无双线性配对的无证书代理环签名方案*

张春生[1], 苏本跃[1], 姚绍文[2]
(1. 安庆师范学院 计算机与信息学院, 安徽 安庆 246133; 2. 云南大学 软件学院, 昆明 650091)

摘 要: 针对现有的代理环签名方案都是基于双线性对运算或指数运算且计算效率不高的问题,提出了一种无双线性对运算和指数运算的无证书代理环签名方案。该方案只需进行简单的椭圆曲线上的乘法运算,并基于计算 Diffie-Hellman 假设和离散对数困难问题证明了其安全性。通过对方案的复杂性分析,只需要进行 $2n+1$ 次的乘法运算(n 表示环成员的个数),证明系统是已知最有效的无证书代理环签名方案。

关键词: 环签名; 代理环签名; 计算 Diffie-Hellman 假设; 无双线性对运算; 无证书
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2013)12-3797-03
doi:10.3969/j.issn.1001-3695.2013.12.072

Certificateless proxy ring signature scheme without bilinear pairings

ZHANG Chun-sheng[1], SU Ben-yue[1], YAO Shao-wen[2]
(1. *School of Computer & Information, Anqing Normal University, Anqing Anhui* 246133, *China*; 2. *School of Software, Yunnan University, Kunming* 650091, *China*)

Abstract: The previous proxy ring signature schemes need pairings operation or exponent operation. For improving the efficient of operations, this paper proposed a new certificateless proxy ring signature scheme. The scheme only need a simple multiplication on elliptic curves, and proved its security under the computational Diffie-Hellman (CDH) assumption and the hardness of discrete logarithm problem (DLP). The results of complexity analysis show that it is the most efficient certificateless proxy ring signature scheme, it only needs $2n+1$ multiplication (n is the number of members of a ring).

Key words: ring signature; proxy ring signature; CDH (computational Diffie-Hellman) assumption; pairings-free operation; certificateless

0 引言

由于无证书公钥密码体制[1]既避免了基于身份密码系统[2]的私钥托管(key escrow)问题,又简化了传统公钥体制负担过重的证书管理问题,因此,已经成为密码学和信息安全领域研究的热点[3]。它是由第三方密钥生成中心 KGC(key generation center)生成用户的部分私钥和部分公钥,然后由用户选择一个秘密值与这个部分私钥共同生成用户的私钥。

代理环签名[4]既能实现代理人代替原始签名者进行签名,又能保护代理人匿名性的技术。2003 年,Zhang 等人[5]首次提出了一种通过双线性对构建的基于身份的代理环签名方案,但方案执行的效率很低。之后相继提出了一些代理环签名方案[6~8]。文献[6]给出了一种可证明安全的代理环签名方案,但被文献[7]证明是不安全的并进行了改进。文献[8]给出了一种新的无证书代理环签名方案。但这些方案均采用了双线性对运算或指数运算,都存在效率不高的问题。根据文献[9],执行一个 512 位 tate pairings 需要 20 ms,执行一个 1 024 位素数指数操作需要 8.80 ms,执行一次双线性对操作的时间至少是椭圆曲线上点乘运算的 20 倍以上[10]。因此,无双线性对运算和指数运算的方案具有更高的执行效率。

本文提出了一种基于无证书密码体制的代理环签名方案,它无须双线性对运算和指数运算,只需进行简单的椭圆曲线上的点乘运算,既极大地提高了效率,又能满足环签名的安全需求:可验证性、无条件匿名性、不可伪造性和可区分性。

1 相关知识

1.1 困难问题

1)计算性 Diffie-Hellman 问题(CDHP) G 为 q 阶的循环加法群,P 为 G 中 q 阶的生成元,对任意的 $a,b\in Z_q^*$,给定 aP, $bP\in G$,计算 abP。

2)离散对数问题(DLP) G 为 q 阶的循环加法群,P 为 G 中 q 阶的生成元,对任意的 $a\in Z_q^*$,给定 $P,aP\in G$,计算 a。

1.2 代理环签名的安全性需求

1)可验证性 任何人都可以验证签名的正确性。

2)无条件匿名性 原始签名人和其他第三方(包括 KGC)都不知道谁是真实的代理签名人。

3)不可伪造性 只有授权代理人才能生成有效的代理环签名。未经授权的任何人(包括原始签名人和 KGC)都不能伪造合法的代理环签名。

4)可区分性 代理环签名与代理人的一般环签名具有结构上的区别。

收稿日期: 2013-05-02; **修回日期**: 2013-06-31 **基金项目**: 安徽省高校省级自然科学基金资助项目(KJ2011B077)

作者简介:张春生(1968-),男,安徽六安人,讲师,硕士,主要研究方向为密码学、网络与信息安全(zhangchsh2000@126.com);苏本跃(1971-),男,教授,硕导,博士,主要研究方向为多媒体与可视媒体计算、数字图像与视频处理、机器人控制;姚绍文(1966-),男,湖南永顺人,教授,博导,主要研究方向为语义 Web 技术、网络协议工程、网络分布式计算.

1.3 无证书密码体制的两种攻击类型

参照文献[9],给出了两种类型无证书公钥密码系统的敌手:

a)攻击者可以查询用户公钥或替换合法用户的公钥,但不知道系统主密钥和用户的私钥。

b)攻击者可以获得系统主密钥,但不知道用户的私钥,也不能同时替换合法用户公钥。

定义 1 在两种类型敌手的攻击下,若攻击者能在多项式时间内,以不可忽略的概率输出一个关于消息 m 和环成员集合 L 的有效签名,则称攻击成功。

2 新的无证书代理环签名方案

2.1 方案描述

代理环签名有密钥生成中心 KGC、授权人 A(原始签名者)、代理人(真实签名者)和验证者四个参与方,一般包括系统创建、成员私钥的生成、代理密钥产生、签名生成和签名验证五个步骤。

1)系统参数建立(setup)

k 为输入安全参数,生成两个大素数 p、q,且 $q|p-1$。G 为循环加法群,P 为 G 中 q 阶的生成元,选择两个安全 hash 函数 $H_1:\{0,1\}^* \times G \rightarrow Z_q^*$,$H_2:\{0,1\}^* \rightarrow Z_q^*$,KGC 随机选择主密钥 $z \in Z_q^*$,计算 $P_0 = zP$,公开系统参数 (p,q,P,P_0,H_1,H_2),系统主密钥 z 保密。

2)环成员私钥的生成(keyGen)

a)环成员部分私钥生成。输入用户身份 ID_i,KGC 随机选择 $d_i \in Z_q^*$,计算 $Y_i = d_iP, Q_i = H_1(ID_i, Y_i), y_i = d_i + zQ_i$,$Y_i$ 为用户的部分公钥,y_i 为用户的部分私钥。将 y_i 通过安全渠道传给用户 ID_i,用户 ID_i 通过等式 $Y_i + H_1(ID_i, Y_i)P_0 = y_iP$ 是否成立来判断部分私钥是否有效。

b)环成员私钥生成。用户 ID_i 随机选择一个 $x_i \in Z_q^*$ 作为自己的秘密值,计算 $X_i = x_iP$,生成用户私钥 $SK_i = (x_i, y_i)$,公钥 $PK_i = (X_i, Y_i)$,并记 $Y_i' = X_i + Y_i + Q_iP_0 = (x_i + y_i)P$。假设授权人 A 的私钥 $SK_a = (x_a, y_a)$,公钥 $PK_a = (X_a, Y_a)$。

3)代理密钥生成(proxykeyGen)

a)授权人 A 生成一个授权信息 ω(ω 包括授权期限、消息集和代理成员集合等),计算 $h_\omega = H_2(\omega)(x_a + y_a)$,然后把 ω 和 h_ω 的值发送给代理成员集合。

b)代理成员集合中的每一个人验证 $H_2(\omega)Y_a' = h_\omega P$,如果不成立,则拒绝委托代理;否则代理签名人计算代理签名密钥 $SK_i' = h_\omega + H_2(\omega)(x_i + y_i)(i = 1,2,\cdots,n)$。

4)签名过程(proxy ring signing)

假设真正的代理签名人为 ID_s(其公钥为 $PK_s = (X_s, Y_s)$,私钥为 $SK_s = (x_s, y_s)$,代理签名密钥 $SK'_s = h_\omega + H_2(\omega)(x_s + y_s)$),包含代理签名人 ID_s 在内的 n 个代理签名人集合为 $L = \{ID_1, ID_2, \cdots, ID_n\}(1 \leqslant s \leqslant n)$。$ID_s$ 匿名地代表 L 计算签名的过程如下:

a)对待签名的消息 m,ID_s 随机选取不同的 $r_i \in Z_q^*$ $(i = 1, 2, \cdots, n; i \neq s)$,计算 $R_i = r_iP, h_i = H_2(m \| L \| R_i)$。

b)ID_s 随机选取 $r_s \in Z_q^*$,计算

$$R_s = r_sH_2(\omega)(Y_s' + Y_a') - \sum_{i=1,i\neq s}^{n} R_i + h_iH_2(\omega)Y_i'$$

$$h_s = H_2(m \| L \| R_s)$$

$$\sigma = (r_sSK_s' + h_sH_2(\omega)(x_s + y_s))P \quad (1)$$

则 ID_s 对消息 m 的签名为 $(m, L, R_1, R_2, \cdots, R_n, \sigma)$。

5)验证过程(verification)

验证者收到签名 $(m, L, R_1, R_2, \cdots, R_n, \sigma)$ 后,对 $i = 1, 2, \cdots, n$ 依次计算 $h_i = H_2(m \| L \| R_i)$,然后验证

$$\sigma = \sum_{i=1}^{n} h_iH_2(\omega)Y_i' + \sum_{i=1}^{n} R_i \quad (2)$$

如果式(2)成立,接受签名,否则拒绝。

2.2 方案分析

2.2.1 方案可验证性

定理 1 如果 $(m, L, R_1, R_2, \cdots, R_n, \sigma)$ 是对消息 m 的正确签名,则式(2)$\sigma = \sum_{i=1}^{n} h_iH_2(\omega)Y_i' + \sum_{i=1}^{n} R_i$ 一定成立。

证明 假设 $(m, L, R_1, R_2, \cdots, R_n, \sigma)$ 是对消息 m 的正确签名,由式(1)有

$$\sigma = (r_sSK_s' + h_sH_2(\omega)(x_s + y_s))P =$$

$$r_sSK_s'P + h_sH_2(\omega)(x_s + y_s)P + \sum_{i=1,i\neq s}^{n} R_i +$$

$$h_iH_2(\omega)Y_i' - \sum_{i=1,i\neq s}^{n} R_i + h_iH_2(\omega)Y_i' =$$

$$r_sH_2(\omega)(x_a + y_a + x_s + y_s)P -$$

$$\sum_{i=1,i\neq s}^{n} R_i + h_iH_2(\omega)Y_i' + h_sH_2(\omega)(x_s + y_s)P +$$

$$\sum_{i=1,i\neq s}^{n} R_i + h_iH_2(\omega)Y_i' =$$

$$r_sH_2(\omega)(Y_a' + Y_s') - \sum_{i=1,i\neq s}^{n} R_i +$$

$$h_iH_2(\omega)Y_i' + h_sH_2(\omega)Y_s' +$$

$$\sum_{i=1,i\neq s}^{n} h_iH_2(\omega)Y_i' + \sum_{i=1,i\neq s}^{n} R_i =$$

$$R_s + \sum_{i=1}^{n} h_iH_2(\omega)Y_i' + \sum_{i=1,i\neq s}^{n} R_i = \sum_{i=1}^{n} h_iH_2(\omega)Y_i' + \sum_{i=1}^{n} R_i$$

由上可见,如果 $(m, L, R_1, R_2, \cdots, R_n, \sigma)$ 是对消息 m 的正确签名,则验证式(2)一定成立。

2.2.2 方案的无条件匿名性

定理 2 方案是无条件匿名的,攻击者能正确猜出真实代理签名者的概率不大于 $\frac{1}{n}$。

证明 因为在签名过程中,$r_i \in Z_q^*$ $(i = 1, 2, \cdots, n; i \neq s)$ 是 ID_s 随机选取的,则计算 R_i 的概率为 $\frac{1}{q-1} \times \frac{1}{q-2} \times \cdots \times \frac{1}{q-n+1}$。另外,$r_s$ 也是随机选取的,计算 R_s 的概率为 $\frac{1}{q-n}$。因此,计算 R_i $(i = 1, 2, \cdots, n)$ 的概率为 $\frac{1}{q-1} \times \frac{1}{q-2} \times \cdots \times \frac{1}{q-n+1} \times \frac{1}{q-n}$。该值与签名者无关,因此,即使攻击者得到了所有签名者的私钥,他能正确猜出真实签名人的概率不超过 $\frac{1}{n}$,方案满足无条件匿名性。

2.2.3 不可伪造性

定理 3 提出的方案满足不可伪造性。

证明

a)授权人 A 的私钥 $SK_a = (x_a, y_a)$ 是安全的,因为任何攻击者想从签名 h_ω 中求解出授权人 A 的私钥,就必须要解决 G 上的离散对数难题。

b)代理密钥 $SK_i' = h_\omega + H_2(\omega)(x_i + y_i)$ 是安全的,因为代理签名密钥 SK_i' 是授权人 A 与代理签名人两者的签名之和,任何攻击者想求解出 SK_i',也必须要解决 G 上的离散对数

难题。

c)任何人(包括授权人 A 和 KGC)不能伪造一个不包括自己的环签名。因为由式(1)可知,σ 是代理密钥 SK_i' 的签名与代理人的私钥 $SK_i=(x_i,y_i)$ 签名之和,任何人(包括授权人 A 和 KGC)都无法通过 σ 解出代理密钥 SK_i' 和代理人的私钥 SK_i,除非他能解决离散对数难题。因此,攻击者所伪造的环签名不可能通过验证式(2)。所以,任何人(包括授权人 A 和 KGC)不能伪造一个不包括自己的环签名。

因此,本文提出的方案满足不可伪造性。

2.2.4　可区分性

定理 4　提出的方案满足可区分性。

证明　可区分性。因代理签名密钥 SK_i' 与代理签名人的私钥 SK_i 不同,代理环签名与代理人的一般环签名具有结构上的区别,所以提出的方案满足可区分性。

2.3　效率分析

由于系统建立、用户密钥生成的时间开销不大,而且可以通过预处理来完成,所以本方案的效率分析主要考虑签名和验证两个阶段。用 P_g 表示双线性对运算,M_u 表示在循环加法群 G 上的乘法运算,则本文方案与文献[6,7]的比较如表 1 所示。假设进行比较的方案的环成员数量都是 n。

表 1　本文方案与文献[6,7]的比较

方案	M_u	P_g
罗大文等人[6]	$4n$	2
张小萍等人[7]	$3n+2$	2
本文方案	$2n+1$	0

由表 1 可得,文献[6]需要进行 $4n$ 次乘法和 2 次双线性对运算,文献[7]需要进行 $3n+2$ 次乘法和 2 次双线性对运算,而本文方案无须对运算和指数运算,仅需要 $2n+1$ 次乘法运算,是目前已知方案中效率最高的。

3　结束语

本文基于无证书密码体制提出了一种高效的代理环签名方案。该方案无双线性对运算和指数运算,只需进行 $2n+1$ 次乘法运算,既极大地提高了效率,又能满足环签名的安全需求。如何设计标准模型下无双线性对运算和指数运算的无证书代理环签名方案,是值得进一步研究的课题。

参考文献:

[1] Al-RIYAMI S S, PATERSON K G. Certificateless public key cryptography [C]//Advance in Cryptology. Berlin: Springer-Verlag, 2003: 452-473.

[2] SHAMIR A. Identity-Based cryptosystems and signature schemes [C]//Proc of Cryptology-Crypto'84. New York: Springer-Verlag, 1984:47-53.

[3] 张福泰,孙银霞,张磊,等. 无证书公钥密码体制研究[J]. 软件学报,2011,22(6):1316-1332.

[4] 余婷,赵泽茂,任锡洋. 标准模型下基于身份的高效环签名[J]. 计算机应用,2012,32(7):2015-2017,2026.

[5] ZHANG Fang-guo, SAFAVI-NAINI R, LIN C Y. New proxy signature, proxy blind signature and proxy ring signature schemes from blinear pairings[EB/OL]. (2003-05-20)[2013-04-20]. http://eprint.iacr.org/2003/.

[6] 罗大文,何明星,李琥. 一种新的可证明安全的代理环签名方案[J]. 计算机工程与应用,2009,45(7):100-102.

[7] 张小萍,钟诚. 改进的代理环签名方案[J]. 计算机应用研究,2011,28(9):3505-3507.

[8] 张俊茸,任平安,李文莉. 一种新的无证书的代理环签名方案[J]. 计算机工程与应用,2012,48(2):63-65.

[9] 刘文浩,许春香. 无双线性配对的无证书签密方案[J]. 软件学报,2011,22(8):1918-1926.

[10] CHEN L, CHENG Z, SMART N P. Identity-based key agreement protocols from pairings[J]. International Journal of Information Security, 2007, 6(4): 213-241.

(上接第 3796 页)

4　结束语

本文构造了一种双线性对上的可公开验证可更新多秘密共享方案,给出了秘密份额的动态更新过程,基于椭圆曲线上的离散对数问题的难解性和双线性对的性质,任何人都可以对秘密份额和更新份额的有效性进行验证。与传统的秘密共享方案相比,该方案有以下优点:a)秘密份额 $s_i^{(0)}$ 由参与者自己选取,避免了分发者对参与者的欺骗;b)秘密份额 $s_i^{(0)}$ 可以被重复使用,当变更共享秘密时,无须重新选择;c)参与者与分发者之间不需要维护安全信道,降低了系统代价;d)方案具有可公开验证性,能有效地防止内外部攻击;e)秘密份额可定期更新,并且一次秘密共享过程可以共享多个秘密。本方案虽然在运行效率上没有太大优势,但在一定程度上提高了系统的安全性和实用价值,为今后研究更高效的可公开验证可更新多秘密共享方案奠定了基础。

参考文献:

[1] SHAMIR A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613.

[2] BLAKLEY G R. Safeguarding cryptographic keys[C]//Proc of AFIPS 1979 National Computer Conference. 1979: 313-317.

[3] CHOR B, GOLDWASSER S, MICALI S, *et al*. Verifiable secret sharing and achieving simultaneity in the presence of faults[C]//Proc of the 26th IEEE Symposium on the Foundations of Computer Science. [S.l.]: IEEE Press, 1985: 383-395.

[4] STADLER M. Publicly verifiable secret sharing[C]//Advances in Cryptology, Eurocryptp'96. Berlin: Springer-Verlag, 1996: 190-199.

[5] 张建中,张艳丽. 一个双线性对上公开可验证多秘密共享方案[J]. 计算机工程与应用,2011,47(25):82-84.

[6] 肖艳萍,杜伟章. 基于双线性对的可验证可更新的秘密分享方案[J]. 计算机应用研究,2011,28(9):3519-3521.

[7] WU T Y, TSENG Y M. A pairing-based publicly verifiable secret sharing scheme[J]. Journal of Systems Science and Complexity, 2011, 24(1): 186-194.

[8] 田有亮,马建峰,彭长根,等. 椭圆曲线上的信息论安全的可验证秘密共享方案[J]. 通信学报,2011,32(12):96-102.

[9] 秦华旺,朱晓华,戴跃伟. 访问结构上的动态先应式秘密共享方案[J]. 电子科技大学学报,2012,41(6):927-931.

[10] 李婧,李志慧,赖红. 基于 hash 函数的无分发者的多秘密共享方案[J]. 计算机工程与应用,2012,48(18):64-65,131.

[11] MIAO Fu-you, DU Xian-chang, RUAN Wen-jing, *et al*. A strong PVSS scheme[C]//Lecture Notes in Electrical Engineering, vol 131. New York: Springer-Verlag, 2013: 521-528.

[12] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//Advances in Cryptology, CRYPTO 2001. Berlin: Springer-Verlag, 2001: 213-229.