无证书盲签名方案

苏万力[1,2]，张跃宇[1]，张晓红[2]，王育民[1]

(1. 西安电子科技大学综合业务网理论及关键技术国家重点实验室 西安 710071; 2. 青岛农业大学信息科学与工程学院 山东 青岛 266109)

【摘要】将盲签名和无证书密码结合，充分利用二者的优势，提出了一种无证书盲签名方案，使得签名方案既无对证书的需求，又无密钥托管的弊端，同时又具有盲签名的特性。给出了由系统初始化、局部密钥提取、签名者秘密信息建立、签名者公钥计算、签名者密钥计算、签名和验证7个算法组成的算法模型，并对其安全性给予了证明。分析表明，该方案具有高的安全性。

关 键 词 算法; 盲签名; 无证书签名; 无证书盲签名; 密码学

中图分类号 TP309 **文献标识码** A doi:10.3969/j.issn.1001-0548.2009.04.014

Certificateless Blind Signature Scheme

SU Wan-li[1,2], ZHANG Yue-yu[1], ZHANG Xiao-hong[2], and WANG Yu-min[1]

(1. State Key Lab. of Integrated Service Networks, Xidian University Xi'an 710071;

2. College of Information Science and Engineering, Qingdao Agricultural University Qingdao Shandong 266109)

Abstract Combining blind signature with certificateless cryptology, a certificateless blind signature scheme is proposed. This scheme solves the escrow problem and retains the merits of blind signature with no deed of certificate. This scheme includes various functional algorithms such as system initialization, partial-key-extract, set-secret-value, set-public-key, set-private-key, and so on. Finally, an analysis of the scheme's security is presented. The results demonstrate its capability of achieving high level of security.

Key words algorithms; blind signature; certificateless blind signature; certificateless signature; cryptography

文献[1]首次提出盲签名这种特殊的数字签名，盲签名与一般数字签名的不同之处在于，签名者对其所签消息的内容是未知的，或者对其所签消息提供者的身份是盲的，使得盲签名可广泛应用于电子现金、匿名电子选举和网上招(投)标等许多领域。文献[2-3]提出了盲签名的安全模型，其后有不少盲签名方案被提出[4-11]，其中文献[4]首次提出基于身份的盲签名方案，文献[9]则提出了更有效的基于身份的盲签名方案。

文献[12]提出的无证书签名(CL-PKC)密码体制，既消除了传统密码体制对证书的的需求，又解决了基于身份密码体制的密钥托管问题。该密码体制的基本思想是：第3方无权访问用户私钥，密钥生成中心KGC只提供部分私钥(由用户的身份产生)给用户，然后用户结合自己的密钥产生最终的实际私钥。用户的公钥(由用户的私有信息结合系统的参数)对他方可用，以进行加密或签名验证使用。无证书密码体制的这种优势使其比基于身份的密码体制有更大的应用空间。不少学者提出了安全的无证书签名方案[13-17]和特殊的无证书签名方案[18-23]。

本文将盲签名和无证书密码结合，充分利用二者的优势，提出一种无证书盲签名方案，使得签名方案既消除了对证书的需求，又无密钥托管的弊端，还具有盲签名的特性。另外，本文给出了算法模型并证明了其安全性。分析表明，本文提出的方案具有更高的安全性。

1 有关的数学知识

1.1 双线性对

假设G_1为由P生成的阶数为素数q的循环加法群，G_2为具有相同阶q的循环乘法群。一个双线性对是一个映射$e:G_1\times G_2\to G_2$，满足下面的性质：(1) 双线性性：对于所有的$R,Q\in G_1$，$a,b\in Z_q^*$，都有$e(aR,bQ)=e(R,Q)^{ab}$。(2) 非退化性：存在$R,Q\in G_1$，

收稿日期：2008－10－06；修回日期：2009－03－17

基金项目：国家863计划(2007AA01Z435)；国家自然科学基金(60803151，60772136)

作者简介：苏万力(1963－)，男，博士生，副教授，主要从事密码学、信息安全等方面的研究.

满足 $e(R,Q)\neq 1$。(3) 可计算性：对于所有的 $R,Q\in G_1$，存在有效的算法计算 $e(R,Q)$。

1.2 有关的数学困难问题

(1) 计算性 Diffie-Hellman(CDH)问题：给定 $P, aP, bP\in G_1$，对于未知的 $a,b\in Z_q^*$，计算 $abP\in G_1$。

(2) 离散对数(DLP)问题：给定 $P, aP\in G_1$，计算 $a\in Z_q^*$。

(3) 修改的逆计算性 Diffie-Hellman(mICDH)问题：给定 $b, P, aP\in G_1$，计算 $(a+b)^{-1}P$，其中 $a,b\in Z_q^*$。

2 无证书盲签名的定义和安全性

2.1 无证书盲签名定义

无证书盲签名结合了无证书签名和盲签名的特征，它由系统初始化、局部密钥提取、签名者秘密信息建立、签名者公钥计算、签名者密钥计算、签名和验证7种个算法组成，具体定义如下：

1) 系统建立算法(setup)是由 KGC 运行的概率性多项式时间算法，输入安全参数 k 和输出系统参数 params 和主密钥 s，其中系统参数 params 公开，而主密钥 s 由 KGC 秘密保管。

2) 部分私钥生成算法(PKGen)是由 KGC 运行的确定性多项式时间算法，输入系统参数 params、主密钥 s 和签名者身份 ID，输出签名者部分私钥 D_{ID}。

3) 设置秘密值算法(SSVal)是由签名者运行的概率性多项式时间算法，输入系统参数 params 和签名者身份 ID，输出签名者秘密值 x_{ID}。

4) 签名者的密钥生成算法(UPGen)是由签名者运行的确定性多项式时间算法，输入签名者的秘密值 x_{ID}、公钥 $\mathrm{PK}_{\mathrm{ID}}$ 和部分私钥 D_{ID}，输出签名者的完全密钥 $\mathrm{SK}_{\mathrm{ID}}$。

5) 设置公钥算法(SPKey)是由签名者运行的确定性多项式时间算法，输入系统参数 params，签名者的身份 ID 和秘密值 x_{ID}，输出签名者的公钥 $\mathrm{PK}_{\mathrm{ID}}$。

6) 签名生成算法(sign)是签名者和用户之间的交互式协议，由下列过程组成：(1) 签名者向用户签发一个承诺值；(2) 用户对信息进行盲化处理；(3) 签名者对用户的盲化信息进行签名后发回给用户；(4) 用户去盲化，产生最后签名 σ。

7) 签名验证算法(verify)是确定性多项式时间算法，输入系统参数 params 和签名者的公钥 $\mathrm{PK}_{\mathrm{ID}}$、消息 m 及其签名 σ，检验 σ 是否为有效签名，如果 σ 有效，输出 1；否则输出 0。

上述算法需要满足以下正确性的要求：

$$\forall\ (\mathrm{params}, s)\leftarrow \mathrm{Setup}(k)\ ;$$

$$D_{\mathrm{ID}}\leftarrow \mathrm{PKGen}(\mathrm{params}, s, \mathrm{ID})\ ;$$

$$x_{\mathrm{ID}}\leftarrow \mathrm{SSVal}(\mathrm{params}, \mathrm{ID})\ ;$$

$$\mathrm{PK}_{\mathrm{ID}}\leftarrow \mathrm{SPKey}(\mathrm{params}, \mathrm{ID}, x_{\mathrm{ID}})\ ;$$

$$\Rightarrow\ \mathrm{Verify}(\mathrm{params}, \mathrm{PK}_{\mathrm{ID}}, m\ ;$$

$$\mathrm{Sign}(\mathrm{params}, D_{\mathrm{ID}}, \mathrm{SK}_{\mathrm{ID}}, m))=1。$$

2.2 无证书盲签名的安全性

无证书盲签名方案的安全性必须满足盲性和存在性不可伪造，即如果一个无证书签名方案满足盲性和存在性不可伪造这两个特性，方案就是安全的。

盲性：签名者并不知道他所签发文件的具体内容，签名者也不可能将签名过程与最终所得的签名对应起来。盲签名的这种性质称为盲性[2-3]。

存在性不可伪造：无证书签名方案定义了两种类型敌手攻击：(1) 类型1敌手A_1攻击不能访问主密钥，但能替换任何实体的公钥。(2) 类型2敌手A_2攻击能够访问主密钥，但不能替换公钥。

因此本文定义无证书盲签名安全性对两类敌手的存在性不可伪造[12]。

3 个无证书盲签名方案

3.1 方案构造

文献[24]提出了有效的无证书签名方案[24]，并证明了其在随机预言机模型下的安全性。本文基于有效的无证书签名方案和基于身份的盲签名方案提出无证书盲签名方案，具体算法描述如下。

1) 系统初始化。产生系统参数和主密钥，KGC 做如下操作：(1) 生成系统参数 (G_1, G_2, q, e)；(2) 随机选取群 G_1 的一个生成元 $P\in G_1$；(3) 随机选取 $s\in Z_q^*$，并计算 $P_{\mathrm{pub}}=sP$；(4) 选取3个密码哈希函数 $H_1:\{0,1\}^*\rightarrow G_1$、$H_2:\{0,1\}^*\rightarrow G_1$ 和 $H_3:\{0,1\}^*\rightarrow Z_q$，系统公开参数为 params= $\{e, G_1, G_2, q, P, P_{\mathrm{pub}}, H_1, H_2, H_3\}$，主密钥 s 由KGC保管。

2) 局部密钥提取。该算法KGC为签名者生成部分私钥，输入参数为params、主密钥 s 和签名者身份 ID_A，进行以下运算：(1) 计算 $Q_A=H_1(\mathrm{ID}_A)$；(2) 输出签名者的部分密钥 $D_A=sQ_A$，并将 D_A 通过安全认证信道发送给签名者，签名者可以通过验证等式 $e(D_A,P)=e(Q_A,P_{\mathrm{pub}})$，以检验其私钥的合法性。

3) 签名者秘密信息生成。签名者选取 $x_A\in Z_q^*$ 作为其部分私钥。

4) 签名者公钥计算。签名者产生自己的公钥

$\mathrm{PK}_A = x_A P$，令 $R_A = \mathrm{PK}_A$。

5) 签名者密钥生成。签名者产生自己完全的密钥，计算 $y_A = H_2(R_A)$ 和 $S_A = D_A/(x_A + y_A)$。返回完全私钥 $\mathrm{SK}_A = S_A$。

6) 签名交互协议。签名交互过程如下：

User　　Signer

随机选取 $r \in Z_q^*$

$\xleftarrow{U}$　计算 $U = rQ_A$

随机选取 $\alpha, \beta \in Z_q^*$

计算：$U' = \alpha U + \alpha\beta Q_A$

$h = \alpha^{-1} H_3(m, U') + \beta$

$\xrightarrow{h}$　计算 $V = (r+h)S_A$

$\xleftarrow{V}$

计算 $V' = \alpha V$

签名为 $\sigma = (U', V')$。

7) 验证：输入系统公开参数、信息 $m \in \{0,1\}^*$、R_A、签名者身份 ID_A 和签名 $\sigma = (U', V')$，计算 $Q_A = H_1(\mathrm{ID}_A)$、$y_A = H_2(R_A)$ 和 $H_3(m, U')$，验证 $e(V', R_A + y_A P) = e(U' + H_3(m, U')Q_A, P_{\mathrm{pub}})$ 是否成立，如果成立，则为合法签名；否则为不合法签名。

3.2 算法的正确性

签名的验证如下：

$$e(V', R_A + y_A P) = e(\alpha V, R_A + y_A P) =$$
$$e(\alpha(r+h)S_A, (R_A + y_A P)) =$$
$$e\left(\alpha(r+h) \times \frac{s}{(x_A + y_A)} Q_A, (x_A P + y_A P)\right) =$$
$$e(\alpha(r+h) \times Q_A, P_{\mathrm{pub}}) =$$
$$e((\alpha r + H_3(m, U') + \alpha\beta) \times Q_A, P_{\mathrm{pub}}) =$$
$$e(\alpha U + \alpha\beta Q_A + H_3(m, U')Q_A, P_{\mathrm{pub}}) =$$
$$e(U' + H_3(m, U')Q_A, P_{\mathrm{pub}})$$

4 安全性证明

4.1 盲性证明

本文提出的无证书盲签名方案满足盲性。

证明　对于任意给定的一个有效签名 (m, U', V') 以及在盲签名发布中产生的任意视图 (U, h, V)，总是存在一对唯一盲因子 α、β。

由于盲因子 $\alpha, \beta \in Z_q^*$ 是随机选取的，因此满足签名方案的盲性，也必使下列等式成立：

$$U' = \alpha U + \alpha\beta Q_A \quad (1)$$
$$h = \alpha^{-1} H_3(m, U') + \beta (\mathrm{mod}\, q) \quad (2)$$
$$V' = \alpha V \quad (3)$$

由式(3)可知，$\alpha \in Z_q^*$ 是唯一存在的，令 $\alpha = \log_V V$。由式(2)可得 $\beta = h - (\log_V V)^{-1} H_3(m, U')$，$\beta$ 也是唯一存在的。

下面将证明 α、β 满足式(1)。由于双线性对的非退化性，可得到 $U' = \alpha U + \alpha\beta Q_A \Leftrightarrow e(U', P_{\mathrm{pub}}) = e(\alpha U + \alpha\beta Q_A, P_{\mathrm{pub}})$，因此，只需证明 α、β 满足 $e(U', P_{\mathrm{pub}}) = e(\alpha U + \alpha\beta Q_A, P_{\mathrm{pub}})$。又由于 (m, U', V') 是合法的签名，则满足 $e(V', R_A + y_A P) = e(U' + H_3(m, U')Q_A, P_{\mathrm{pub}})$，于是有：

$$e(\alpha U + \alpha\beta Q_A, P_{\mathrm{pub}}) =$$
$$e((\log_V V)U + (\log_V V)(h - (\log_V V)^{-1}$$
$$H_3(m, U'))Q_A, P_{\mathrm{pub}}) =$$
$$e((\log_V V)U + (\log_V V)hQ_A, P_{\mathrm{pub}})$$
$$e(H_3(m, U')Q_A, P_{\mathrm{pub}})^{-1} =$$
$$e((\log_V V)\frac{(r+h)sQ_A}{x_A + y_A}, (x_A + y_A)P)$$
$$e(U', P_{\mathrm{pub}})e(V', R_A + y_A P)^{-1} =$$
$$e((\log_V V)(r+h)S_A, R_A + y_A P)$$
$$e(U', P_{\mathrm{pub}})e(V', R_A + y_A P)^{-1} =$$
$$e((\log_V V)V, R_A + y_A P)e(U', P_{\mathrm{pub}})\ e(V', R_A + y_A P)^{-1} =$$
$$e(U', P_{\mathrm{pub}})$$

因此，盲因子 α、β 总是存在，签名过程的视图和任何合法的签名无关联。

4.2 安全性证明

无证书盲签名方案对文献[12]中定义的两种类型敌手存在性不可伪造，证明方法与文献[24]的方法基本相同。对于类型1敌手 A_1，在CDH困难问题假设和随机预言机模型下，本文的无证书盲签名方案存在性不可伪造。对于类型2敌手 A_2，在mICDH困难问题假设和随机预言机模型下，本文的无证书盲签名方案存在性不可伪造。通过对签名过程的分析，可以证明敌手不会在签名过程中得到秘密信息。

敌手和签名者ID交互，设 (U,h,V) 是敌手在签名过程中所见到的信息，由于 $V = (r+h)S_A$，敌手 A 已知 (V,h)，敌手 A 要得到 S_A 必须知道 r，而 r 是签名者随机选取的，A 知道 $U = rQ_A$，但要从该等式中得到 r，就相当于解决DLP问题。因此，敌手 A 不会从签名的交互过程中得到任何秘密信息。

4.3 性能分析

本文提出的方案在无证书密码体制下避免了密钥托管，因此，本方案的安全性比基于身份的公钥密码体制下的盲签名的安全性高。在一个基于身份的签名方案中，PKC能伪造用户签名，从而造成

签名不能达到真正的不可伪造。在效率方面，签名过程没有使用双线性对运算，验证过程只有3个双线对运算，相应地减少了运算量。

5 结 论

本文将盲签名和无证书密码结合，提出了一种无证书盲签名方案，使得签名方案既消除了对证书的需求，又无密钥托管的弊端，还具有盲签名的特性，无证书盲签名方案有了更大的应用空间。本文还给出了算法模型，并证明该方案具有高的安全性。

参 考 文 献

[1] CHAUM D. Blind signatures for untraceable payments[C]// Crypto ’82. New York: Plenum Press, 1983: 199-203.

[2] JUELS A, LUBY M，OSTROVSKY R. Security of blind digital signatures[C]//Crypto ’97, LNCS 1294. Berlin: Springer- Verlag，1997: 150-164.

[3] POINTCHEVAL D, STERN J. Provably secure blind signature schemes[C]//Asiacrypt ’96, LNCS 1163. Berlin: Springer-Verlag，1996:252-265.

[4] ZHANG F, KIM K. ID-based blind signature and ring signature from pairings[C]//Asiacrpt 2002, LNCS 2501. Berlin: Springer-Verlag, 2002: 533-547.

[5] ABE M, FUJISAKI E. How to date blind signatures[C]//Asiacrypt ’96, LNCS 1163. Berlin: Springer-Verlag, 1996: 244-251.

[6] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.

[7] POINTCHEVAL D. Strengthened security for blind signatures[C]//Eurocrypt 1998, LNCS 1403. Berlin: Springer- Verlag, 1998: 391-405.

[8] CAMENISCH J, PIVETEAU J M, STADLER M. Blind signatures based on the discrete logarithm problem[C]// Eurocrypt 1994, LNCS 950. Berlin: Springer- Verlag, 1995: 428-432.

[9] ZHANG F, KIM K. Efficient ID-based blind signature and proxy signature from bilinear pairings[C]//ACISP 2003, LNCS 2727. Berlin: Springer-Verlag, 2003: 312-323.

[10] BOLDYREVA A. Threshold Signature, Multi- signature and blind signature schemes based on the Gap-Diffie-Hellman-Group signature scheme[C]//PKC ’03, LNCS 2567. Berlin: Springer-Verlag, 2003: 31-46.

[11] OKAMOTO T. Efficient blind and partially blind signatures without random oracles[C]//TCC 2006, LNCS 3876. Berlin: Springer-Verlag, 2006: 80-99.

[12] AL-RIYAMI S, PATERSON K. Certificateless public key cryptography[C]//Asiacrypt 2003, LNCS 2894. Berlin: Springer-Verlag, 2003: 452-473.

[13] HUANG X, SUSILO W, MU Y, et al. On the security of a certificateless signature scheme[C]//CANS 2005, LNCS 3810. Berlin: Springer-Verlag , 2005: 13-25.

[14] LI X, CHEN K, SUN L. Certificateless signature and proxy signature schemes from bilinear pairings[J]. Lithuanian Mathematical Journal. 2005, 45(2): 76-83.

[15] ZHANG Z, WONG D, XU J, et al. Certificateless public-key signature: security model and efficient construction[C]//ACNS 2006, LNCS 3989. Berlin: Springer-Verlag, 2006: 293-308.

[16] ZHANG Lei, ZHANG Fu-tai, ZHANG Fang-guo. New efficient certificateless signature scheme[C]//EUC Workshops 2007, LNCS 4809. Berlin: Springer-Verlag, 2007: 692-703.

[17] 明 洋, 王育民. 有效的无证书签名方案[J]. 电子科技大学学报，2008, 37(2): 175-177.
MING Yang, WANG Yu-min. Efficient certificateless signature scheme based on bilinear pairings[J]. Journal of University of Electronic Science and Technology of China, 2008, 37(2): 175-177.

[18] CHOW S, YAP W. Certificateless ring signatures[DB/OL]. [2008-02-18]. http://eprint.iacr.org/ 2007/ 236.

[19] ZHANG L, ZHANG F, WU W. A provably secure ring signature scheme in certificateless cryptography[C] //Provable Secuirty-ProvSec ’07, LNCS 4784. Berlin: Springer-Verlag, 2007: 103-121.

[20] MA C, AO F, HE D. Certificateless group inside signature[C]//International Symposiumon Autonom- ous Decentralized Systems-ISADS ’05. [S.l.]: IEEE Computer Society, 2005: 194-200.

[21] YAP W S, CHOW S M, HENG S H, et al. Security mediated certificateless signatures[C]//Applied Cryptography and Network Security-ACNS ’07, LNCS 4521. Berlin: Springer-Verlag, 2007: 459-477.

[22] HUANG X, SUSILO W, MU Y, et al. Certificateless designated verifier signature schemes[C]//20th International Conference on Advanced Information Networking and Applications-AINA ’06. [S.l.]: IEEE Computer Society, 2006: 15-19.

[23] BARBOSA1 M, FARSHIM P. Certificateless signcryption [DB/OL]. [2008-02-18]. http://eprint.iacr.org/ 2008/143.

[24] CHOI K Y, PARK J H, HWANG J Y, et al. Efficient certificateless signature schemes[C]//ACNS 2007, LNCS 4521. Berlin: Springer-Verlag, 2007: 443-458.

编 辑 熊思亮