改进的随机化部分盲签名方案

何俊杰， 王　娟， 祁传达

(信阳师范学院 数学与信息科学学院　河南 信阳 464000)

摘要: 对张建中等提出的基于双线性对的随机化部分盲签名方案进行了安全性分析,发现方案不能抵抗篡改公共信息攻击. 为此,提出了一个改进方案. 分析结果表明,改进方案在满足不可伪造性、不可追踪性的同时,能够有效防止恶意的签名请求者非法修改事先协商的公共信息,保护签名者的合法权益.

关键词: 盲签名; 部分盲签名; 公共信息; 双线性对

中图分类号: TP 309　　**文献标志码**: A　　**文章编号**: 1671 - 6841(2013)03 - 0041 - 04

DOI: 10.3969/j.issn/1671 - 6841.2013.03.010

0　引言

1982 年,Chuam 首次提出了盲签名的概念[1]. 盲签名可以有效地保护签名请求者的隐私,在匿名电子投票系统、不可跟踪的电子支付系统中有着广泛的应用. 但在盲签名的产生过程中,签名者对消息是不可见的,致使签名很容易被非法请求和使用. 1996 年,Abe 和 Fujisaki 提出了部分盲签名的概念[2]. 部分盲签名在待签消息的后面嵌入签名者和请求者事先协商的公共信息,可以对消息范围、签名有效期等进行限定. 部分盲签名方案既保护了签名请求者的隐私,又使签名者对消息是部分可控的,较好地解决了盲签名在匿名性和可控性之间的矛盾. 因此,部分盲签名一经提出,就受到了广泛关注,基于不同的数学难题,如离散对数问题[3]、大数分解问题[4]、计算 Diffie-Hellman 问题(CDHP)[5] 和 Chosen-target Inverse CDHP[6] 等,提出了大量的部分盲签名方案.

最近,张建中等[7] 设计了一种新的基于双线性对的随机化部分盲签名方案. 本文对文献[7]方案进行分析,结果表明方案不能抵抗篡改公共信息攻击. 针对文献[7]方案的安全缺陷,本文提出了一个改进方案,并对改进方案进行了详细的安全性分析.

1　文献[7]方案回顾

(a) 系统初始化. 签名者随机选择大素数 q,生成 q 阶加法循环群 G_1 和 q 阶乘法循环群 G_2; 选取 G_1 的生成元 P,并构造双线性对 $e: G_1 \to G_2$; 选择两个安全的哈希函数 $H_0: \{0,1\}^* \times G_1 \to G_1$, $H_1: \{0,1\}^* \to Z_q^*$; 随机选择私钥 $x_1, x_2 \in Z_q^*$,计算对应的公钥 $Y_1 = x_1 P$, $Y_2 = x_2 P$. 系统公开参数为 $\{q, H_0, H_1, G_1, G_2, e, P, Y_1, Y_2\}$.

(b) 盲化. 签名请求者与签名者事先协商好嵌入待签消息后面的公共信息 M. 签名者随机选择 $t \in Z_q^*$,计算 $W = tP$,并将 W 发送给请求者; 签名请求者收到 W 后,随机选择 $v, r_1, r_2 \in Z_q^*$,计算随机性参数 $U = vW$,计算 $M_1 = r_1 H_0(m \| U) + r_2 P$, $m_2 = r_1 v \bmod q$,并将盲消息 (M_1, m_2) 发送给签名者.

(c) 签名. 签名者收到 (M_1, m_2) 后,计算 $S' = x_1 M_1 + (x_2 + H_1(M)) m_2 W$,并将 S' 发送给请求者.

(d) 脱盲. 签名请求者计算 $S = r_1^{-1}(S' - r_2 Y_1)$,则消息 m 和公共信息 M 的签名为 (S, m, U, M).

(e) 验证. 验证者验证等式 $e(S, P) = e(H_0(m \| U), Y_1)\, e(U, Y_2)\, e(H_1(M) U, P)$ 是否成立,若等式成立,则签名有效,否则签名无效.

收稿日期: 2012 - 12 - 25

基金项目: 国家自然科学基金资助项目,编号 61272465; 河南省自然科学基金资助项目,编号 102102210242, 122400450189; 河南省教育厅科学技术研究重点项目,编号 12A520034.

作者简介: 何俊杰(1981 -),男,讲师,主要从事信息安全和密码学研究,E-mail: hejj99@163.com.

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

2 对文献[7]方案的篡改公共信息攻击

假设恶意的签名请求者试图将协商的公共信息 M 篡改为 $\hat{M}(\hat{M}\neq M)$. 在脱盲阶段,请求者收到签名者发来的 S' 后,计算 $\hat{S}'=S'+(H_1(\hat{M})-H_1(M))m_2W$, $S=r_1^{-1}(\hat{S}'-r_2Y_1)$,则 $(S,m,U,\hat{M})$ 为消息 m 和公共信息 $\hat{M}$ 的部分盲签名. 事实上,

$$\begin{aligned}e(S,P)&=e(r_1^{-1}(\hat{S}'-r_2Y_1),P)=e(r_1^{-1}(S'+H_1(\hat{M})m_2W-H_1(M)m_2W-r_2Y_1),P)\\&=e(r_1^{-1}(x_1M_1+(x_2+H_1(\hat{M}))m_2W-r_2Y_1),P)\\&=e(r_1^{-1}(x_1r_1H_0(m\|U)+r_2x_1P+(x_2+H_1(\hat{M}))r_1vW-r_2Y_1),P)\\&=e(x_1H_0(m\|U)+x_2U+H_1(\hat{M})U,P)=e(x_1H_0(m\|U),P)e(x_2U,P)e(H_1(\hat{M})U,P)\\&=e(H_0(m\|U),Y_1)e(U,Y_2)e(H_1(\hat{M})U,P),\end{aligned}$$

说明 $(S,m,U,\hat{M})$ 可以通过验证,是有效的部分盲签名.

3 文献[7]方案的改进

在文献[7]方案中,签名方程实质上可分为3项的和,即 $S'=x_1M_1+x_2m_2W+H_1(M)m_2W$,其中含公共信息 M 的项 $H_1(M)m_2W$ 对于签名请求者来说是可计算的. 所以,恶意的请求者在收到 S' 后,可利用 $\hat{S}'=S'+H_1(\hat{M})m_2W-H_1(M)m_2W$ 将 $H_1(M)$ 篡改为 $H_1(\hat{M})$,而验证者无法发现这种篡改.

为了防止不诚实的请求者篡改协商的公共信息,可以对文献[7]方案进行改进:

(a) 在初始化阶段,将哈希函数 H_1 改为 $H_1:\{0,1\}^*\rightarrow G_1$.

(b) 在签名阶段,将签名方程改为 $S'=x_1M_1+x_2m_2W+tm_2H_1(M)$.

(c) 在验证阶段,验证方程相应的改为 $e(S,P)=e(H_0(m\|U),Y_1)e(H_1(M)+Y_2,U)$.

4 改进方案的分析

4.1 正确性分析

改进方案的正确性可以由(1)式保证.

$$\begin{aligned}e(S,P)&=e(r_1^{-1}(S'-r_2Y_1),P)=e(r_1^{-1}(x_1M_1+x_2m_2W+tm_2H_1(M)-r_2Y_1),P)\\&=e(r_1^{-1}(x_1r_1H_0(m\|U)+r_2x_1P+x_2r_1vW+tr_1vH_1(M)-r_2Y_1),P)\\&=e(x_1H_0(m\|U)+x_2U+tvH_1(M),P)=e(x_1H_0(m\|U),P)e(x_2U,P)e(H_1(\hat{M}),tvP)\\&=e(H_0(m\|U),y_1)e(U,y_2)e(H_1(\hat{M}),U)=e(H_0(m\|U),Y_1)e(U,Y_2)e(H_1(M)U,P).\end{aligned}\quad(1)$$

4.2 安全性分析

4.2.1 不可伪造性

定理1 在随机预言模型和CDHP困难的假设下,改进方案对自适应选择消息攻击是存在不可伪造的.

证明 假设攻击者 A 能够以不可忽略的概率伪造签名,下面构造算法 C 解决CDHP.

给定 $aP,bP\in G_1$,其中 $a,b\in Z_q^*$ 未知,为了计算 abP,算法模拟挑战者 C 与攻击者 A 进行交互,回答攻击者 A 的询问. 具体过程如下:

(a) 系统设置. 挑战者 C 生成系统参数 $\{q,H_0,H_1,G_1,G_2,e,P,Y_1,Y_2\}$,并发送给攻击者 A,其中 $Y_1=aP$,即用 a 模拟用户的第一个私钥 x_1.

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

(b) 询问. A 可以向 C 提出多项式有界次的 H_0,H_1 随机预言询问和签名询问.

(i) H_0 询问. C 通过维护列表 L_0 响应 A 的 H_0 询问. 关于 (m_i,U_i) $(1\leqslant i\leqslant q_0)$ 的每一次询问,C 首先检查 L_0,如果在 L_0 中已经存在项 (m_i,U_i,δ_i,H_i),C 将 H_i 返回给 A 作为 $m_i\parallel U_i$ 的 H_0 哈希值; 否则,C 随机选取 $\delta_i\in_R Z_q^*$,计算 $H_i=\delta_i P$,将 (m_i,U_i,δ_i,H_i) 添加到 L_0,并将 $H_0(m_i\parallel U_i)=H_i$ 返回给 A.

(ii) H_1 询问. C 通过维护列表 L_1 响应的 H_1 询问. 关于 M_i $(1\leqslant i\leqslant q_1)$ 的每一次询问,C 首先检查 L_1,如果在 L_1 中已经存在项 (M_i,τ_i,H_i'),C 将 H_i' 返回给 A 作为 M_i 的 H_1 哈希值; 否则,C 随机选取 $\tau_i\in_R Z_q^*$,计算 $H_i'=\tau_i P$,将 (M_i,τ_i,H_i') 添加到 L_1,并将 $H_1(M_i)=H_i'$ 返回给 A.

(iii) 签名询问. 对 A 关于 (m,M) 的签名询问(假设已经做过关于 M 的 H_1 询问,否则先执行 H_1 询问),C 从 L_1 中找出项 (M,τ,H'); 随机选取 $k,\delta\in_R Z_q^*$,计算 $U=kP$,如果 (m,U,δ,H) 已经在 L_0 中,则重新选取 k 和 δ 并计算 U; 计算 $S=\delta Y_1+k(Y_2+H')$,并将 (m,U,δ,H) 加到 L_0. C 将 $\sigma=(U,S)$ 返回给 A 作为 (m,M) 的签名. C 对 A 的所有签名询问的回答是有效的. 事实上,

$$e(S,P)=e(\delta Y_1+k(Y_2+H'),P)=e(Y_1,H)\,e(Y_2+H',U)=e(Y_1,H_0(m\parallel U))\,e(Y_2+H_1(M),U),$$

即 $\sigma=(U,S)$ 是 (m,M) 的有效盲签名.

(c) 伪造. 如果算法没有终止,则 A 在没有做过 (m^*,M^*) 的签名询问的情况下,以不可忽略的概率对消息 (m^*,M^*) 输出一个有效的部分盲签名 (U,S). 根据 Forking 引理[8],通过对 A 哈希重放,C 可以获得消息 (m^*,M^*) 的两个有效签名 (m^*,M^*,U,H,H',S_1) 和 $(m^*,M^*,U,\hat{H},H',\hat{S}_1)$,其中 $\hat{H}=H+bP$. 由验证方程知有效签名满足 $S=x_1H_0(m\parallel U)+k(H_1(M)+Y_2)$,其中 $U=kP$,所以

$$S=x_1H+k(H'+Y_2),\ \hat{S}=x_1\hat{H}+k(H'+Y_2),$$

于是 $k(H'+Y_2)=S-x_1H=\hat{S}-x_1\hat{H}$,所以 $\hat{S}-S=x_1(\hat{H}-H)=abP$,则 C 得到 CDHP 的解.

综上所述,在 CDHP 困难的假设下,改进方案对自适应选择消息攻击是存在不可伪造的.

4.2.2　部分盲性

一方面,签名请求者在不知道 t 的情况下无法计算 $tm_2H_1(M)$,当然也就无法通过第 2 节的攻击方法篡改协商的公共信息 M. 另一方面,由于签名者是对 (M_1,m_2) 进行签名的,而 (M_1,m_2) 是请求者将原始消息 m 经过盲化因子盲化和哈希函数双重作用后的数据,在不知道盲化因子 $v,r_1,r_2\in Z_q^*$ 的情况下,签名者得不到原始消息的任何信息.

4.2.3　不可链接性

假设签名者保留了每次签名的中间结果 (t,W,M_1,m_2,S'). 当用户公布签名 $(m,M,(S,U))$ 后,考虑等式:

$$U=vW, \tag{2}$$

$$M_1=r_1H_0(m\parallel U)+r_2P, \tag{3}$$

$$m_2=r_1v \bmod q, \tag{4}$$

$$S=r_1^{-1}(S'-r_2Y_1), \tag{5}$$

由式(2)可以唯一确定 $v\in Z_q^*$,记为 $v^*=\log_U W$; 进而由式(4)可以唯一确定 $r_1\in Z_q^*$,记为 $r_1^*=m_2v^{*-1}$; 最后由式(3)可以唯一确定 $r_2\in Z_q^*$,记为 $r_2^*=\log_P(M_1-r_1^*H_0(m\parallel U))$. 下面说明由式(2),(3),(4)唯一确定的 v^*,r_1^*,r_2^* 满足式(5). 由于 S' 满足 $S'=x_1M_1+x_2m_2W+tm_2H_1(M)$,则

$$\begin{aligned}S'-r_2^*Y_1&=x_1M_1+x_2m_2W+tm_2H_1(M)-r_2^*x_1P=x_1(M_1-r_2^*P)+m_2(x_2W+tH_1(M))\\&=x_1r_1^*H_0(m\parallel U)+r_1^*v^*(x_2W+tH_1(M)),\end{aligned}$$

进而

$$\begin{aligned}e(r_1^{*-1}(S'-r_2^*Y_1),P)&=e(x_1H_0(m\parallel U),P)\,e(v^*x_2W+v^*tH_1(M),P)\\&=e(H_0(m\parallel U),Y_1)\,e(v^*W,x_2P)\,e(H_1(M),v^*tP)\\&=e(H_0(m\parallel U),Y_1)\,e(v^*W,Y_2)\,e(H_1(M),v^*W)\\&=e(H_0(m\parallel U),Y_1)\,e(U,Y_2+H_1(M))=e(S,P),\end{aligned}$$

即 $S=r_1^{*-1}(S'-r_2^*Y_1)$,表明由式(2),(3),(4)确定的 v^*,r_1^*,r_2^* 满足式(5).

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

因此,在签名者保留的任一组签名中间数据和公开的任一个有效部分盲签名之间总可以确定一组盲因子. 所以,即使签名者具有无限的计算能力,也不能将用户公布的部分盲签名与他的某个签名过程联系起来,当然也就无法追踪到签名的请求者. 也就是说,改进方案满足不可链接性.

4.3 性能比较

将改进的新方案与文献[7]方案进行计算性能方面的比较. 可以发现,改进方案在签名阶段增加了一次G_1中的标量乘运算,但是在验证阶段又减少了一次G_1中的标量乘运算,所以总的计算复杂度变化不大.

5 结束语

对张建中等人[7]提出的基于双线性对的随机化部分盲签名方案进行安全性分析,结果显示方案不能抵抗恶意请求者对协商的公共信息的篡改攻击. 本文对方案进行了改进,分析表明改进方案不仅满足不可链接性和不可伪造性,还能有效防止恶意签名请求者篡改公共信息.

参考文献:

[1] Chaum D. Blind signatures for untraceable payments [C] //Advances in Cryptology-CRYPTO 82. New York: Plenum Press, 1983: 199 - 203.

[2] Abe M, Fujisaki E. How to date blind signatures [C] // Advances in Cryptology-ASIACRYPTO96, LNCS 1163. Berlin: Springer-Verlag, 1996: 244 - 251.

[3] Abe M, Okamoto T. Provably secure partially blind signatures [C] // Advances in Cryptology-CRYPTO00, LNCS 1880. Berlin: Springer-Verlag, 2000: 271 - 286.

[4] Lin D D, Xui R. A randomized RSA-based partially blind signature scheme for electronic cash [J]. Computers and Security, 2005, 24(1): 44 - 49.

[5] 何俊杰,王娟,祁传达. 安全高效的基于身份的部分盲签名方案[J]. 计算机应用, 2012, 32(5): 1388 - 1391.

[6] Zhang F G, Safavi-Naini R, Susilo W. Efficient verifiably encrypted signature and partially blind signature from bilinear pairings [C] //Proc of Indocrypt'03, LNCS 2904. Berlin: Springer-Verlag, 2003: 191 - 204.

[7] 张建中,马冬兰. 一种随机化部分盲签名方案[J]. 计算机工程,2011, 37(23): 127 - 128.

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

Improved Randomized Partially Blind Signature Scheme

HE Jun-jie, WANG Juan, QI Chuan-da

(*College of Mathematics and Information Science, Xinyang Normal University, Xinyang* 464000, *China*)

Abstract: The security of the randomized partially blind signature scheme based on bilinear pairing proposed by Zhang et al. was analyzed. And the result showed that the scheme couldn't resist the tampering common information attack. An improved scheme was proposed to overcome the attack. Security analysis results showed that the improved scheme not only satisfied unforgeability and unlinkability, but also could prevent the malicious signature requesters from tampering the common information which the signer and the user had agreed on, and protect the legal rights and interests of the signers effectively.

Key words: blind signature; partially blind signature; common information; bilinear pairing

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net