

一个具有强匿名性和选择关联性的环签名框架

李德荣

(大庆师范学院 计算机科学与技术系, 黑龙江 大庆 163712)

摘 要: 提出了一个具有强匿名性和可选择关联性的环签名框架. 环签名框架采用随机数作为可关联标签, 即使在获得私钥和公开信息的情况下, 随机数作为可关联标签都具有不可重构性. 分析了方案的匿名性, 可选择关联性.

关键词: 环签名; 匿名性; 选择关联性

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2010)01-0138-03

A Ring Signature Scheme with Strong Anonymity and Selectively Linkable

LI De-rong

(Department of Computer Science and Information Technology, Daqing Normal University, Daqing 163712, China)

Abstract: Constructed a ring signature scheme providing strong anonymity and selectively linkability. The basic idea of our scheme is to make a link tag of a ring signature using random numbers such that the link tag is not reconstructible with a private key and the public information. Analyzed the anonymity and selectively linkability of our scheme.

Key words: ring signature; anonymity; selectively linkability

1 引言

环签名可以被视为一种特殊的群签名, 环签名因为其签名隐含的某个参数按照一定的规则组成环状而得名. 环签名在管理, 军事, 政治及经济等多个方面有着广泛的应用.

关联环签名是具有签名人关联性的环签名. 签名人关联性是指通过关联环签名可以确定某两个签名是否由某用户代表同一群体签署产生. 2004 年, Joseph K. Liu 等^[1]首次提出了关联环签名的概念, 并指出关联环签名是满足自发性、匿名性和关联性的一种环签名. 他们给出了第一个关联环签名方案 - LSAG, 并用改造后的分叉引理证明了方案的安全性, 同时, 基于该方案构造了不需注册的电子投票系统. Liu 等人指出, 他们的可关联环签名框架不具有强匿名性, 设计一个具有强匿名性的可关联环签名是一个待解决的问题. 在此之后, 参照文献^[1], 有许多可关联的环签名框架被提出^[2-6], 然而, 这些可

关联的环签名框架都提供了弱匿名性和强可关联性.

文中提出了一个具有强匿名性和可选择关联性的环签名框架.

2 环签名基本概念

2.1 环签名的定义

定义 1 假定有 n 个用户, 每一个用户 u_i 拥有一个公钥 y_i 和与之对应的私钥 x_i . 环签名是一个能够实现签名者无条件匿名的签名方案, 它主要由下述算法组成:

(1) 生成 Gen. 一个概率多项式时间(PPT)算法, 输入为安全参数 k , 输出为公钥和私钥. 这里假定 Gen 为每一个用户 u_i , 产生一个公钥 y_i 和私钥 x_i , 并且不同用户的公私钥可能来自不同的公钥体制, 如有的来自 RSA, 有的来自 DL.

(2) 签名 Sign. 一个 PPT 算法, 在输入消息 m 和 n 个环成员的公钥 $L = \{y_1, \dots, y_n\}$ 以及其中一个

成员的私钥 x_s 后,对消息 m 产生一个签名 R ,其中 R 中的某个参数根据一定的规则呈环状.

(3) 验证 Verify. 一个确定性算法,在输入 (m, R) 后,若 R 为 m 的环签名则输出“True”,否则为“False”.

2.2 环签名的安全性要求与特性

一个好的环签名必须满足以下的安全性要求:

(1) 无条件匿名性. 攻击者即使非法获取了所有可能签名者的私钥,他能确定出真正的签名者的概率不超过 $1/n$, 这里 n 为环成员(可能签名者)的个数.

(2) 不可伪造性. 外部攻击者在不知道任何成员私钥的情况下,即使能够从一个产生环签名的随机预言者那里得到任何消息 m 的签名,他成功伪造一个合法签名的概率也是可以忽略的.

(3) 环签名具有良好的特性. 可以实现签名者的无条件匿名;签名者可以自由指定自己的匿名范围;构成优美的环形逻辑结构;可以实现群签名的主要功能但无需可信第三方或群管理员等.

3 强匿名性和可选择关联的环签名方案

3.1 既具有强匿名性又具有强可关联性的环签名方案不存在

定理 在一个环签名框架中,不可能既具有强匿名性又具有强可关联性.

证明: 如果一个环签名 δ 既具有强匿名性又具有强可关联性,假设攻击者 A 想破坏强匿名性,攻击者 A 获得了所有私钥,想找到环签名 δ 的实际签名者.

设 $(P_1, P_2, \dots, P_n)$ 是环签名 δ 的所有成员, A 任选一个成员 $P_i (1 \leq i \leq n)$ 的私钥产生一个环签名 τ_i , 由于环签名具有强可关联性,攻击者 A 可以判断 τ_i 和 δ 是否具有关联性,从而可以判断出 P_i 是否是实际的签名者. 因此,如果环签名框架提供了强可关联性,就一定不具有强匿名性.

3.2 强匿名性和可选择关联的环签名框架

为了设计一种具有强匿名性和可选择关联的环签名框架,文中提出可选择关联性的含义:

(1) 一个环中,签名者既可以产生可关联的环签名,也可以产生不可关联的环签名;

(2) 签名者可以选择产生不可联接的环签名,但是,以后签名者在需要时还可以将签名转换成可联接的环签名.

参考文献[2-6]中的环签名框架都是按照文献

[1] 的模式构造的. 文献[1]中的环签名含有一个关联标签 $\tilde{y} = H_2(L)^{x_\pi}$, L 是环中的公钥列表, H_2 是一个 hash 函数, x_π 是签名者的私钥. 如果签名者私钥和公共信息被公开,则关联标签 $\tilde{y}$ 是可以被重构的. 参考文献[2-6]的环签名框架中都有这样的关联标签,因此文献[1-6]中的环签名都具有强可关联性和弱匿名性.

文中提出的环签名框架采用随机数作为可关联标签. 即使在获得私钥和公开信息的情况下,随机数作为可关联标签都具有不可重构性.

设 $G = \langle g \rangle$ 是一个基于离散对数的循环群, 群阶 q 是素数, $H: \{0, 1\}^* \rightarrow Z_q$ 是 hash 函数, 每个成员 P_i 的私钥、公钥对为: $(x_i, y_i = g^{x_i})$.

环签名过程如下: 设环 $R = \{P_1, \dots, P_n\}$, $P_\pi (P_\pi \in R)$ 准备代表环对消息 m 进行签名, 以下过程将产生一个可关联的环签名:

(1) 随机选取 $D_0, a (D_0 \in {}_R G, a \in {}_R Z_q)$, 计算 $D_1 = D_0^a$;

(2) 随机选取 $u, v (u \in {}_R Z_q, v \in {}_R Z_q)$, 计算 $R_\pi = g^u, R_A = D_0^v$;

(3) 选取 $c_i, s_i (c_i \in {}_R Z_q, s_i \in {}_R Z_q)$, 计算 $R_i = g^{c_i} y_i^{s_i} (1 \leq i \leq n, i \neq \pi)$;

(4) 计算 $c = H(D_0, D_1, m, R_1, \dots, R_n, R_A)$;

(5) 计算 c_π , 使得 c_π 满足

$$c = c_1 + \dots + c_\pi + \dots + c_n \bmod q,$$

$$s_\pi = u - x_\pi c_\pi \bmod q, s_A = v - ac \bmod q;$$

环签名

$$\delta(m) = (D_0, D_1, c_1, \dots, c_n, s_1, \dots, s_n, s_A).$$

环签名的验证:

$$c = H(D_0, D_1, m, g^{c_1} y_1^{s_1}, \dots, g^{c_n} y_n^{s_n}, D_0^a D_1^a),$$

如果验证成功,则认可该签名;否则,拒绝接受该签名.

可选择联接的环签名框架: 利用文中的环签名框架,签名者可以选择产生不可联接的环签名. 但是,以后签名者在需要时还可以将签名转换成可联接的环签名.

设: 签名者 P_π 用参数 (D_0, a) 和 (D'_0, a) 产生了两个环签名:

$$\delta(m) = (D_0, D_1, c_1, \dots, c_n, s_1, \dots, s_n, s_A)$$

$$\delta'(m) = (D'_0, D'_1, c'_1, \dots, c'_n, s'_1, \dots, s'_n, s'_A)$$

验证者不能确定 $\delta(m)$ 和 $\delta'(m)$ 是同一个人产生的环签名, 因为联接标签 $(D_0, D_1 = D_0^a)$ 和

$(D'_0, D'_1 = D'_0)$ 是不同的. 但是, 以后签名者在需要时还可以证明签名 $\delta(m)$ 和 $\delta'(m)$ 是同一个人产生的环签名, 因为只有签名者本人能够证明这两个签名的参数 a 是相同的.

4 安全性分析

(1) 强匿名性

即使攻击者知道了环成员的所有私钥和随机数 $a = \log_{D_0} D_1$, 攻击者也不能判断出签名者的身份. 因为, 对于消息 m 的环签名 $\delta(m) = (D_0, D_1, c_1, \dots, c_n, s_1, \dots, s_n, s_A)$, 对于 $1 \leq i \leq n$, 都有 $s_i = \log_g R_i - x_i c_i \bmod q$, 所以, 攻击者不能判断出谁是真正的签名者.

(2) 可选择联接性

签名者既可以产生可关联的环签名, 也可以产生不可关联的环签名: 如果签名者 P_π 用相同的参数 (D_0, a) 产生了两个环签名, 则联接标签 (D_0, D_1) 在这两个签名中是相同的, 因此, 这两个环签名是可联接的; 如果两个环签名中, 签名者 P_π 用不相同的参数 (D_0, a) 和 (D'_0, a') , 则, 联接标签 $(D_0, D_1 = D'_0)$ 和 $(D'_0, D'_1 = D'_0)$ 是不同的, 因此, 这两个环签名是不可联接的.

签名者可以选择产生不可联接的环签名, 以后签名者在需要时还可以将签名转换成可联接的环签名: 签名者 P_π 用参数 (D_0, a) 和 (D'_0, a') 产生了两个环签名, 因为联接标签 $(D_0, D_1 = D'_0)$ 和 $(D'_0, D'_1 = D'_0)$ 是不同的, 因此验证者不能确定 $\delta(m)$ 和 $\delta'(m)$ 是同一个人产生的环签名. 但是, 以后签名者在需要时还可以证明签名 $\delta(m)$ 和 $\delta'(m)$ 是同一个人产生的环签名, 因为只有签名者本人能够证明这两个签名的参数 a 是相同的.

5 结束语

文中提出的环签名框架采用随机数作为可关联标签, 设计了一种具有强匿名性和可选择关联的环签名框架, 并对环签名框架进行了强匿名性和可选择联接性分析.

参考文献:

- [1] Liu J K, Wei V K, Wong D S. Linkable spontaneous anonymous group signature for ad hoc groups[C]//Proc ACISP'04. Berlin: Springer-Verlag, 2004: 325-335.
- [2] Mh A U, Chow S S M, Susilo W. Short linkable ring signatures revisited[C]//EuroPKI 2006. Berlin: Springer-Verlag, 2006: 101-115.
- [3] Tsang P P, Wei V K. Short linkable ring signatures for E-voting, E cash and attestation[C]//Proc. First Information Security Practice and Experience Conf. (ISPEC'05). Berlin: Springer-Verlag, 2002: 48-60.
- [4] Au M H, Liu J K, Susilo W, et al. Constant-size ID-based linkable and revocable - iff - linked ring signature [C]//Proc. Int'l Conf. Cryptology in (INDOCRYPT'06). India, 2006: 364-378.
- [5] Liu J K, Wong D S. Enhanced security models and a generic construction approach for linkable ring signature [J]. Foundations of Computer Science, 2006, 17(6): 1403-1422.
- [6] Zheng D, Wei V K, Chen K F. GDH group-based signature scheme with linkability [J]. IEE Proc. Comm., 2006, 153(5): 639-644.

作者简介:

李德荣 女, (1964-), 硕士, 副教授. 研究方向为通信与信息安全.

(上接第 137 页)

- [2] 胡蓓, 李俊, 郁伟, 等. 对未知攻击进行检测的蜜罐系统的实现[J]. 计算机应用, 2006, 26(10): 2336-2337.
- [3] 王丹, 蔡皖东, 蔡俊朝. 分布式网络行为审计系统设计与实现[J]. 微电子学与计算机, 2008, 25(5): 80-83.
- [4] Moran D B. Tapping and tracking hackers [EB/OL]. (2000-07-15) [2008-09-10]. www.recourse.com.
- [5] 李平均, 刘权, 李天. 基于主被动结合的网络入侵检测系统的设计与实现[J]. 微电子学与计算机, 2007, 24(7): 50-52.

- [6] 连红, 连立祥. 虚拟蜜罐系统的设计[J]. 兵工自动化, 2007, 26(1): 54-55.
- [7] 林果园, 黄皓. 入侵检测动态取证模型[J]. 计算机工程与应用, 2006, 42(27): 140-143.

作者简介:

鄢喜爱 男, (1972-), 硕士, 副教授. 研究方向为信息安全.
杨金民 男, (1967-), 博士, 副教授. 研究方向为系统容错.
常卫东 男, (1967-), 硕士, 副教授. 研究方向为信息安全.