第 37 卷 第 24 期
Vol.37 No.24

计 算 机 工 程
Computer Engineering

2011 年 12 月
December 2011

• 安全技术 •

文章编号：1000—3428(2011)24—0114—03 文献标识码：A 中图分类号：TP311

一种基于身份的代理盲签名方案

丁圣龙，赵一鸣

(复旦大学软件学院，上海 200433)

摘 要：分析一种代理盲签名方案，指出其在生成代理盲签名过程中存在的安全问题，由于不恰当地使用预计算，使攻击者可以轻易计算出代理密钥。为克服该缺陷，提出一种新的基于身份的代理盲签名方案，该方案能够满足不可伪造性、盲性等安全特性，相比于同类方案，其计算复杂度更低。

关键词：基于身份；代理盲签名；双线性对；盲性；代理密钥安全

ID-based Proxy Blind Signature Scheme

DING Sheng-long, ZHAO Yi-ming

(Software School, Fudan University, Shanghai 200433, China)

【Abstract】A proxy blind signature scheme is analyzed. It is found that proxy blind signature generation phase in this scheme is not secure, adversaries can easily find out the proxy key due to improper use of pre-computation. To resolve the problem, this paper proposes a new ID-based proxy blind signature scheme which satisfies the required security properties of unforgeability and blindness. It has lower computing complex compared with other schemes.

【Key words】ID-based; proxy blind signature; bilinear pairings; blindness; proxy key security

DOI: 10.3969/j.issn.1000-3428.2011.24.038

1 概述

代理签名允许原始签名人将签名的权力委托给代理签名人，由代理签名人代替他进行签名，在分布式计算等需要权力委托的应用场景中受到重视。盲签名允许签名请求人在签名者不获知签名消息和最终签名的前提下获取签名，解决了匿名性问题，在电子货币和电子投票等领域中被广泛应用。结合代理签名和盲签名，有学者提出了代理盲签名的概念。

基于身份的公钥系统[1]允许根据用户的唯一标识符(如邮箱、身份证号等)生成公钥，而用户私钥则由可信第三方密钥生成中心 PKG 生成；与基于证书的公钥系统相比，基于身份的公钥系统简化了密钥管理和证书验证，将用户身份与其公钥以最自然的方式捆绑在一起。后来，人们发现利用双线性对可以高效地实现基于身份的加密和签名。最近，利用双线性对构造的基于身份的代理盲签名方案[2-3]相继被提出。不过，文献[4]指出文献[2]方案存在安全缺陷，原始签名人的私钥容易泄漏，同时提出一个改进方案，但是改进方案的效率不高。文献[5]指出文献[3]方案不满足不可伪造性和不可追踪性，并提出一个改进方案。

本文分析文献[5]方案存在的安全缺陷，基于文献[6]中高效安全的基于身份的签名方案，提出一种新的基于身份的代理盲签名方案，证明新方案满足代理盲签名方案应具备的安全特性，且没有文献[5]方案的安全缺陷。

2 预备知识

2.1 双线性对

设 G_1 是素数 q 阶循环加法群，P 是 G_1 的生成元。G_2 是素数 q 阶循环乘法群。双线性对 $e:G_1\times G_1\to G_2$，具有以下性质：

(1)双线性性：$e(aP,bQ)=e(P,Q)^{ab}$。

(2)非退化性：存在 $P,Q\in G_1$，满足 $e(P,Q)\neq 1$。

(3)可计算性：对任意 $P,Q\in G_1$，存在高效算法计算 $e(P,Q)$。

2.2 安全性定义

一般来说，一个基于身份的代理盲签名应该满足以下 5 个性质：

(1)可验证性：从代理盲签名中，验证人可以验证签名的正确性，并验证原始签名人对所签消息的认可。

(2)不可否认性：一旦代理签名人代表原始签名人创建了一个有效的代理盲签名，那么代理签名人不能否认其签名行为，原始签名人也不能否认其授权给代理签名人。

(3)可区分性：任何人都能够区分代理盲签名和一般签名。

(4)不可伪造性：只有被原始签名人委托过的代理签名人能够生成正确的代理盲签名，原始签名人和其他任何人都不能伪造出代理盲签名。

(5)盲性：签名人在签名过程中无法知道消息的内容，签名完成之后也无法将签名过程中获得的数据与签名结果进行链接。关于盲性的详细描述可参考文献[7]中的定义 2。

3 代理密钥安全

文献[5]指出文献[3]中的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，同时指出该方案也不满足盲性，在此基础之上，文献[5]提出一个改进的代理盲签名方案。经过分析后发现，文献[5]方案存在安全缺陷，攻击者通过窃听容易计算出代理密钥，进而可以伪造代理盲签名，具体分析如下：

基金项目：“十一五”国家密码发展基金资助项目

作者简介：丁圣龙(1988－)，男，硕士研究生，主研方向：密码学，信息安全；赵一鸣，副教授

收稿日期：2011-06-22 **E-mail：**10212010009@fudan.edu.cn

文献[5]方案在生成代理盲签名阶段，代理签名人 B 选择 $P_2 \in_R G_1$，计算 $r_B = e(P_2, P)$，将(r_B, r_A, v_A, m_W)发送给签名请求人 R。R 选择 $P_3 \in_R G_1$，$k, c \in_R Z_q^*$，计算 $r = r_B^k e(P_3, P)^c$，$v = H_2(M, r)$，$v' = vk^{-1}$，然后将 v'发送给 B。B 计算 $U_B = v'S_P + P_2$，将 U_B发送给 R。R 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)。

但文献[5]指出 P_2 可以提前选取，从而 $e(P_2, P)$ 可以进行预计算，预计算也正是文献[2,3,5]方案具有较高效率的原因。但是如果使用预计算，B 在短时间内不会对 P_2 重新选值，而是利用预计算的 $e(P_2, P)$ 直接生成签名。基于此，文献[5]方案并不具备不可伪造性，任何人都可以通过窃听短时间内 B 进行的 2 次签名过程计算出代理密钥 S_P，具体过程如下：

假设第 1 次签名过程中，B 发送出 r_{B1} 后，签名请求人计算出 v'_1返还给 B，B 计算$U_{B1} = v'_1 S_P + P_2$并发回；第 2 次签名过程中，B 发出 r_{B2} 后，签名请求人计算出 v'_2返还给 B，B 计算$U_{B2} = v'_2 S_P + P_2$ 并发回。如果 2 次签名过程间隔较短，会有 $r_{B1} = r_{B2}$，即 B 使用的预先计算的同一个 $e(P_2, P)$，这样一来，攻击者可以计算$U_{B1} - U_{B2} = (v'_1 - v'_2)S_P$(在 G_1 中计算 U_{B2} 的逆元-U_{B2} 是容易的)，而 $v'_1, v'_2 \in Z_q^*$是已知的，所以计算 $(v'_1 - v'_2)$ 及其逆元 $(v'_1 - v'_2)^{-1}$ 是容易的，进而可以计算 $S_P = (v'_1 - v'_2)^{-1}(U_{B1} - U_{B2})$，得到代理密钥之后，攻击者便可以伪造出有效的代理盲签名。

综上所述，文献[5]方案是不安全的。一种可行的改进办法是代理签名人在计算 r_B 时选取随机因子 d 并令 $r_B = e(P_2, P)^d$，在签名请求人返回 v'时，计算 U_B 为 $U_B = v'S_P + dP_2$。

4 新的基于身份的代理盲签名方案

为克服文献[5]方案的安全缺陷，本文根据文献[6]提出的高效安全的基于身份的签名方案，提出一种新的基于身份的代理盲签名方案，新方案在保证安全性的同时，也具备了较高的效率。

4.1 系统设置

密钥生成中心 PKG 选择合适的系统参数。G_1 为循环加法群，G_2 为循环乘法群，G_1, G_2 的阶均为素数 q，P 为 G_1 的生成元，双线性对 $e: G_1 \times G_1 \to G_2$，$H_1, H_2$ 是 2 个密码学上的单向哈希函数 $H_1: \{0,1\}^* \to G_1$，$H_2: \{0,1\}^* \times G_2 \to Z_q^*$。最后 PKG 选择主密钥 $s \in_R Z_q^*$，计算 $P_{pub} = sP$，将 s 秘密保存，公开系统参数：$params=\{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$。

4.2 私钥提取

原始签名人 A 和代理签名人 B 向 PKG 提交身份信息 ID_A, ID_B，PKG 计算他们相应的公钥/私钥对为 $Q_A = H_1(ID_A)$，$S_A = sQ_A$ 和 $Q_B = H_1(ID_B)$，$S_B = sQ_B$，然后将私钥通过安全信道发送给 A 和 B。

4.3 代理密钥生成

原始签名人 A 创建授权文件 m_W 来明确 A 对代理签名人 B 的授权以及 B 的权力限制和有效时间，这样保证了 B 只有在有效期内对特定的文件才能进行有效的代理签名。A 选择 $r \in_R Z_q^*$，计算 $R_A = e(Q_A, P_{pub})^r$，$h = H_2(m_W, R_A)$，$V_A = (rh + 1)S_A$，然后将(R_A, V_A, m_W)发送给 B。B 验证等式 $e(V_A, P) = R_A^{H_2(m_W, R_A)} e(Q_A, P_{pub})$ 是否成立，如果成立，B 计算代理密钥 $S_P = V_A + S_B$。

4.4 代理盲签名

代理签名人 B 选择 $d \in_R Z_q^*$，计算 $R' = e(S_P, P)^d$，将 R'发送给签名请求人 U。U 选择 $P_1 \in_R G_1$，$k, c \in_R Z_q^*$，计算 $R = R'^k e(P_1, P)^c$，$h = H_2(M, R)$，$h' = hk$，然后将 h'发送给 B。B 计算 $V' = (dh' + 1)S_P$，将(m_W, R_A, V')发送给 U。U 计算 $V = V' + hcP_1$，则 B 对消息 M 的代理盲签名为(V, R, R_A, m_W)。

4.5 验证

验证者首先验证消息 M 是否满足代理授权文件 m_W 中的约定，若满足，再验证等式 $e(V, P) = R^{H_2(M,R)} R_A^{H_2(m_W, R_A)} e(Q_A + Q_B, P_{pub})$ 是否成立，若成立，表示(V, R, R_A, m_W)为 B 代表 A 生成的一个对消息 M 有效代理盲签名。

5 新方案分析

5.1 安全性分析

由于有效的代理盲签名(V, R, R_A, 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，因此容易证明本文的代理盲签名方案满足不可否认性和可区分性。下面主要分析可验证性、不可伪造性和盲性。

(1)可验证性

如果(V, R, R_A, m_W)是消息 M 的有效签名，那么必然满足：

$$\begin{aligned} e(V, P) &= e((dh' + 1)S_P, P) e(P_1, P)^{hc} = \\ & e(S_P, P)^{dhk} e(P_1, P)^{hc} e(S_P, P) = \\ & R'^{hk} e(P_1, P)^{hc} e(V_A, P) e(S_B, P) = \\ & R^{H_2(M,R)} R_A^{H_2(m_W, R_A)} e(P_A + P_B, P_{pub}) \end{aligned}$$

(2)不可伪造性

本文提出的新的基于身份的代理盲签名方案的不可伪造性的证明可以归约到文献[6]提出的基于身份的签名方案。具体分析如下：

1)攻击者在不知道代理密钥 S_P 的情况下伪造出一个有效的代理盲签名。

由于本文方案中代理盲签名阶段是基于文献[6]方案，因此攻击者必然能够构造出文献[6]方案的一个有效签名，不过该方案已经被证明基于 CDHP 假设是不可伪造的，所以攻击者无法构造出一个有效的代理盲签名。

2)攻击者首先伪造出一个有效的代理密钥 S_P，再伪造一个有效的代理盲签名。

由于代理盲签名过程中，攻击者需要发送 R_A，因此攻击者能够伪造出一对有效的(S_P, R_A)满足：

$$e(S_P, P) = R_A^{H_2(m_W, R_A)} e(Q_A + Q_B, P_{pub})$$

如果攻击者为 B，那么根据 $S_P = V_A + S_B$ 可以计算出 V_A，所以 B 能够伪造出一对有效的(V_A, R_A)，而这正是 A 对授权文件 m_W 的签名，因此 B 能够伪造出文献[6]方案的一个有效签名，矛盾。

如果攻击者为 A，如果 A 首先选择 S_P，那么由于 H_2 是密码学上的单向哈希函数，A 通过等式 $e(S_P, P) = R_A^{H_2(m_W, R_A)} e(Q_A + Q_B, P_{pub})$ 来计算出 R_A 的概率是可以忽略的；所以 A 必须首先构造出 $R_A = e(Q_A, P_{pub})^r$，那么计算 $S_P = (rH_2(m_W, R_A) + 1)S_A + S_B$ 就必须知道 S_B，而显然 A 无法获得 B 的私钥 S_B，因此也就无法计算 S_P。

如果攻击者不是 A 或 B，攻击能力更弱，更不可能伪造出有效的代理密钥。

综上所述，本文方案具有不可伪造性。

(3)盲性

定理 本文方案具有盲性。

证明：考虑文献[7]定义 2 中的游戏，设 $\tilde{A}$ 是签名人或一个控制签名人的 PPT 算法，并通过私钥提取获得了签名人 B 的公私钥对(Q_B, S_B)。

如果 $\tilde{A}$ 得到⊥，则显然 $\tilde{A}$ 赢得游戏的概率为 1/2。现在考虑 $\tilde{A}$ 获得 2 个有效签名的情形。对于 i=0, 1，设(R'_i, h'_i, V'_i)为签名过程中交换的变量，将最终签名(V_0, R_0)、(V_1, R_1)交给 $\tilde{A}$。那么可以证明存在 2 个随机因子(k, c)使得对于每一个 i, $j \in \{0,1\}$，能够将(R'_i, h'_i, V'_i)映射到(V_j, R_j)，这样的 $k = h'_i h_j^{-1}$，c 满足 $V_j = V'_i + h_j c P_1$。由于 $e(V'_i, P) = R_i^{h'_i} e(S_P, P)$，$e(V_j, P) = R_j^{h_j} e(S_P, P)$，因此有：

$$R_i'^{k} e(P_1, P)^c = R_i^{h'_i h_j^{-1}} e(P_1, P)^c =$$
$$(e(V'_i, P)/e(S_P, P))^{h_j^{-1}} e(P_1, P)^c =$$
$$e(V'_i + h_j c P_1, P)^{h_j^{-1}} e(S_P, P)^{-h_j^{-1}} =$$
$$e(V_j, P)^{h_j^{-1}} e(S_P, P)^{-h_j^{-1}} = R_j$$

所以，(R'_i, h'_i, V'_i)和(R_j, V_j)之间的关系是相同的；并且无论(R'_i, h'_i, V'_i)和(R_j, V_j)为何值，上面的盲因子(k, c)总是存在的。所以，即使 $\tilde{A}$ 有无限能力，它输出正确 b'的概率仍为 1/2。

综合上述 2 种情形，$\tilde{A}$ 赢得游戏的概率为 1/2，因此，本文方案具有盲性。

(4)代理密钥安全性分析

本文方案不存在文献[5]中代理密钥泄漏的安全缺陷。

假设第 1 次签名过程中，B 发出 $R'_1 = e(S_P, P)^{d_1}$ 后，签名请求人计算出 h'_1返还给 B，B 计算 $V'_1 = (d_1 h'_1 + 1) S_P$ 并发回；在第 2 次签名过程中，B 发出 $R'_2 = e(S_P, P)^{d_2}$ 后，签名请求人计算出 h'_2返还给 B，B 计算 $V'_2 = (d_2 h'_2 + 1) S_P$ 并发回。但是攻击者无法通过$(R'_1, R'_2, h'_1, h'_2, V'_1, V'_2)$计算出 S_P，这是因为 $S_P = (d_1 h'_1 - d_2 h'_2)^{-1}(V'_1 - V'_2)$，攻击者能够计算出 S_P 当且仅当攻击者知道 d_1 和 d_2(仅知道 d_1 或 d_2 也可以利用 $S_P = (d_i h'_i + 1)^{-1} V'_i$ 计算出 S_P)，而 d_1、d_2 是签名人选取的，攻击者无法获得。

5.2 性能分析

表 1 给出了本文方案和具备同等安全性的基于身份的代理盲签名方案[4]及文献[5]中存在安全缺陷的方案的性能比较，方便起见，用 P_a 表示双线性对中的对运算，P_m 表示 G_1 上的标量乘，P_e 表示 G_2 上的指数运算，忽略其他运算。在本文方案中，P_1 由签名请求人提前选取，所以 $e(P_1, P)$ 可以预先计算；另外 $e(Q_A, P_{pub})$，$e(S_P, P)$，$e(Q_B, P_{pub})$ 也是可以预计算的。同时，在考虑计算复杂性时也对文献[4-5]方案的相关双线性对进行预计算。

表 1 3 种方案的性能比较

方案	生成代理密钥	代理盲签名	签名验证
文献[5]	$1P_a+3P_m+2P_e$	$4P_m+2P_e$	$1P_a+3P_e$
文献[4]	$2P_a+3P_m$	$4P_m+3P_e$	$2P_a+2P_e$
本文方案	$1P_a+1P_m+2P_e$	$2P_m+3P_e$	$1P_a+2P_e$

在各种运算中，最耗时的是 P_a，其次是 P_m 和 P_e。从表 1 可以看出，文献[5]方案的计算复杂度约为 $2P_a+7P_m+7P_e$，文献[4]方案的计算复杂度约为 $4P_a+7P_m+5P_e$，本文方案的计算复杂度约为 $2P_a+3P_m+7P_e$。与具备同等安全性的方案[4]相比，本文方案减少了 2 个双线对运算，在效率上有了很大提高；相比于文献[5]方案，本文方案在克服该方案中的安全缺陷的同时，效率上也略有提高。

6 结束语

在对文献[5]方案分析后发现，该方案生成代理盲签名算法中存在安全缺陷，由于不恰当地使用预计算导致攻击者容易计算出代理密钥，从而不满足不可伪造性。为克服这一缺陷，本文基于文献[6]方案，提出了一种新的基于身份的代理盲签名方案，并证明新方案可以满足代理盲签名方案应该具备的安全性及较高的效率。

参考文献

[1] Shamir A. ID-based Cryptosystems and Signature Schemes[C]// Proc. of CRYPTO'84. New York, USA: [s. n.], 1984.

[2] 张学军, 王育民. 高效的基于身份的代理盲签名[J]. 计算机应用, 2006, 26(11): 2586-2588.

[3] 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.

[4] 张 妮, 奚雪峰, 陆卫忠, 等. 基于身份的代理盲签名方案分析与改进[J]. 计算机工程, 2010, 36(16): 110-112.

[5] 农 强, 吴顺祥. 一种基于身份的代理盲签名方案的分析与改进[J]. 计算机应用, 2008, 28(8): 1940-1942.

[6] Huang Zhenjie, Chen Kefei, Wang Yuming. Efficient Identity-based Signatures and Blind Signatures[C]//Proc. of CANS'05. Berlin, Germany: [s. n.], 2005.

[7] Zhang Fangguo, Kim K. ID-based Blind Signature and Ring Signature from Pairings[C]//Proc. of ASIACRYPT'02. Berlin, Germany: [s. n.], 2002.

编辑 陈 文

(上接第 113 页)

方法能够有效抵抗一阶、二阶无效曲线攻击和符号改变故障攻击。由于仅需在算法初始化时进行预处理，因此本文方法易扩展到点乘的其他快速实现算法中，且其中间变量亦被随机化，使其具有一定的抵抗差分功耗分析攻击和差分电磁分析攻击的能力。

参考文献

[1] Boneh D, de Millo R A, Lipton R J. On the Importance of Checking Cryptographic Protocols for Faults[C]//Proceedings of EUROCRYPT'97. [S. l.]: Springer-Verlag, 1997.

[2] 刘上力, 赵劲强, 聂勤务. AES 差分故障攻击的建模与分析[J]. 计算机工程, 2010, 36(1): 189-190.

[3] Biehl I, Meyer B, Müller V. Differential Fault Attacks on Elliptic Curve Cryptosystems[C]//Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer-Verlag, 2000.

[4] Blömer J, Otto M, Seifert J P. Sign Change Fault Attacks on Elliptic Curve Cryptosystems[J]. Lecture Notes in Computer Science, 2006, 4236: 36-52.

[5] Dottax E, Giraud C, Rivain M, et al. On Second-order Fault Analysis Resistance for CRT-RSA Implementations[J]. Lecture Notes in Computer Science, 2009, 5746: 68-83.

[6] Yen S M, Kim D, Lim S, et al. RSA Speedup with Residue Number System Immune Against Hardware Fault Cryptanalysis[C]//Proceedings of 2001 Information Security and Cryptology Conference. [S. l.]: Springer-Verlag, 2001: 397-413.

编辑 张 帆