文章编号: 1001- 9081(2008) 08- 1940- 03

一种基于身份的代理盲签名方案的分析与改进

农 强[1,2], 吴顺祥[2]
(1.漳州师范学院 计算机科学与工程系, 福建 漳州 363000; 2.厦门大学 自动化系, 厦门 361005)
(nong_qiang@ 163. com)

摘 要: 通过对 Li-Zhang基于双线性映射的基于身份的代理盲签名方案的分析, 指出该方案并不满足不可伪造性, 原始签名人可以伪造一个有效的代理盲签名, 代理签名人可以滥用代理签名权, 同时当签名被用户泄露后, 代理签名人能将自己在签名协议中的签名和签名的消息联系起来, 这就是所谓的可追踪性。在此基础上提出了改进的代理盲签名方案, 改进后的方案有效克服了原方案的安全缺陷, 并满足代理盲签名所需要的各种安全性要求, 其计算量虽有少量增加, 但仍低于其他同类方案。

关键词: 基于身份; 代理盲签名; 不可伪造性; 双线性映射
中图分类号: TP309 文献标志码: A

Cryptanalysis and improvement of ID-based proxy blind signature scheme

NONG Qiang[1,2], WU Shun-xiang[2]
(1. *Department of Computer Science and Engineering, Zhangzhou Normal University, Zhangzhou Fujian 363000, China*;
2. *Department of Automation, Xiamen University, Xiamen Fujian 361005, China*)

Abstract The security of the Li-Zhang's ID-based proxy blind signature scheme from bilinear pairings was analyzed, and it was found that this scheme did not possess the unforgeability property. The original signer can forge a valid proxy blind signature for any message, and the proxy signer can misuse the signing capabilities. At the same time, the proxy signer can make a linkage between a signature and the corresponding message of signing protocol after signing, which is called linkability. An improved proxy blind signature scheme was proposed, which can resolve the security problems existing in the original scheme and satisfy other required properties of a proxy blind signature scheme. The calculative complexity is lower than that of the other schemes despite a little increase.

Key words ID-based; proxy blind signature; unforgeability; bilinear pairings

0 引言

1996年, 由 Mambo[1]等人首先提出代理签名的概念, 目前人们已经提出了许多种代理签名方案, 代理盲签名方案是其中重要的一种, 它结合代理签名和盲签名的优点, 在实际中具有非常重要的应用价值。在 2000年, Lin 和 Jan第一个提出了代理盲签名方案[2]。之后, 多个代理盲签名方案被相继提出[3-5]。然而, 在这些已有的代理盲签名方案大多基于离散对数问题。1984年, Shamir提出了一个基于身份的加密和签名方案[6], 去除了由 CA 颁发公钥证书所带来的存储和管理开销等问题。后来, 人们发现利用双线性映射可以高效实现密码学上基于身份的加密、签名等应用。最近, 利用双线性对构造的一些基于身份的代理盲签名方案[7-9]被提出, 具有一些较好的性质。从理论上来讲, 如何设计出安全高效的代理盲签名方案, 并不断拓展其新的应用领域目前仍然是一个研究热点。

本文着重对文献[9] (以下称 Li-Zhang方案)中提出的代理盲签名方案进行了安全性分析, 指出该方案并不满足不可伪造性, 原始签名人可以伪造一个有效的代理盲签名, 同时该方案也不能预防代理签名人权力的滥用以及代理签名人在事后可以追踪签名。在此基础上提出了改进的代理盲签名方案, 改进的方案有效克服了原方案的安全缺陷, 与已有的一些典型的基于身份的代理盲方案相比, 本文方案的效率更高。

1 数学知识

设 $(G_1, +)$ 和 $(G_2, \times)$ 为 q 阶循环群, q 为一大素数。P 为 G_1 的生成元, 设在群 G_1, G_2 中离散对数问题是困难的。可定义双线性映射为 $e: G_1 \times G_1 \rightarrow G_2$, 其满足双线性、非退化性和可计算性三种特性。对于这样定义的 G_1, 我们可以定义离散对数问题(DLP)、可计算 Diffie-Hellman 问题(CDHP)、可判定 Diffie-Hellman问题(DDHP)、Gap Diffie-Hellman (GDH)问题等难解问题, 并称具有 CDH 问题难解而 DDH 问题易解特征的群为 GDH 群。有关详细内容可参看文献[10]。

2 Li-Zhang代理盲方案[9]及分析

2.1 初始阶段

群 $(G_1, +)$ 和 $(G_2, \times)$ 的阶数为素数 q, P 为 G_1 的生成元, $e: G_1 \times G_1 \rightarrow G_2$ 为一个安全的双线性对, 同时定义两个 Hash函数 $H_1: \{0,1\}^* \rightarrow G_1$, $H_2: \{0,1\}^* \times G_2 \rightarrow Z_q^*$。可信中心选择 $s \in_R Z_q^*$, 计算 $Q_{TA} = sP$, 将 s秘密保存, 公开其系统参数: $Params = \{G_1, G_2, e, q, P, Q_{TA}, H_1, H_2\}$。当用户需要与他的身份相对应的私钥时, 向可信中心提出申请, 可信中心在验证了用户的身份后计算出用户的私钥。

2.2 代理授权阶段

设原始签名人 A 的身份是 ID_A, 代理签名人 B 的身份是

收稿日期: 2008- 03- 10; 修回日期: 2008- 04- 25。 基金项目: 国家"十一五"科技支撑计划项目(2007BAK34B04); 国家自然科学基金资助项目(60704042); 厦门大学 985二期信息创新平台项目(2004- 2007)。

作者简介: 农强(1978-), 男, 广西南宁人, 讲师, 硕士研究生, 主要研究方向: 密码学、网络安全; 吴顺祥(1967-), 男, 湖南邵阳人, 教授, 博士, 主要研究方向: 信息安全、数据挖掘、智能信息系统、人工智能与机器学习。

ID_B, 则 A 的公钥为 $Q_A = H_1(ID_A)$, B 的公钥为 $Q_B = H_1(ID_B)$; A 的私钥为 $S_A = sQ_A$, B 的私钥为 $S_B = sQ_B$。A 选取 $P_1 \in_R G_1$, 计算 $r_A = e(P_1, P)$, $v_A = H_2(ID_B, r_A)$, $U_A = v_A S_A + P_1$, 并将 U_A, r_A 发送给 B。B 代理方验证等式 $e(U_A, P) = e(Q_A, Q_{TA})^{v_A} r_A$ 是否成立, 如果成立, 则授权合法, 计算代理签名私钥: $S_P = U_A + S_B$。

2.3　代理盲签名过程

代理人 B 选择 $P_2 \in_R G_1$, 计算 $r_B = e(P_2, P)$, 将 r_A, r_B 发送给消息持有人 R。R 选择 $P_3 \in_R G_1$, $k \in_R Z_q^*$, 计算 $r = r_B^k e(P_3, P)$, $v = H_2(M, r)$, $v' = v/k$, 然后将盲化的消息 v' 发送给 B, B 计算 $U_B = v' S_P + P_2$, 并将 U' 发送给 R。R 进行去盲, 计算 $U = kU_B + P_3$, 则代理盲签名为 (U, r, v)。R 验证: $e(U, P) = e(Q_A, Q_{TA})^{v r_A} r_A^v e(Q_B, Q_{TA})^{v r}$, 如果验证等式成立, 则签名是 B 代表 A 的盲签名, R 接受; 否则, 为非法代理盲签名, 丢弃。

2.4　原始签名人的伪造攻击分析

原始签名人 A 可以伪造代理签名人 B 代表他对信息 M 的代理盲签名。首先 A 选择 $P' \in_R G_1$, 计算 $r_A = e(P', P) e(Q_B, Q_{TA})^{-1}$, $v_A = H_2(ID_B, r_A)$, $S_P' = v_A S_A + P'$, 则 S_P' 就是 A 伪造的一个有效的代理密钥。于是, 不诚实的原始签名人 A 冒充 B 与 R 按照 2.3节的算法交互后将产生一个有效的代理盲签名 (U, r, v), 并通过 R 的验证, 这是因为:

$$
\begin{aligned}
&e(U, P) = \\
&\quad e(kU_B + P_3, P) = e(k(v' S_P + P_2) + P_3, P) = \\
&\quad e(kv' S_P, P) e(kP_2, P) e(P_3, P) = \\
&\quad e(vS_P, P) e(P_2, P)^k e(P_3, P) = \\
&\quad e(S_P, P)^v r_B^k e(P_3, P) = e(v_A S_A + P', P)^v r = \\
&\quad e(S_A, P)^{v v_A} e(P', P)^v r = \\
&\quad e(Q_A, Q_{TA})^{v v_A} e(P', P)^v r = \\
&\quad e(Q_A, Q_{TA})^{v v_A} [r_A e(Q_B, Q_{TA})]^v r = \\
&\quad e(Q_A, Q_{TA})^{v v_A} r_A^v e(Q_B, Q_{TA})^v r
\end{aligned}
$$

2.5　代理签名权的滥用分析

在 Li-Zhang方案中, 原始签名人对代理签名人的代理签名权没作任何限制, 比如代理有效期限, 代理签名文件的范围等, 一旦原始签名人将代理签名权委托给代理签名人, 势必导致代理签名人可以在任何时候对任何文件进行代理签名, 这样对原始签名人是很不利的。一般情况下, 原始签名人只希望代理签名人在某一段时间内对某些文件具有代理签名权, 这样可以防止代理签名权被滥用。

2.6　签名可追踪性分析

在 Li-Zhang方案中, 声称在签名过程中, B 和 R 之间实行的是交互协议, 在交互时, 消息并没有发给签名人, 所以签名人不知道所签消息是什么, 当签名 (U, r, v) 被公开后, 他也无法将其与某个签名联系起来。但实际上, 只要盲签名人 B 记录所有他能够收集到的每次签名时的交互信息 (r_B, v', U_B), 即使最终签名 (U, r, v) 是用随机值 P_3 和 k 处理后的结果, 当签名 (U, r, v) 被公开后, B 可以计算 $v'' = H_2(M, r)$, $k' = v''/v'$, 然后计算 $P_3' = U - k' U_B$, 验证等式 $r = r_B^{k'} e(P_3', P)$ 是否成立, 若等式成立, 那么说明签名 (U, r, v) 就是 B 使用 (r_B, v', U_B) 所做出的盲签名, 所以上述的方案不具有不可追踪性。

3　改进的代理盲签名方案

针对 Li-Zhang方案存在的安全缺陷, 本节将从代理授权阶段和代理盲签名过程对其加以改进, 得到一个新方案。本文方案的系统参数设置如上述, 签名过程如下:

3.1　代理授权阶段

原始签名人 A 在开始代理授权之前先准备授权文件 m_W, 其中包含了代理人信息如代理签名人公钥以及代理签名的文件类型、时间以及代理签名文件的范围等信息, 这样保证了代理签名人只有在有效期内对特定的文件进行的代理签名才是有效的。A 选取 $P_1 \in_R G_1$, $t \in_R Z_q^*$, 将原方案的 $r_A = e(P_1, P)$ 改为 $r_A = e(P_1, P)^t$, 将 $v_A = H_2(ID_B, r_A)$ 改为 $v_A = H_2(m_W, r_A)$, 并将原方案的代理授权方程 $U_A = v_A S_A + P_1$ 改为 $U_A = v_A S_A + tP_1$, 这样能够有效的防止原始签名人冒充代理签名人伪造代理密钥对消息进行签名, 然后将 (U_A, v_A, r_A, m_W) 发送给 B。B 代理方验证等式 $r_A = e(U_A, P)(e(Q_A, Q_{TA}))^{-v_A}$ 是否成立, 如果成立, 则授权合法, 计算代理签名私钥: $S_P = U_A + v_A S_B$。

3.2　代理盲签名过程

代理人 B 选择 $P_2 \in_R G_1$, 计算 $r_B = e(P_2, P)$, 将 (r_A, r_B, v_A, m_W) 发送给消息持有人 R。R 选择 $P_3 \in_R G_1$, $k, c \in_R Z_q^*$, 将原方案的 $r = r_B^k e(P_3, P)$ 改为 $r = r_B^k e(P_3, P)^c$, 计算 $v = H_2(M, r)$, $v' = v/k$, 然后将盲化的消息 v' 发送给 B, B 计算 $U_B = v' S_P + P_2$, 并将 U_B 发送给 R, R 对 U_B 进行去盲, 计算 $U = kU_B + cP_3$, 则 B 对消息 M 的代理盲签名为 (U, r, v, m_W)。接受方 R 验证签名: $e(U, P) = e(Q_A, Q_{TA})^{v v_A} r_A^v e(Q_B, Q_{TA})^{v v_A r}$, 如果验证等式成立, 则 (U, r, v, m_W) 是 B 代表 A 对消息 M 的有效代理盲签名。该签名是可验证的, 这是因为:

$$
\begin{aligned}
&e(U, P) = e(kU_B + cP_3, P) = \\
&\quad e(k(v' S_P + P_2) + cP_3, P) = \\
&\quad e(vS_P, P) e(kP_2, P) e(cP_3, P) = \\
&\quad e(S_P, P)^v e(P_2, P)^k e(P_3, P)^c = \\
&\quad e(S_P, P)^v r_B^k e(P_3, P)^c = e(U_A + v_A S_B, P)^v r = \\
&\quad e(v_A S_A + tP_1 + v_A S_B, P)^v r = \\
&\quad e(S_A, P)^{v v_A} e(P_1, P)^{tv} e(Q_B, Q_{TA})^{v v_A} r = \\
&\quad e(Q_A, Q_{TA})^{v v_A} r_A^v e(Q_B, Q_{TA})^{v v_A} r
\end{aligned}
$$

3.3　安全性分析

由于有效的代理盲签名 (U, r, v, m_W) 中包含了授权证书 m_W, 且授权证书 m_W、原始签名人 A 和代理签名人 B 的公钥 Q_A、Q_B 都在签名的验证算法中出现, 易证本文的代理盲签名方案满足可验证性、可区分性、可识别性、不可否认性、抗滥用性, 下面主要分析其满足不可伪造性、盲性和不可追踪性。

定理 1　文中所提的代理盲签名方案具有不可伪造性。

证明　攻击者的最终目的是伪造基于身份的代理盲签名或授权证书。非形式地说, 对一个基于身份的代理盲签名体制, 如果攻击者存在性授权伪造 (提供一个新的授权证书) 成功或存在性代理盲签名伪造 (提供一个新的有效的 (授权证书、消息、代理盲签名) 组) 成功的概率是可以忽略的, 则称该体制是适应性选择消息和身份攻击下存在性不可伪造的。

首先, 我们将存在性授权伪造的困难性归约为 Hess[11]的基于身份签名体制的存在性不可伪造。本文方案在代理授权过程中用到的签名是 Hess签名的一种简单变形, 实质上完全等价。

签名: 攻击者随机选择 $P_1 \in G_1$, $t \in Z_q^*$, 计算 $r_A = e(P_1, P)^t$, $v_A = H_2(m_W, r_A)$, $U_A = v_A S_A + tP_1$, 则授权证书为 $\sigma = (m_W, v_A, r_A, U_A)$。

验证: 当收到授权证书 σ 时, 验证者计算 $v_A = H_2(m_W, r_A)$ 和 $Q_A = H_1(ID_A)$, 授权证书时有效的, 当且仅当 $r_A =$

$e(U_A, P)(e(Q_A, Q_{TA}))^{-vA}$。

由于 Hess 的基于身份的签名已经在随机预言机模型中被证明对适应性选择消息及身份攻击是存在性不可伪造的，所以本文方案也能够抵抗存在性授权伪造攻击。

其次，代理盲签名的存在性不可伪造性可归约为离散对数问题假设。

假设原始签名人 A 欲伪造代理盲签名，他必须知道代理密钥 S_P，而由 $S_P = U_A + v_A S_B$ 和 $S_B = sQ_B$ 可知，A 必须知道代理签名人 B 的私钥 S_B，而 B 的私钥取决于可信中心的系统主密钥 s，通过 $Q_{TA} = sP$ 得到 s 相当于破解离散对数问题。H_1 和 H_2 均为密码学上的单向 Hash 函数，因此，除代理签名人 B 以外的其他人（包括原始签名人和其他第三方）通过原始签名人和代理签名人的公钥 Q_A，Q_B 来成功来建立有效的代理密钥的概率是可忽略的。既然原始签名人 A 不能伪造代理盲签名，其他任何攻击者更无法伪造代理盲签名，因此，该方案是不可伪造的。

定理 2　文中所提的代理盲签名方案具有盲性。

证明　关于盲性的定义可参考文献[12]。由签名算法，如果给定一个有效的代理盲签名 (U, r, v, m_W) 以及在签名发行过程中交换的数据 (r_B, v', U_B)，下列等式成立：

$$v' = v/k \tag{1}$$

$$U = kU_B + cP_3 \tag{2}$$

$$r = r_B^k e(P_3, P)^c \tag{3}$$

很显然，对于等式(1)，必存在一个唯一的盲因子 $k \in Z_q^*$ 满足 $k = v/v'$；同理，对于等式(2)，也必存在另一个唯一的盲因子 $cP_3 \in G_1$ 满足 $cP_3 = U - kU_B$。因为 (U, r, v, m_W) 是一个有效的代理盲签名，所以其满足验证方程 $e(U, P) = e(Q_A, Q_{TA})^{vvA} r_A^v e(Q_B, Q_{TA})^{vvA} r$，故：

$$\begin{aligned}
r &= e(U, P)e(Q_A, Q_{TA})^{-vvA} r_A^{-v} e(Q_B, Q_{TA})^{-vvA} = \\
&e(kU_B + cP_3, P)e(S_A, P)^{-vvA} e(P_1, P)^{-v} e(S_B, P)^{-vvA} = \\
&e(kU_B, P)e(P_3, P)^c e(v_A S_A + vP_1, P)^{-v} e(S_B, P)^{-vvA} = \\
&e(kU_B, P)e(P_3, P)^c e(U_A, P)^{-v} e(v_A S_B, P)^{-v} = \\
&e(kU_B, P)e(P_3, P)^c e(-v(U_A + v_A S_B), P) = \\
&e(kU_B, P)e(P_3, P)^c e(-vS_P, P) = \\
&e(kU_B - vS_P, P)e(P_3, P)^c = \\
&e(kU_B - kv'S_P, P)e(P_3, P)^c = \\
&e(U_B - v'S_P, P)^k e(P_3, P)^c = \\
&e(P_2, P)^k e(P_3, P)^c = r_B^k e(P_3, P)^c
\end{aligned}$$

从推导过程可知，盲因子 (k, cP_3) 总是存在且能够满足式(3)的定义，这点与文献[12]所证明签名的盲性原理相同。

定理 3　文中所提的代理盲签名方案具有不可追踪性。

证明　在所提方案中，给定一个合法的消息 — 签名对 (U, r, v, m_W)，对于一组代理签名人 B 所掌握的中间协议消息 (r_B, v', U_B)，不管它们是否相对应，都存在一组由消息持有人 R 秘密选取的随机数据 (k, c, P_3) 与之对应。这说明代理人签名 B 不能通过自己所掌握的 (r_B, v', U_B) 来确定 (U, r, v, m_W) 是否就是一个转化后公开的代理盲签名，因此改进方案具有不可追踪性。

4　性能评价

表 1 给出了本文方案和目前一些较为典型的基于身份的代理盲签名方案[7-8]的性能比较，为了方便，用 P_a 表示双线性映射中的对操作，P_m 表示 G_1 上的标量乘，忽略其他运算的消耗。在本文方案中，P_1，P_2 和 P_3 可以提前选取，因此可以对相关的双线性对 $e(P_1, P)$，$e(P_2, P)$，$e(P_3, P)$，$e(Q_A, Q_{TA})$ 和 $e(Q_B, Q_{TA})$ 进行预运算。同时，在考虑计算复杂性时也已经对文献[7]和文献[8]方案中的相关双线性对进行了预计算。

表 1　本文方案与其他方案的性能比较

方案	代理密钥生成阶段	签名生成阶段	签名验证阶段
文献[7]方案	$2P_a + 4P_m$	$2P_a + 6P_m$	$3P_a + 1P_m$
文献[8]方案	$1P_a + 2P_m$	$1P_a + 6P_m$	$1P_a$
本文方案	$1P_a + 3P_m$	$4P_m$	$1P_a$

可以看出，文献[7]方案的计算复杂度大约是 $7P_a + 11P_m$，文献[8]方案的计算复杂度大约是 $3P_a + 8P_m$，而本文方案的计算复杂度大约是 $2P_a + 7P_m$。尽管人们对对运算的有效实现作了相当的研究，但目前对运算仍然是基于身份密码体制实现中效率的瓶颈。显然，本文方案在签名生成阶段不需要双线性对运算，因此相比而言具有明显的效率优势。

5　结语

针对文献[9]提出的代理盲签名方案中存在的各种安全缺陷，本文给出了一种改进方案，改进的方案能够有效地防止原始签名人冒充代理签名人对消息进行签名。在该方案中，原始签名人通过授权证书适当的限制代理签名人的权力范围和期限，制止了可能的签名滥用问题。同时，当签名被泄露后，代理签名人不能将自己在签名协议中的签名和签名的消息联系起来，保护了消息持有人的权益。本文方案在签名生成阶段不需要双线性对运算，与已有的一些典型的基于身份的代理盲方案相比，本文方案的效率更高。

参考文献：

[1] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures: delegation of the power to sign messages[J]. IEICE Transactions on Fundamentals, 1996, E79-2A(9): 1338-1353.

[2] LIN W D, JAN J K. A security personal learning tools using a proxy blind signature scheme[C]// Proceedings of International Conference on Chinese Language Computing. Washington: IEEE Computer Society, 2000: 273-277.

[3] 谭作文，刘卓军，唐春明. 基于离散对数的代理盲签名[J]. 软件学报，2003，14(11)：1931-1935.

[4] AWASTHI A K, LAL S. Proxy blind signature scheme[J]. JFCR Transaction on Cryptology, 2005, 2(1): 5-11.

[5] SUN H M, HSIEH B T. On the security of some proxy blind signature schemes[EB/OL]. [2007-08-20]. http://eprint.iacr.org.

[6] SHAMIR A. Identity-based cryptosystems and signature schemes[EB/OL]. [2007-08-15]. http://www.iseca.org/downloads/Shamir47.pdf.

[7] ZHENG DONG, HUANG ZHENG, CHEN KE-FEI. ID-based proxy blind signature[C]// 18th International Conference on Advanced Information Networking and Applications [s.l.]: IEEE, 2004: 380-383.

[8] LANG WEI-MIN, TAN YUN-MENG, YANG ZONG-KAI. A new efficient ID-based proxy blind signature scheme[C]// ISCC 2004. Washington: IEEE Computer Society, 2004: 407-411.

[9] 李素娟，张福泰. 基于 ID 的代理盲签名[J]. 计算机工程，2006，32(17)：203-204.

[10] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[C]// Asiacrypt 2001, LNCS 2248. Berlin: Springer, 2001: 514-532.

[11] HESS F. Efficient identity based signature schemes based on pairing[C]// SAC 2002, LNCS 2596. Berlin: Springer, 2003: 310-324.

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