文章编号: 1006-2475(2017) 04-0105-04

一种基于身份的盲签名方案及其安全性证明

毛昱昉,邓伦治

(贵州师范大学数学科学学院,贵州 贵阳 550001)

摘要: 盲签名是一种特殊的数字签名,它可以保护用户的个人隐私。目前,已有的盲签名方案中,使用了比较多的双线性映射,因此计算成本过高,而且部分方案并没有给出严格的安全性证明。针对这些情况,本文提出一种新的基于身份的盲签名方案,基于 n-CDH 问题,在随机预言模型下证明了该方案是安全的。该方案在签名阶段没有使用双线性映射,验证阶段只使用 1 次双线性映射,因此与其他盲方案比较,计算成本更低。

关键词: 基于身份密码; 盲签名; 盲性; 双线性对

中图分类号: TP309 文献标识码: A doi: 10.3969/j.issn.1006-2475.2017.04.021

An Identity-based Blind Signature Scheme and Its Security Proof

MAO Yu-fang, DENG Lun-zhi

(School of Mathematical Science, Guizhou Normal University, Guiyang 550001, China)

Abstract: Blind signature is a special digital signature which can protect the user's privacy. At present, most of the blind signature schemes use the bilinear pairings, so the cost of computing is relatively high, and a part of the schemes do not give the proof on security. To deal with these problems, a new blind signature scheme based on identity is proposed, it is proved to be security based on n-CDH problem in the random oracle model. The scheme does not use bilinear pairing in signing and uses only once bilinear pairing in verification, compared with other blind signature schemes, the cost of computing is lower.

Key words: identity-based cryptography; blind signature; blindness; bilinear pairing

0 引 言

1984 年,Shamir [1] 提出了基于身份的公钥密码体制,这是密码学应用的一次变革。基于身份的密码系统将用户的私人信息作为公钥而不再使用繁琐的公钥证书。这种新的密码体制避开了证书的管理问题,因此这种密码体制系统相对地提高了管理效率。2001 年,Boneh [2] 利用椭圆曲线上的双线性对设计出一种可行的基于身份加密方案。基于椭圆曲线的密码需要相对较小的空间,因此椭圆曲线广泛应用在数字签名中。

1982 年,Chaum [3] 提出盲签名概念。盲性是盲签名的特点,具有有效保护签署消息内容的优点。盲签名可以使用在需要保护用户隐私的场合(如电子现金、电子投票等) 。盲签名被提出后立即得到了广泛的发展和应用。当前的盲签名主要有 2 个研究方向: 一个是基于大素数分解、二次剩余等提出的一系列盲签名方案; 另一个是将盲签名和其他的数字签名糅合衍生的分支,例如代理盲签名、公平盲签名 [4] 、多重盲签名和群盲签名等。一个盲签名由盲化、签名、解盲、验证 4 个部分组成。基于身份的盲签名取消了公钥证书的使用,达到了提高效率的目的。

Zhang [5] 等人基于 Diffie-Hellman [6] 问题提出了无证书盲签名方案,该方案在运算效率上有所欠缺; 向新银 [7] 等提出的基于双线性对的盲签名方案频繁使用双线性对且没有证明方案的安全性; 虽然褚万霞 [8] 等人提出了高效的基于身份的盲签名方案,减少了双线性对的使用次数,但是方案中没有具体的方案安全性证明,所以该方案的安全性无法确定; 黄如芬 [9] 等人提出了无证书盲签名方案,文献中仔细地证明了方案的安全性,但是在效率方面有些不尽如人意; 何俊杰 [10] 等人提出了无可信私钥生成中心的盲

收稿日期: 2016-07-31

基金项目: 国家自然科学基金资助项目(61562012) ; 贵州省教育厅创新群体重大研究项目(黔教合 KY 字 [2016] 026)

作者简介: 毛昱昉(1990-) ,男,河南正阳人,贵州师范大学数学科学学院硕士研究生,研究方向: 密码学; 邓伦治(1979-) ,男,贵州桐梓人,教授,博士,研究方向: 密码学与信息安全。

签名，但是该方案在运算效率方面过低；Gao[11] 等人设计了一种假设不含 ROS 的基于身份的盲签名方案，经测算该方案的运算效率过低；邓伦治[12] 等人基于 n-CDH 问题设计了一种基于身份的高效代理方案并且完整地证明了方案自身的安全性；赵菲菲[13] 等提出了基于椭圆曲线的盲签名，虽然该方案同时存在 2 种签名方案，但是没有安全证明也没有盲性分析，无法确定方案的安全性；龚国昌[14] 等人基于 ECDLP 问题提出具有强盲性的高效无证书盲签名方案，并且证明了方案安全性；基于 DLP 问题，何俊杰[15] 等人提出无证书盲签名方案，并完整地证明了方案的安全性。

本文构造了一种新的方案，与同类方案对比，本方案在效率上有着一定的优势，并论述了本文方案的安全性。

1 背景知识

1.1 双线性映射

设 G_1、G_2 是 2 个阶为素数 p 的循环群，G_1 为加法循环群，G_2 为乘法循环群，P 是群 G_1 的一个生成元。e: $G_1 \times G_1 \to G_2$ 是一个满足下列要求的映射：

1) 任取 $P_1, P_2 \in G_1$，$a, b \in Z_q$，则 $e(aP_1, bP_2) = e(P_1, P_2)^{ab}$；

2) 存在 $P_1, P_2 \in G_1$，使得 $e(P_1, P_2) \neq 1_{G_2}$，1_{G_2} 为 G_2 的单位元；

3) 存在一个高效的计算方法对于任意的 $P_1, P_2 \in G_1$，可以计算 $e(P_1, P_2)$。

1.2 对 n-CDH 问题的定义

定义 1 P 是群 G_1 的一个生成元，给定 e: $G_1 \times G_1 \to G_2$ 是一个双线性映射，若存在 $\left(P, aP, b, d_1, d_2, \cdots, d_n, \frac{1}{a+d_1}P, \frac{1}{a+d_2}P, \cdots, \frac{1}{a+d_n}P\right)$，试问能否计算 $\frac{1}{a+b}P$。

2 方案的提出

1) 参数设置。给出安全参数 n，私钥生成中心 (PKG) 选择 2 个阶为素数 q($q > 2^n$) 的群 G_1 和 G_2，其中，P 是 G_1 的一个生成元，双线性映射 e: $G_1 \times G_1 \to G_2$，$s \in Z_q^*$，计算 $P_{Pub} = sP$，选择 2 个 hash 函数 H_0: $\{0,1\}^* \to Z_q^*$，H_1: $\{0,1\}^* \times G_2 \to Z_q^*$。PKG 公布参数 pamars = $\{G_1, G_2, P, q, e, g, H_0, H_1, P_{Pub}\}$；其中 $g = e(P, P)$。

2) 私钥生成。首先，PKG 输入用户的身份 $ID_i \in \{0,1\}^*$，然后计算公钥 $d_{ID_i} = H_0(ID_i)$ 和 $S_{ID_i} = \frac{1}{s + d_{ID_i}}P$，最后使用安全信道把 S_{ID_i} 发给用户。

3) 签名发布。设 m 是待签名的消息，用户 B 和签名者 A 进行如下交互：

签名 1：用户 B 选取 $\alpha \in Z_q^*$，$V = g^\alpha$ 并通过安全信道将 V 发给签名者 A，签名者 A 任取 $k \in Z_q^*$，然后计算 $r_A = V^k$，并将 r_A，d_{ID_A} 发给用户 B。

盲化：用户 B 选取 $\beta \in Z_q^*$，计算 $r = r_A^\beta$，$h = H_1(m, r)$，$\bar{h} = \beta^{-1}\alpha^{-1}h$，并将 $\bar{h}$ 发给签名者 A。

签名 2：签名者 A 计算 $\bar{U} = (\bar{h} + k) S_{ID_A}$，将 $\bar{U}$ 发给用户 B。

解盲：用户 B 计算 $U = \alpha\beta\bar{U}$，用户得到的盲签名为 $\sigma = (U, r)$。

验证：验证者收到消息 m 的盲签名 $\sigma = (U, r)$ 后，根据公开参数计算 $h = H_1(m, r)$，并验证等式 $e(U, P_{Pub} + d_{ID_A}P) = r \cdot g^h$ 是否成立。如果等式成立，则判定盲签名有效；若不成立，则判定盲签名无效。

3 安全性分析

3.1 不可伪造性

定理 1 在随机预言模型下，设 A 是一个自适应的选择密文攻击者，在时间 t 内，至多做 q_{H_0} 次 H_0 查询，q_{H_1} 次 H_1 查询，q_E 次私钥查询，q_S 次签名查询。如果 A 能以 ε 的优势给出有效的伪造，则存在挑战者 C，能以 $\frac{\varepsilon}{q_{H_0}}$ 的优势解决 n-CDH 问题。

证明：假设 C 遇到一个 n-CDH 问题，$\left(P, aP, b, d_1, d_2, d_3, \cdots, d_n, \frac{1}{a+d_1}P, \frac{1}{a+d_2}P, \cdots, \frac{1}{a+d_n}P\right)$，而且 C 可以将 A 作为一个子程序调用，C 在游戏中扮演 A 的挑战者。同时 C 生成 pamars = $\{G_1, G_2, e, P, P_{Pub} = aP, g, H_0, H_1\}$，$g = e(P, P)$，并将其发送敌手，a 对于挑战者是保密的。

A 将对 C 做多项式次数查询，并且假定 A 每次查询的内容互不相同，同时 A 将在身份 ID 用作其他的查询前先对 ID 做 H_0 查询。

H_0 查询：C 以 (ID_i, d_i) 的形式设置列表 L_0，初始化 L_0，当 A 查询 $H_0(ID_i)$ 时，C 按下列步骤应答 A 的查询：

在 A 的第 j 次查询时 C 用 $H_0(ID^*) = b$ 回答，当 $i \neq j$ 时，设定 $H_0(ID_i) = d_i$ 并且将 (ID_i, d_i) 储存在 L_0 中，此时 $n > q_{H_0}$。

H_1 查询：以 (m_i, r_i, h_i) 的格式设置列表 L_1，当查询 $H_1(m_i, r_i)$ 时，$\forall h \in Z_q^*$，并设 $h = H_1(m_i, r_i)$，储存 (m_i, r_i, h_i) 到表 L_1 中。

私钥查询: 当 A 对身份 ID_i 做私钥查询时,C 在 L_0 找到相应的记录(ID_i,d_i),如果 $ID_i = ID^*$ 则失败,游戏结束; 若 $ID_i \neq ID^*$,计算 $S_{ID_i} = \frac{1}{a + d_{ID_i}}P$,并将其发送给 A。

签名查询: A 发送(m,ID_i)至 C。

1) 若 $ID_i \neq ID^*$,则根据签名算法进行。

2) 若 $ID_i = ID^*$,则按以下步骤进行:

①$\forall h \in Z_q^*$,$U \in G$;

②计算 $r = e(U,P_{Pub} + bP)g^{-h}$;

③令 $h = H_1(m,r)$,储存(m,r,h)到列表 L,若产生碰撞,则重做①至③。

伪造: A 给出伪造签名 $\eta^* = (m^*,U^*,r^*)$ 且没有查询签名者的私钥。

解决 n-CDH 问题:

1) 若 $ID_i \neq ID^*$,则游戏结束;

2) 若 $ID_i = ID^*$ 时,由 Forking 引理[16],C 可以获得 $\eta^* = (m^*,U^*,r^*)$ 和 $\eta^{*\prime} = (m^*,U^{*\prime},r^*)$ 2 个有效的盲签名,$h^* = H_1(m^*,r^*)$ 并且 $h^* \neq h^{*\prime}$,$U^* = \frac{h^* + r^*}{a+b}P$,$U^{*\prime} = \frac{h^{*\prime} + r^*}{a+b}P$,$U^* \neq U^{*\prime}$,$\frac{1}{h^* - h^{*\prime}}(U^* - U^{*\prime}) = \frac{1}{a+b}P$,若伪造成功,则证明安全。$b \notin \{d_{i_1},d_{i_2},\cdots,d_{i_{q_E}}\}$ 的概率是 $1 - \frac{q_E}{q_{H_0}}$,所以私钥查询不失败的概率是 $1 - \frac{q_E}{q_{H_0}}$; 签名查询不失败的概率 $\Pr[ID_i = ID^*] = \frac{1}{q_{H_0} - q_E}$; 所以 C 成功解决 n-CDH 问题的成功率是: $\varepsilon(1 - \frac{q_E}{q_{H_0}})\frac{1}{q_{H_0} - q_E} = \frac{\varepsilon}{q_{H_0}}$。

所以在 n-CDH 问题下本文提出的方案可以抵抗自适应的选择密文伪造攻击。

3.2　方案盲性

定理 2　本文提出的基于身份的盲签名方案满足盲性。

证明: 对于一个公开后的合法盲签名方案 $\sigma = (ID_A,m,U,r)$ 和任意的一组签名者私自保存签名过程中的交互中间变量 $\sigma' = (V,\bar{h},\bar{U})$,可知:

$$V = g^{\alpha} \tag{1}$$

$$U = \alpha\beta\bar{U} \tag{2}$$

$$r = g^{\alpha\beta k} \tag{3}$$

可得到 $\alpha = \log_g V$,$\alpha \in Z_q^*$,可知 α 是唯一确定的,$\beta = \alpha^{-1}\log_{\bar{U}}U$,其中 $\alpha,\beta \in Z_q^*$,可知 α,β 的唯一性。以下证明由式(1)和式(2)所确定的 α,β 也满足式(3)。由于 $\sigma = (ID_A,m,U,r)$ 是合法的盲签名方案,因此满足等式 $e(U,P_{Pub} + d_{ID_A}P) = g^h \cdot r$,其中,$\bar{U} = (\bar{h} + k)S_{ID_A}$,$k = \log_{S_{ID_A}}\bar{U} - \bar{h}$,则以下等式成立:

$$\begin{aligned} g^{\alpha\beta k} &= g^{\log_{\bar{U}}U(\log_{S_{ID_A}}\bar{U} - \bar{h})} \\ &= g^{\log_{\bar{U}}U\log_{S_{ID_A}}\bar{U} - h} \\ &= g^{\log_{S_{ID_A}}U - h} \\ &= e((\log_{S_{ID_A}}U)P,P) \cdot g^{-h} \\ &= e((\log_P U)P,(\log_P S_{ID_A})^{-1}P) \cdot g^{-h} \\ &= e(U,P_{Pub} + d_{ID_A}P) \cdot g^{-h} = r \end{aligned}$$

可知,由式(1)和式(2)所确定的 α,β 满足式(3),所以任意的一个盲签名 σ 与它的签名过程中产生的中间变量 σ' 之间可以确定唯一的一组盲化因子 $\alpha,\beta \in Z_q^*$ 使得 σ 映射到 σ' 而不产生矛盾。因此,本文所提的基于身份盲签名方案满足盲性要求。

4　效率分析

本方案与其他盲签名方案进行计算效率对比,运算效率如表 1 所示。表 1 中涉及的比较数据来自 Islam[17] 等通过实际测算得到的结果,各种方案的实际效率比较见表 2。

表 1　运算效率

运算	缩写	运算效率
Z_p^* 中模乘运算	m	–
群 G_1 中的标量乘运算	M	1M≈29m
双线性对运算	P	1P≈87m
群 G_2 中的幂乘运算	E	1E≈29m
Z_p^* 中求逆运算	I	1I≈11.6m
maptopoint 散列运算	H	1H≈29m
普通散列运算	h	可以忽略

表 2　效率比较

方案	签名发布	验证	运算总和
文献[5]	4M + 3E + 1H	3P + 1E + 2H + 1I	562.6m
文献[7]	9M + 4P	4P	957m
文献[9]	3E + 4M	1P + 1E + 1M	348m
文献[10]	8M	3P	493m
文献[11]	7E + 4P	4P	899m
本文方案	2M + 3E + 2I	1P + 1M + 1E	313.2m

5　结束语

本文利用双线性对的同时最大程度优化盲签名的结构,使得盲签名的过程更加简单。文中证明了该方案的不可伪造性和盲性,最终的结果显示是安全的。在本方案中,只需要 1 次双线性对的计算,3 次标量乘运算,4 次幂乘运算,2 次求逆运算,与以往的方案比较,在效率方面有明显的提高。

参考文献:

[1] Shamir A. Identity-based cryptosystems and signature schemes [C] // Proceedings of CRYPTO'84 on Advances in Cryptology. 1984:47-53.

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairing [C] // Proceedings of CRYPTO 01 on Advances in Cryptology. 2001:213-229.

[3] Chaum D. Blind signature for untraceable payments [C] // Proceedings of CRYPTO'82 on Advances in Cryptology. 1982:199-203.

[4] Verma G K. New ID-based fair blind signature [J]. IACR Eprint Archive, 2008.

[5] Zhang Lei, Zhang Futai. Certificateless signature and blind signature [J]. Journal of Electronics (China), 2008, 25(5):629-635.

[6] Diffie W, Hellman M E. New directions in cryptography [J]. IEEE Transactions on Information Theory, 1976, 22(6):644-654.

[7] 向新银,郝会兵,党荣香. 基于双线性对的盲签名方案 [J]. 计算机工程与应用, 2008, 44(11):122-123.

[8] 褚万霞,张建中. 高效的基于身份的盲签名方案 [J]. 计算机工程与应用, 2010, 46(36):112-113.

[9] 黄茹芬,农强,黄振杰. 一个高效的无证书盲签名方案 [J]. 计算机工程, 2013, 39(2):130-136.

[10] 何俊杰,张帆,祁传达. 新的无可信私钥生成中心的盲签名方案 [J]. 计算机应用, 2013, 33(4):1061-1064.

[11] Gao Wei, Wang Guilin, Wang Xueli, et al. One-round ID-based Blind Signature Cheme Without ROS Assumption [EB/OL]. http://iacr.org/cryptodb/data/paper.php?pubkey=13289, 2007-01-05.

[12] 邓伦治,吴云顺. 高效的基于身份代理签名 [J]. 计算机工程与应用, 2013, 49(14):99-100.

[13] 赵菲菲,魏仕民. 基于椭圆曲线的盲签名 [J]. 淮北师范大学学报(自然科学版), 2013, 34(4):10-13.

[14] 龚国昌,石志寒. 具有强盲性的高效无证书盲签名方案 [J]. 计算机应用, 2014, 34(7):1890-1892.

[15] 何俊杰,张雪峰,祁传达. 一种不含双线性对的无证书盲签名方案 [J]. 计算机工程, 2015, 41(7):174-176.

[16] Pointcheval D, Stern J. Security proofs for signature schemes [C] // Proceedings of CRYPTO'96 on Advances in Cryptology. 1996:387-398.

[17] Islam S H, Biswas G P. A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks [J]. Annals of Telecommunications, 2012, 67(11):547-558.

(上接第 93 页)

参考文献:

[1] 王永固,张庆. MOOC:特征与学习机制 [J]. 教育研究, 2014(9):112-120.

[2] 蒋卓轩,张岩,李晓明. 基于 MOOC 数据的学习行为分析与预测 [J]. 计算机研究与发展, 2015, 52(3):614-628.

[3] 李丽. 基于 MOOC 模式的开放教育研究 [J]. 重庆广播电视大学学报, 2014(4):3-6.

[4] 谢树爽. 基于大数据的 MOOCs 发展研究 [J]. 软件导刊, 2015, 14(6):13-16.

[5] Kay J, Reimann P, Diebold E, et al. MOOCs: So many learners, so much potential [J]. IEEE Intelligent Systems, 2013, 28(3):70-77.

[6] Fisher A, Anderson G B, Peng R, et al. A randomized trial in a massive online open course shows people don't know what a statistically significant relationship looks like, but they can learn [J]. PeerJ, 2014, 2(1):e589.

[7] Williams B. Roll call: Taking a census of MOOC students [C] // Proceedings of the Workshops at the 16th International Conference on Artificial Intelligence in Education. 2013.

[8] Klapp A. MOOCs Open Doors for Diverse Student Body [EB/OL]. http://www.diversityjournal.com/10107-moocs-open-doors-for-diverse-student-body/, 2013-08-01.

[9] Ho A D, Reich J, Nesterko S, et al. HarvardX and MITx: The First Year of Open Online Courses (HarvardX Working Paper No. 1) [EB/OL]. http://harvardx.harvard.edu/multiple-course-report, 2014-02-02.

[10] 王萍. 基于 edX 开放数据的学习者学习分析 [J]. 现代教育技术, 2015, 25(4):86-93.

[11] 赵翔,胡艳丽,唐九阳. MOOC 教育大数据辨析初探:方法与启示 [J]. 科教文汇(上旬刊), 2015(1):1-3.

[12] 姜强,赵蔚,王朋娇,等. 基于大数据的个性化自适应在线学习分析模型及实现 [J]. 中国电化教育, 2015(1):85-92.

[13] 杨李娜. 通信行业大数据平台项目应用与实践研究 [J]. 数字通信世界, 2015(9):43-46.

[14] 原亚纳. 浅析大数据在教育领域的应用 [J]. 长春教育学院学报, 2014(22):60.

[15] 徐鹏,王以宁,刘艳华,等. 大数据视角分析学习变革 [J]. 远程教育杂志, 2013(6):11-17.

[16] 杨进中,张剑平. 基于社交网络的个性化学习环境构建研究 [J]. 开放教育研究, 2015, 21(2):89-97.

[17] 吴进宝. K-means 算法研究综述 [J]. 电子技术与软件工程, 2014(18):207.