transformed from the zero-knowledge proof of a secret value x satisfying $y = f(x)$ with the well-known Fiat-Shamir transformation. An efficient algorithm $A(*)$ is a probabilistic Turing machine running in expected polynomial time. An adversary A is a PPT interactive Turing machine. If $A(*)$ is an efficient algorithm and x is an input for A, then $A(x)$ denotes the probability space that assigns to a string σ the probability that A, on input x, outputs σ. An efficient algorithm is deterministic if for every input x, the probability mass of $A(x)$ is concentrated on a signed output string σ. For a probability space P, $x \leftarrow P$ denotes the algorithm that samples a random element according to P. For a finite set X, $x \leftarrow X$ denotes the algorithm that samples an element uniformly at random from X.

2.2 Definition of Secure Partially Blind Signature Scheme

In this section we recall the definition of a secure partially blind signature scheme [11-12]. Note that this definition includes that of a secure blind signature scheme[13] as a special case where the piece of information shared by the signer and user, info, is a null string, $\perp$ (i.e., info = $\perp$**).**

Partial Blindness. To define the blindness property, let us introduce the following game among adversarial signer S^* and two honest users U_0 and U_1.

(1) Adversary $S^*(1^n, \mathrm{info})$ outputs pk and (m_0, m_1).

(2) Set up the input tapes of U_0, U_1 as follows:

Randomly select $b \in \{0, 1\}$ and put m_b and $m_{\bar{b}}$ on the private input tapes of U_0 and U_1, respectively ($\bar{b}$ denotes $1 - b$ hereafter).

Put (info, pk) on the public input tapes of U_0 and U_1.

Randomly select the contents of the private random tapes.

(3) Adversary S^* engages in the signature issuing protocol with U_0 and U_1.

(4) If U_0 and U_1 output valid signatures $(\mathrm{info}, m_b, \sigma_b)$ and $(\mathrm{info}, m_{\bar{b}}, \sigma_{\bar{b}})$, respectively, then give those outputs to S^* in random order. If either U_0 and U_1 outputs a valid signature, $(\mathrm{info}, m_b, \sigma_b)$ or $(\mathrm{info}, m_{\bar{b}}, \sigma_{\bar{b}})$, then give this output to S^*. Give $\perp$ to S^* otherwise.

(5) S^* outputs $b' \in \{0, 1\}$.

The advantage of A is defined by $\mathrm{Adv}^{\mathrm{Bld}}_{\mathrm{PBS},A}(\lambda) = 2\Pr[b = b'] - 1$.

Definition 1 (Partial Blindness) A PBS scheme

satisfies partial blindness, if for any PPT adversary signer S^*, the function $\mathrm{Adv}^{\mathrm{Bld}}_{\mathrm{PBS},S}(\lambda)$ is negligible in λ. If S^*'s computational power is unlimited, the blindness is unconditional.

Unforgeability. To define unforgeability, let us introduce the following game among adversarial user U^* and an honest signer *S*.

1) (*pk*, *sk*) is generated by $G(1^n)$, *pk* is put on the public input tapes of U^* and *S*, and *sk* is put on the private input tape of *S*.

2) For each run of the signature issuing protocol with *S*, adversary U^* outputs info, which is put on the public input tape of *S*. Then, U^* engages in the signature issuing protocol with *S* in a concurrent and interleaving way.

3) For each info, let l_{info} be the number of executions of the signature issuing protocol where *S* outputs completed, given info on its input tape. (For info that has never appeared on the input tape of *S*, define $l_{\mathrm{info}}=0$.) Even when info $=\perp$, $l_{\perp}$ is also defined in the same manner.

4) U^* wins the game if U^* output l valid signatures $(\mathrm{info},m_1,s_1),(\mathrm{info},m_2,s_2),\cdots,(\mathrm{info},m_l,s_l)$ for some info such that: (1) $m_i\neq m_j$ for any pair (*i*,*j*) with $i\neq j$ ($i,j\in\{1,2,\cdots,l\}$); (2) $l>l_{\mathrm{info}}$.

We define $\mathrm{Adv}^{\mathrm{unforge}}_{\mathrm{PBS}}$ to be the probability that U^* wins the above game, taken over the coin tosses made by U^*, *G* and *S*.

Definition 2 (Unforgeability) An adversary $U^*(t,qs,\varepsilon)$-forges a partially blind signature scheme if U^* runs in time at most t, U^* executes at most qs times the signature issuing protocol, and $\mathrm{Adv}^{\mathrm{unforge}}_{\mathrm{PBS}}$ is at least ε. A partially blind signature scheme is (t,qs,ε)-unforgeable if no adversary $U^*(t,qs,\varepsilon)$-forges the scheme.

3 Proposed Partially Blind Signatures

In this section, we propose our partially blind signatures, which is a blind version of knowledge proof signature where the signer knows $(x_1+z)^{-1}$ and $x_2(x_1+z)^{-1}$ which represent the inverse of the sum of Okamoto-Schnorr secret key and the hashed value of common information *c* and the product of x_2 and $(x_1+z)^{-1}$ respectively. Hence, we refer to it as partially blind inverse-Okamoto-Schnorr signature. It can be generalized to suit other signatures derived from knowledge proofs of discrete logarithms.

In the following, we demonstrate the solution to transform blind signatures to partially blind signatures by linking different public keys with different common information. However, we must address the issue to generate and manage the exponentially many public/private key pairs corresponding to the different common information. The trick is to use a publicly available deterministic algorithm to evolve the public key and allow the signer to evolve its private key accordingly. To illustrate this technique, we implement this transformation with the known blind Okamoto-Schnorr signature [14].

Let *G* be a cyclic group with prime order *q*, and *g*, *h* are elements in *G* of order *q*. We assume that any polynomial-time algorithm solves $\log_g h$ in Z_q only with negligible probability when *h* is selected randomly from *G*. Let $H,F:\{0,1\}^*\rightarrow Z_q$ be public cryptographic hash functions. Let $x_1,x_2\in Z_q$ be secret keys and $Y=g^{x_1}h^{x_2}$ be the corresponding public key, the signer and the user first agree on common information *c* in a predetermined way. The signature issuing protocol on the user's blind message *m* is as follows.

(Key Evolution) The signer computes $z=F(c)$, $Y=yg^z$ as its new public key and set $X_1=(x_1+z)^{-1}\bmod q$, $X_2=x_2(x_1+z)^{-1}\bmod q$ accordingly as its new private keys.

(Initialization) The signer randomly selects $t,u\in Z_q$, and sends $a=Y^th^u$ to the user as a commitment.

(Blinding) The user computes $z=F(c)$, $Y=yg^z$. It picks random numbers $\beta,\gamma,\delta\in Z_q$, computes $\alpha=aY^{\beta}h^{\gamma}g^{\delta}$, $\varepsilon=H(\alpha\,\|\,m\,\|\,z)$, and returns a challenge $e=\varepsilon-\delta \bmod q$.

(Signing) The signer computes $R=t-eX_1\bmod q$, $S=u+eX_2\bmod q$, and send the pair (*R*,*S*) back.

(Unblinding) The user first computes $Y^Rh^Sg^e$ to see if it equals to *a*, otherwise the signature issuing protocol stops. The user then computes $\rho=R+\beta\bmod q$, $\sigma=S+\gamma\bmod q$ and outputs $(\varepsilon,\rho,\sigma)$ as the resulting signature on *m*, and the predetermined common information *c*.

(Verification) The signature is valid if and only if $\varepsilon=H(Y^{\rho}h^{\sigma}g^{\varepsilon}\,\|\,m\,\|\,z)$ and $z=F(c)$, $Y=yg^z$.

4 Security

This section proves the security of our scheme assuming the intractability of the discrete logarithm problem and ideal randomness of hash functions *H* and *F*.

Theorem 1 (Correctness) If the signer and user follow the protocol, the output of the user will be accepted by the verification algorithm.

Proof Note that :

$$Y^{\rho}h^{\sigma}g^{\varepsilon}=Y^{R+\beta}h^{S+\gamma}g^{e+\delta}=$$
$$Y^{t-e(x_1+z)^{-1}}h^{u+ex_2(x_1+z)^{-1}}g^{e}Y^{\beta}h^{\gamma}g^{\delta}=$$
$$Y^{t}(g^{x_1+z}h^{x_2})^{-e(x_1+z)^{-1}}h^{u}.h^{ex_2(x_1+z)^{-1}}g^{e}Y^{\beta}h^{\gamma}g^{\delta}=$$
$$Y^{t}h^{u}Y^{\beta}h^{\gamma}g^{\delta}=aY^{\beta}h^{\gamma}g^{\delta}=\alpha$$

It follows that $\varepsilon = H(Y^{\rho}h^{\sigma}g^{\varepsilon}\|m\|z)$, $z=F(c)$. The verification holds.

Theorem 2 (Partially blindness) The above partially blind signature is unconditionally blind.

Proof It is sufficient to prove that, for any view (a,e,R,S,c) of the adversary signer S^* and any signature pair (e,r,s,m,c), there exists a blind factor tuple that maps the view and the signature pair.

For *i*=0,1, let (a_i,e_i,R_i,S_i,c) be view of S^* and $(\varepsilon_j,\rho_j,\sigma_j,m_j,c)$ be two valid partially blind signatures from user *j*=0,1, respectively. Let $\beta=\rho_j-R_i$, $\gamma=\sigma_j-S_i$, $\delta=\varepsilon_j-e_i$, since $Y^{R_i}h^{S_i}g^{e_i}=a_i$ and the signatures are valid, it follows that:

$$\varepsilon_j=h(a_iY^{\beta}h^{\gamma}g^{\delta}\|m\|z)=$$
$$h(Y^{R_i}h^{S_i}g^{e_i}Y^{\beta}h^{\gamma}g^{\delta}\|m\|z)=$$
$$h(Y^{R_i}h^{S_i}g^{e_i}Y^{\rho_j-R_i}h^{\sigma_j-S_i}g^{\varepsilon_j-e_i}\|m\|z)=$$
$$h(Y^{\rho_j}h^{\sigma_j}g^{\varepsilon_j}\|m\|z)$$

Hence, given $j\in\{0,1\}$, (a_0,e_0,R_0,S_0,c) and (a_1,e_1,R_1,S_1,c) have the same relation with $(\varepsilon_j,\rho_j,\sigma_j,m_j,c)$ defined by the signing protocol. Therefore, given a signature $(\varepsilon_j,\rho_j,\sigma_j,m_j,c)$, an infinitely powerful adversary signer S^* can guess *j* correctly with probability exactly 1/2.

Theorem 3 (Unforgeability) In the random oracle model, under the DLP assumption, the above partially blind signature is (*l*,*l*+1)-unforgeable against the sequential attack.

After *l* interactions with the signer, the adversary user U^* can not forge a valid signature that the common information has never appeared in the interactions. Because both sides of the partially blind signature use common information *c* to finish the protocol, the signer use *c* to generate its private signing key X_1 and X_2 along with the public verification key *Y*, meanwhile, an honest user use *c* to calculate *Y* which is used in the user's part of the protocol. If an adversary user U^* replace *c* in the final signature with *c'*, then the signature received by an verifier will be $(\varepsilon,\rho,\sigma,m,c')$ .Thus, $F(c')$ and $yg^{F(c')}$ which represent *z* and *Y* respectively in the verification equitation will certainly not satisfy the equation $\varepsilon=H(Y^{\rho}h^{\sigma}g^{\varepsilon}\|m\|z)$ because of the property of hash function. Hence, an adversary user U^* can not replace the pre-determined common information *c* with c' which may bring him some advantange.

For an adversary U^* which outputs *l*+1 valid signature with the same common information *c* after *l* interactions with the signer, the adversary U^* can be directly used to break (*l*,*l*+1)-unforgeability of the underlying blind Okamoto-Schnorr signature which has been proven secure in the random oracle model. Therefore, U^* can not do such a thing and our scheme also have the (*l*,*l*+1)-unforgeability character.

5 Conclusion

In this paper, an efficient partially blind signature is proposed, which uses publicly deterministic algorithm and the pre-determined common information to calculate the public key and the corresponding private key before the signing and verification protocol run. In such a manner, our partially blind signature is more efficient than the one proposed by Abe and Okamoto.

As we have seen above, except for an efficient additional key evolution procedure with *c* as the common information, our scheme is the same as the blind Okamoto-Schnorr signature. Therefore, it enjoys the same secure property as the known blind Okamoto-Schnorr signature and has all the advantages of partially blind signature. The proposed partially blind signature scheme can be used in the area of *E*-cash or *E*-voting efficiently and securely.

Reference

[1] DIFFIE W, Hellma M E. New directions in cryptography[J]. IEEE Trans on Information Theory, 1976, IT-22(6): 644-654.

[2] GOLDWASSER S, MICALI S, RIVEST R. A digital signature scheme secure against adaptive chosen-message attacks[J]. SIAM Journal on Computing, 1988, 17(2): 281-308.
[3] CHAUM D. Blind signature for untraceable payment[C]// Crypto1982. Berlin: Springer-Verlag, 1983.
[4] ZHANG F, KIM K. ID-based blind signature scheme and ring signature from pairing[C]//ASIACRYPT 2002. Belin: Springer-Verlag, 2002.
[5] KIM J, KIM K, CHULSOO L. An efficient and provably secure threshold blind signature scheme[C]//ICICS 2001. Berlin: Springer-Verlag, 2001.
[6] ABE M， FUJISAKI E. How to date blind signatures[C]// Asiacrypt ’96. [S.l.]: Springer-Verlag, 1996.
[7] CHOW S S M, HUI L C K, YIU S M, et al. Two improved partially blind signature schemes from bilinear pairings[C]//In ACISP ’05. [S.l.]: Springer-Verlag, 2005.
[8] FAN C I, LEI C L. Low-computation partially blind signatures for electronic cash[J]. ICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1998, E81- A(5): 818-824.
[9] ZHANG F, SAFAVI N R, SUSILO W. Efficient verifiably encrypted signature and partially blind signature from bilinear pairings[C]//In Indocrypt ’03. [S.l.]: Springer-Verlag, 2003.
[10] MAITLAND G, BOYD C. A provably secure restrictive partially blind signature scheme in public key cryptography[C]//PKC 2002. [S.l.]: Springer-Verlag, 2002.
[11] ABE M, OKAMOTO T. Provably secure partially blind signatures[C]. Crypto ’00. [S.l.]: Springer-Verlag , 2000.
[12] CAMENISCH J, KOPROWSKI M, WARINSCHI B. Efficient blind signatures without random oracles[C]// Forth Conference on Security in Communication Networks-SCN ’04. [S.l.]: Springer-Verlag, 2004.
[13] JUELS A, LUBY M, OSTROVSKY R. Security of blind digital signatures[C]//Crypto ’97. [S.l.]: Springer-Verlag, 1997.
[14] POINTCHEVAL D. Strengthened security for blind signatures[C]//In Eurocrypt ’98. [S.l.]: Springer-Verlag, 1998.

编　辑　熊思亮

(上接第1166页)

利用(n，k)门限密钥共享体制，认证请求节点仍可以通过获取其他k个合法节点的私钥分量或证书分量，完成认证，被攻破的节点不会影响整个系统的安全性，系统具有较好的入侵容忍性；在较长的一段时间周期内，有可能大于k个的CA节点被攻破或俘获而造成系统的不安全，可以利用Proactive方案周期性更新系统的密钥，从而有效地防止在一定时间周期内大于k个CA节点被攻击或俘获；证书链中的节点可能发布虚假证书进行欺骗攻击，方案中采用了两种方法来抵御这种攻击，一种是证书链认证的中间节点尽可能选取被分布CA中心或者是门限CA节点认证的节点，提高单条证书链认证的安全性。另一种是采用多条证书链，通过计算多条证书链的合并信任值来降低中间节点欺骗攻击的风险。对于非CA节点和非证书链中间节点的一般节点，它的安全性不会影响到整个系统的安全。本方案在提高认证成功率的同时保证了系统的安全性。

6　结　论

在总结分析门限机制方案和证书链方案的优势和存在的问题基础上，本文提出了混合式密钥管理方案，方案集成了门限机制和证书链机制，认证时首先采用门限机制，在门限机制失败时利用证书链信任值方法来完成认证。仿真结果表明，在增加少量通信量的情况下，提高了自组网的认证成功率，同时利用分布式CA和证书链保证了系统的安全性，较好地平衡了自组网的安全性和认证服务的可用性，满足自组网应用的安全要求。

参　考　文　献

[1] 于宏毅. 无线移动自组织网[M]. 北京: 人民邮电出版社, 2005.
[2] ZHOU L, HASS Z J. Secure Ad hoc networks[J]. IEEE Networks, 1999, 13(6): 24-30.
[3] LUO H, KONG J. Ubiquitous and robust access control for mobile Ad hoc networks[J]. IEEE/ACM Transactions on Networking (ToN), 2004, 12(6): 1049-1063.
[4] ASOKAN N, GINZBOORG P. Key agreement in Ad hoc network[J]. Computer Communications, 2000, 23: 1627-1637.
[5] CAPKUN S, BUTTYAN L, HUBAUX J P. Self-organized public key management for mobile Ad hoc networks[J]. IEEE Transactions on Mobile Computing, 2003, 2(1): 52-64.
[6] HUBAUX J P, BUTTYAN L, CAPKUN S. The quest for security in mobile Ad hoc networks[C]//In Proceedings of the ACM Symposium on Mobile Ad hoc Networking and Computing (MobiHoc). Long Beach: ACM Press, 2001.
[7] BROCH J. MALTZ D A, JOHNSON D B, et al. A performance comparsion of multi-hop wireless Ad hoc network routing protocol[C]//In ACM MOBICOM. Dallas: ACM Press, 1998.
[8] CANETTI R, HALEVI S, HERZBERG. A. Maintaining authenticated communication in the presence of break-ins[J]. Journal of Cryptology, 2000, 13(1): 61-105.
[9] REITER M K, STUBBLEBINE S G. Authentication metric analysis and design[J]. ACM Transactions on Information and System Security, 1999, 2(2): 138-158.
[10] KEVIN F, KANNAN V. The ns manual[J/OL]. [2007-07-10]. http://www.isi.edu/nsnam/ns/ns-documentation. html.
[11] PADMAPARNA H, JOHN H. Network simulator tutorial [J/OL]. http://www.isi.edu/nsnam/ns/ns-tutorial, 2007-07-10.

编　辑　税　红