LeeB 私钥分发协议的改进方案

侍伟敏
（北京工业大学 计算机学院，北京 100124）

摘 要：为了解决 LeeB 协议中存在的用户私钥托管问题，通过采用公开的身份密钥对来确认用户的身份，提出一种改进方案，并分析了该方案的安全性与执行效率. 改进方案解决了 LeeB 协议中存在的安全问题，且运算量减少了 $4n$ 次对运算和 $2n$ 次哈希运算.

关键词：基于身份的加密；私钥分发协议；私钥托管；身份密钥对
中图分类号：TP 309 **文献标志码**：A **文章编号**：0254 - 0037(2010)03 - 0401 - 04

IBE 身份认证技术可采用用户的身份标识，如电话号码、e-mail 地址和身份证号码等，这些公钥与用户的身份绑定，不需要公钥证书来确认用户身份[1-3]. IBE 不需要对证书进行管理. 当 KGC 向用户分发私钥时，需要在 KGC 和用户之间建立安全的通道以保证用户私钥的安全.

目前已提出的安全私钥分发协议，可分为三大类：1）基于多信任机构的方式，如 Boneh 等[4]提出了门限共享私钥分发协议，该方案由 n 个对等的可信第三方 KGC 共享主密钥，用户的私钥以 t 门限的方式产生. Chen 等[5]提出了另一种基于多信任机方式即基于多密钥的用户私钥分发协议，该方案与 Boneh 等[4]方案不同的是 n 个 KGC 独立产生主密钥，且用户的私钥是这 n 个不同的主密钥和产生. 尽管以上 2 种方案解决了单个 KGC 的用户私钥托管问题，然而当用户申请私钥时，不仅需要向多个可信机构认证自己的身份，而且还需要与它们建立安全通道来确保私钥的安全传输；2）基于用户选择密文方式，如 Gentry[6]提出了一种基于证书即 CBE（certificate-based encryption）方案、Al-Riyami 等[7]又提出了一种基于公钥即 CLPKE（certificateless publice key encryption）方案，这 2 种方案不仅解决了用户私钥的私管问题而且用户私钥的传输不需要安全的通道，但是由于公钥无法直接从用户的身份标识中获取，因此这两种方案无法体现 IBE 的优势；3）基于盲技术方式，如 Lee 等[8]提出一种安全私钥分发协议，为解决私钥托管问题，该方案采用单个 KGC 为用户产生私钥且有多个 KPA 来保护用户私钥.

本文对 LeeB 协议进行了安全性分析并指出该协议是不安全的且不能解决 IBE 的私钥托管问题，针对该协议存在的安全漏洞提出一种改进方案.

1 LeeB 私钥分发协议

1.1 协议的实现

1.1.1 系统参数建立（KGC）

1）产生素数阶为 q 的 2 个群 $(G_1, +)$，$(G_2, \cdot)$ 以及双曲线映射 $e: G_1 \times G_1 \rightarrow G_2$；

2）随机产生主密钥 $s_0 \in Z_q^*$，相应的公钥 $P_0 = s_0 P$，其中 $P \in G_1$；

3）选择 2 个 hash 函数 H_1, H_2；

4）保密 s_0，公开 $\{G_1, G_2, e, P, H_1, H_2, P_0\}$；

收稿日期：2008-04-20.
基金项目：国家“九七三”基金资助项目（2007CB311100）；北京工业大学博士科研启动基金资助项目（52007016200704）；北京工业大学青年科学基金（X1007016200802）.
作者简介：侍伟敏（1978—），女，河南新乡人，讲师.

1.1.2 系统公钥产生

$KPA_i(i=1,2,3,\cdots,n)$随机产生主密钥 $s_i \in Z_q^*$，相应的公钥 $P_i = s_i P$. 若 $Y' = P_0$，且 $KPA_1, KPA_2, \cdots, KPA_n$ 依次计算 $Y_1' = s_1 P_0, Y_2' = s_2 Y_1', \cdots, Y_n' = s_n Y_{n-1}'$，最终获取系统公钥 $Y = s_0 s_1, \cdots, s_n P$.

1.1.3 用户私钥产生

1）身份标识为 ID 的用户 A 随机产生主密钥 $x \in Z_q^*$，计算 $X = xP$；

2）用户 A 发送$\{ID, X\}$给 KGC，KGC 需要做以下工作

① 检查用户 A 的身份；

② 计算用户 A 的公钥 $Q_{ID} = H_1(ID, ID_0, ID_1, ID_2, \cdots, ID_n)$，其中 $ID, ID_0, ID_1, ID_2, \cdots, ID_n$ 分别表示 A、KGC、KPA_1、$\cdots KPA_n$ 实体的身份标识；

③ 产生用户 A 的部分私钥 $Q_0' = H_2(e(s_0 X, P_0)) s_0 Q_{ID}$；

④ 签名 Q_0'，即 $Sig_0(Q_0') = s_0 Q_0'$ 并发送$\{Q_0', Sig_0(Q_0')\}$给用户 A；

3）用户 A 发送$\{ID, X, Q_{i-1}', Sig_{i-1}(Q_{i-1}')\}$给 $KPA_i(i=1,2,\cdots,n)$，KPA_i 验证 $e(Sig_{i-1}(Q_{i-1}'), P) = e(Q_{i-1}', P_{i-1})$，计算 $Q_i' = H_2(e(s_i X, P_i)) s_i Q_{i-1}'$ 和 $Sig_i(Q_i') = s_i Q_i'$，并发送$\{Q_i', Sig_i(Q_i')\}$给用户 A；

4）用户 A 计算自己的私钥

$$D_{ID} = \frac{Q_n'}{H_2(e(p_0, p_0)^x) \cdots H_2(e(P_n, P_n)^x)} = s_0 s_1 \cdots s_n Q_{ID}$$

用户可以通过验证 $e(D_{ID}, P) \stackrel{?}{=} e(Q_{ID}, Y)$来确认自己私钥的正确性.

1.2 协议的安全性

LeeB 私钥分发协议中的 KGC 负责验证用户的身份及产生部分私钥给用户. 用户发送$\{ID, X, Q_0', Sig_0(Q_0')\}$给 KPA_1，KPA_1 验证 $Sig_0(Q_0')$，若验证成功计算 Q_1'. 该过程存在一安全漏洞，即 KPA_1 通过$\{ID, X, Q_0', Sig_0(Q_0')\}$信息不能确认用户的身份：一方面 KPA_1 无法确认 Q_0' 的值是否由该用户 ID 生成；另一方面该协议没有提供其他机制来确认$\{ID, X, Q_0', Sig_0(Q_0')\}$是否由该用户所发. 如果 KCG 被攻击，恶意者便可利用此漏洞成功的获取用户的私钥，其攻击过程如下.

1）用户 A 发送$\{ID, X\}$给 KGC

2）恶意的 KGC 要想获取用户 A 的私钥，需要做以下工作

① 随机产生主密钥 $x^* \in Z_q^*$，计算 $X^* = x^* P$；

② 计算 $Q_{ID} = H_1(ID, ID_0, ID_1, ID_2, \cdots, ID_n)$；

③ 产生部分私钥 $Q_0' = H_2(e(s_0 X^*, P_0)) s_0 Q_{ID}$；

④ 计算签名值 $Sig_0(Q_0') = s_0 Q_0'$；

3）恶意的 KGC 发送$\{ID, X^*, Q_0', Sig_0(Q_0')\}$给 KAP_1，KAP_1 需要做以下工作

① 验证 $e(Sig_0(Q_0'), P) = e(Q_0', P_0)$；

② 计算 $Q_1' = H_2(e(s_1 X^*, P_1)) s_1 Q_0'$ 和 $Sig_1(Q_1') = s_1 Q_1'$；

③ 发送$\{Q_1', Sig_1(Q_1')\}$给用户 KGC；

4）依次类推恶意的 KGC 发送$\{ID, X^*, Q_{i-1}', Sig_{i-1}(Q_{i-1}')\}$给 $KPA_i(i=2,\cdots,n)$，最终得到 Q_n'，恶意的 KGC 计算用户 A 的私钥

$$D_{ID} = \frac{Q_n'}{H_2(e(p_0, p_0)^{x^*}) \cdots H_2(e(P_n, P_n)^{x^*})} = s_0 s_1 \cdots s_n Q_{ID}$$

由以上分析可知，LeeB 私钥分发协议没有真正解决 IBE 中用户私钥的托管问题.

2 LeeB 私钥分发协议的改进方案

2.1 改进方案的实现

2.1.1 系统公钥产生

1）系统产生主密钥 $s \in Z_q^*$，n 个 $KPA_i(i=1,2,\cdots,n)$共享 s，每个 KPA_i 都拥有自己的子密钥 $s_i(i=1,$

$2,\cdots,n)$，且相应的公钥为 $P_i = s_i P_0$；

2）KGC 计算系统公钥 $Y = \sum \lambda_i P_i$，其中 λ_i 是 Lagrange 系数.

2.1.2　用户身份密钥对产生

1）用户 A 随机选择身份密钥 $x \in Z_q^*$ 并计算 $Q_x = xQ_{ID}$，其中 $Q_{ID} = H(ID)$；

2）x 保密，公开身份密钥对 (Q_{ID}, Q_x).

2.1.3　用户私钥产生

1）用户 A 计算 $T_x = xP_0$，并发送 $\{T_x\}$ 给 KGC；

2）KGC 验证 $e(T_x, Q_{ID}) \stackrel{?}{=} e(P_0, Q_x)$，计算 $Q_0 = s_0 Q_x$，并发送 $\{Q_0\}$ 给用户 A；

3）用户 A 接收到信息 $\{Q_0\}$ 以后计算 $D_x = x^{-1}P$，发送信息 $\{D_x, Q_0\}$ 给 $\mathrm{KPA}_i (i = 1,2,\cdots,t)$；

4）$\mathrm{KPA}_i (i = 1,2,\cdots,t)$ 接收到信息 $\{D_x, Q_0\}$ 后验证 $e(D_x, Q_x) \stackrel{?}{=} (P, Q_{ID})$，和 $e(Q_0, P) \stackrel{?}{=} e(Q_x, P_0)$，计算 $Q_i = s_i Q_0$，并发送 $\{Q_i\}$ 给用户 A；

5）用户 A 计算自己的私钥 S_{ID}

① 计算 $S'_{ID} = \sum \lambda_i Q_i$，其中 λ_i 是 Lagrange 系数；

② 验证私钥的正确性通过 $e(S'_{ID}, P) \stackrel{?}{=} e(Q_x, Y)$；

③ 去盲获取得私钥 $S_{ID} = x^{-1} S'_{ID} = x^{-1} \sum \lambda_i s_i s_0 x Q_{ID} = \sum \lambda_i s_i s_0 Q_{ID}$.

2.2　进方案分析

2.2.1　安全性分析

在改进方案中，$\mathrm{KPA_s}$ 通过基于用户 A 身份密钥的短签名 D_x 值来确认其身份，其中短签名 D_x 的安全性是基于 G_1 的离散对数问题，恶意的 KGC 不能获取用户 A 的密钥 x 来伪造该用户的签名，由以下过程分析可知，即使 KGC 被攻击者控制，也无法获取用户 A 的私钥.

1）用户 A 发送 $\{T_x\}$ 给 KGC，恶意的 KGC 企图获取用户 A 的私钥，

① 计算 $Q_0 = s_0 Q_x$；

② 伪造用户 A 的身份密钥 $x^* \in Z_q^*$，计算 $D_q^* = x^{*\,-1} P$；

③ 发送 $\{D_x^*, Q_0\}$ 给 $\mathrm{KPA}_i (i = 1,2,\cdots,t)$；

2）$\mathrm{KPA}_i (i = 1,2,\cdots,t)$ 接收到 $\{D_x^*, Q_0\}$，验证 $e(Q_0, P) \stackrel{?}{=} e(Q_x, P_0)$ 成功，验证 $e(D_x^*, Q_x) \stackrel{?}{=} e(P, Q_{ID})$，即 $e(D_x^*, Q_x) = e(x^{*\,-1}P, xQ_{ID}) = e(P, Q_{ID})^{x^{*\,-1}x}$.

因 $x^* \neq x$，所以 $e(P, Q_{ID})^{x^{*\,-1}x} \neq e(P, Q_{ID})$ 即 $e(D_x^*, Q_x) \neq e(P, Q_{ID})$，$\mathrm{KPA}_i$ 确认信息 $\{D_x^*, Q_0\}$ 不是来自用户 A，因此恶意的 KGC 企图获取用户 A 的盲部分私钥 Q_i 失败. 另外，在用户 A 去盲获取得私钥 S_{ID} 的过程中，由于恶意的 KGC 不能获得其身份密钥 x，最终无法获取用户私钥 S_{ID}.

同样的，在 KGC 为用户 A 颁发部分私钥 Q_0 的过程，通过 $e(T_x, Q_{ID}) = e(P_0, Q_x)$ 来确认用户 A 的身份，其中 T_x 是基于用户 A 身份密钥的短签名，同以上分析过程一样，最终恶意的 $\mathrm{KPA_s}$ 也不获取用户的私钥. 因此，在改进方案中，只要 KGC 和 $\mathrm{KPA_s}$ 不同时受到攻击者控制，攻击者是无法获取用户的私钥，从而解决了 LeeB 方案中用户私钥托管问题.

2.2.2　效率分析

改进方案不仅解决了 LeeB 协议的私钥托管问题而且在效率上也有很大提高，一方面改进方案通过共享主密钥 s，为用户产生部分私钥信息. 而文献 LeeB 方案中需为 KGC 产生 n 对公私钥，额外增加了系统的负担. 另一方面，对比两种方案的运算量，改进方案的运算量明显较少，如表 1 所示. 改进方案与 LeeB 方案相比尽管增加了 $3n$ 次乘法运算，但

表 1　效率对比

Table 1　Efficiency comparison

运算	LeeB	改进方案
乘法	$7n+6$	$4t+5$
逆	n	2
哈希	$2n+3$	1
对	$6n+5$	$2(t+1)$

注：$t \leqslant n$

哈希和对运算分别减少了 $2n$ 次和 $4n$ 次运算量，而其中对运算最耗时，因此改进方案的实现效率明显提高.

3 结束语

对 LeeB 私钥分发协议进行了安全性分析，并针对该协议存在的安全问题提出一种改进方案. 在改进方案中，基于用户身份密钥解决了 LeeB 私钥分发协议中的用户私钥的托管问题，改进方案与 LeeB 方案相比，减少了 $4n$ 次对运算和 $2n$ 次哈希运算.

参考文献：

[1] SHAMIR A. Identity-based cryptosystem and signature schemes[C]// Advances in Cryptology 1984. Berlin: Springer-Verlag, 1984: 47-53.

[2] PATERSON K G. ID-based signatures from pairings on elliptic curves[J]. Electronics Letters, 2003, 38(18): 1025-1026.

[3] BONEH D, FRANKLI N M. Identity based encryption from weil pairing[C]// Advances in Cryptology 1984. Berlin: Springer-Verlag, 2001: 213-229.

[4] BONEH D, FRANKLI N M. Short signature from weil pairing[C]// Boyd C Asiacrypt 2001, Berlin: Springer-Verlag, 2001: 514-532.

[5] CHEN L, HARRISON K, SOLDERA D, et al. Applications of multiple trust authorities in pairing based cryptosystems[C]// Proc of Infrastructure Security Conference. Berlin: Springer-Verlag, 2002: 260-275.

[6] GENTRY C. Certificate-based encryption and the certificate revocation problem[C]// Advances in Cryptology- EUROCRYPT 2003. Berlin: Springer-Verlag, 2003: 272-293.

[7] AL-RIYAMI S, PATERSON K. Certificateless public key cryptography[C]// Advances in Cryptology- Asiacrypt´2003. Berlin: Springer-Verlag, 2003: 452-472.

[8] LEE B, BOYD E, DAESON E, et al. Secure key issuing in ID-based cryptography[C]// In Proceedings of the Second Australian Information Security Workshop-AISW 2004. New Zealand: Australian Computer Society, Inc, 2004: 69-74.

An Improved Sche me of LeeB Secure Key Issuing Protocol

SHI Wei-min

(College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China)

Abstract: To resolve user's key escrow problem of Lee B et al's protocol, this paper presents an improvement by an identity-password pair published for confirming user identity and analyzes its security and efficence. The improved scheme overcomes the disadvantages of LeeB et al. 's scheme and save at least $4n$ pairing and $2n$ Hash operations.

Key words: identity-based cryptography; key issuing protocol; key-escrow problem; Identity key pair

(责任编辑 张士瑛)