第35卷 第15期 计 算 机 工 程 2009年8月
Vol.35 No.15 Computer Engineering August 2009
·安全技术· 文章编号：1000—3428(2009)15—0135—03 文献标识码：A 中图分类号：TN918.4

无证书的可验证环签名方案

罗大文[1,2]，何明星[1]，李 旎[1,2]
(1. 西华大学数学与计算机学院，成都 610039；2. 西南交通大学信息编码与传输四川省重点实验室，成都 610031)

摘 要：将无证书的密码体制与可验证环签名相结合，提出一个无证书的可验证环签名方案。方案具有环签名的性质，在需要时，真实签名者还可向验证者证明自己的身份。方案基于无证书的密码体制，克服了基于身份的密码体制的密钥托管问题，避免基于证书密码体制的公钥存储和管理问题。

关键词：环签名；无证书的密码体制；可验证的环签名；计算性 Diffie-Hellman 问题

Certificateless Verifiable Ring Signature Scheme

LUO Da-wen[1,2], HE Ming-xing[1], LI Xiao[1,2]
(1. School of Mathematics and Computer Engineering, Xihua University, Chengdu 610039;
2. Key Laboratory of Information Coding and Transmission, Sichuan Province, Southwest Jiaotong University, Chengdu 610031)

【Abstract】This paper proposes a certificateless verifiable ring signature scheme. It is based on the concepts of certificateless cryptosystem and verifiable ring signature scheme. The scheme has the properties of ring signature scheme, if necessary, the actual signer can prove to the verifier that he(she) actually signed the signature. The scheme is based on certificateless cryptosystem, so it can overcome the key escrow of ID-based cryptosystem, and avoid the public key management and storage of certificate-based cryptosystem.

【Key words】ring signature; certificateless cryptosystem; verifiable ring signature; Computational Diffie-Hellman Problem(CDHP)

1 概述

环签名[1]是一种简化的类群签名，与群签名不同，它没有群管理员，签名用户没有组织结构程序，无须协调一致。任何用户(真实签名者)都可以使用自己的私钥和环成员(包括真实签名者在内的可能的签名者)的公钥签名而无须其他成员同意，环签名保护签名者的匿名性，它使验证者可以确信签名来自一个环，但不知道谁是真正的签名者，它是一种很好的以匿名方式透露可靠消息的技术。

但在某些时候，真实签名者希望验证者知道自己的身份。如政府根据签名者提供的匿名信息破获了一起贪污大案，于是决定给提供信息的人一笔丰厚的奖金。为了得到这笔奖金，真实签名者就需要证实自己的身份。为了解决这类问题，文献[2]给出基于双离散对数的可验证的环签名方案。通过可验证的环签名方案，在需要时，只要真实签名者向验证者提供一些秘密信息，就可以使验证者确定真实签名者的身份。文献[3]提出基于身份的密码体制，由于根据每一个人的姓名、E-mail 地址等就可以方便地计算其公钥，用户不再需要公钥证书，与传统的基于 PKI 的密码体制相比更安全有效。文献[4]把基于身份的密码体制与环签名相结合，提出基于身份的环签名方案。它虽然有许多优点，但却存在密钥托管问题。为了解决该问题，文献[5]提出无证书的密码体制。在这种体制下，拥有主密钥的可信机构只给用户提供与其身份相对应的部分私钥，而用户的私钥是由自己选的秘密信息和可信机构提供的部分私钥构成，用户的公钥不再根据自己的身份来计算，而是用户利用公开参数和秘密信息来产生，这样就解决了基于身份的密码体制的密钥托管问题和基于证书密码体制的公钥存储和管理问题。文献[6]把环签密和无证书的密码体制相结合，给出一个可验证的无证书的环签密方案。文献[7]给出有关环签名的分叉引理，用于证明环签名的安全性。本文在文献[2,5]的基础上，给出一个无证书的可验证的环签名方案。

2 数学知识及环签名分叉引理

2.1 双线性对的性质

设 G_1 是由它的一个生成元 P 生成的加法群，阶为素数 q，G_2 是阶为 q 的乘法群，双线性对是一个映射 $e: G_1\times G_1\to G_2$，它满足如下性质：

(1)双线性性：设 $P,Q\in G_1$，则有 $e(aP,bQ)=e(P,Q)^{ab}$，其中，$a,b\in z_q$。

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

(3)可计算性：存在有效的算法计算 $e(P,Q)$，其中，$P,\ Q\in G_1$。

2.2 几个计算困难性问题

(1)离散对数问题(DLP)：已知 $P,\ Q\in G_1$ 寻找 $n\in z_q^*$，使 $Q=nP$。

(2)计算性 Diffie-Hellman 问题(CDHP)：设 $P\in G_1$，$a,b\in z_q^*$，已知 P, aP, bP，计算 abP。

基金项目：国家自然科学基金资助项目(60773035)；西南交通大学信息编码与传输四川省重点实验室开放研究基金资助项目(08226138)；西华大学人才培养基金资助项目(R0722612)
作者简介：罗大文(1972－)，男，讲师、硕士，主研方向：信息安全；何明星，教授、博士；李 旎，副教授、硕士
收稿日期：2009-02-27 **E-mail：**huling_1976@126.com

(3)双线性对 Diffie-Hellman 问题(BDHP)：设 $P \in G_1$，$a,b,c \in z_q^*$，已知 P, aP, bP, cP，计算 $e(P,P)^{abc}$。

本文假定 CDHP, DLP, BDHP 是计算困难的，即在多项式时间内计算出它们的概率可以忽略不计。

2.3 环签名分叉引理

在方案的安全性证明中用到了一般环签名的定义和环签名分叉引理[7]。

(1)一般的环签名(generic ring signature)：一个一般的环签名产生一个元组 $(m, R_1, R_2, \cdots, R_n, h_1, h_2, \cdots, h_n, \sigma)$，$m$ 是签名消息，n 是环成员的个数，$R_1, R_2, \cdots, R_n$ 是从一个大的集合 G 中随机选出的两两不同的元素，h_i 是 $(m, L, R_i)(i = 1, 2, \cdots, n)$ 的哈希值，L 是环成员集合，σ 的值由 $R_1, R_2, \cdots, R_n, h_1, h_2, \cdots, h_n$ 和 m 确定。

(2)环签名分叉引理：设 $\sum_{Ring}$ 是一个安全参数为 k 的一般的环签名，n 是环成员的个数，伪造者 A 是一个概率多项式时间的图灵机，它的输入只包含公共参数和向随机预言机的 Q 次询问的回答且 $Q \geqslant n$。本文用 $V_{Q,n}$ 表示从 Q 个元素中选出 n 个的排列数，则有 $V_{Q,n} = Q(Q-1)\cdots(Q-n+1)$。假设 A 在时间 T 内能以概率 $\varepsilon \geqslant \frac{7V_{Q,n}}{2^k}$ 产生一个有效的环签名 $(m, R_1, R_2, \cdots, R_n, h_1, h_2, \cdots, h_n, \sigma)$，那么通过对 A 的 *Hash* 重放在时间 $T' \leqslant \frac{16V_{Q,n}T}{\varepsilon}$ 内就能以概率 $\varepsilon' \geqslant \frac{1}{9}$ 产生 2 个有效的环签名 $(m, R_1, R_2, \cdots, R_n, h_1, h_2, \cdots, h_n, \sigma)$ 和 $(m, R_1, R_2, \cdots, R_n, h_1', h_2', \cdots, h_n', \sigma')$，其中，$h_i = h_i', i \in \{1, 2, \cdots, n\} \setminus \{j\}$，而 $h_j \neq h_j'$。

3 方案的一般模型及安全性要求

3.1 无证书的可验证环签名方案的一般模型

无证书的可验证环签名方案(CL-VRS)是由一组多项式时间算法(CL-VRSGen, CL-VRSEet-Par-Key, CL-VRSSet-Sec-Val, CL-VRSSet-Pri-Key, CL-VRSSet-Pub-Key, CL-VRS Sign, CL-VRSVer, CL-VRSIdVer)组成的算法组，其一般模型如下：

(1)参数生成算法(CL-VRSGen)：输入安全参数 $1^\lambda (\lambda \in N)$，输出系统主密钥 *msk* 和包括系统公钥 *mpk* 在内的参数 *para*、可信中心保密 *msk*、公开 *para*。此算法由可信中心完成。

(2)部分私钥提取算法(CL-VRSEet-Par-Key)：输入系统主密钥 *msk*、系统公钥 *mpk* 及用户的身份 $ID \in \{0,1\}^*$，可信中心输出用户的部分私钥 d_{ID} 并通过安全信道把 d_{ID} 传给相应的身份为 *ID* 的用户。此算法由可信中心完成。

(3)秘密值生成算法(CL-VRSSet-Sec-Val)：输入系统公钥 *mpk* 和用户的部分私钥 d_{ID}，用户输出 1 个秘密值 x_{ID}。此算法由用户完成。

(4)密钥生成算法(CL-VRSSet-Pri-Key)：输入系统公钥 *mpk*、用户的部分私钥 d_{ID} 及用户的秘密值 x_{ID}，输出用户的全部秘钥 sk_{ID}。此算法由用户完成。

(5)公钥生成算法(CL-VRSSet-Pub-Key)：输入系统公钥 *mpk* 和用户的秘密值 x_{ID}，输出用户的公钥 pk_{ID}。此算法由用户完成。

(6)无证书的可验证的环签名的生成算法(CL-VRSSign)：输入系统参数 *para*，环成员身份集合 L 及其对应的公钥集合 L_1，秘钥 sk_{ID}，消息 $m \in \{0,1\}^*$，输出对消息的无证书的可验证的环签名 (m, σ)。此算法由用户完成。

(7)无证书的可验证的环签名的验证算法(CL-VRSVer)：输入公钥集合 L_1 和对消息 m 的无证书的可验证的环签名 (m, σ)，若是 1 个合法的签名，则输出“1”，否则输出“0”。此算法由验证者完成。

(8)真实签名者身份验证算法(CL-VRSIdVer)：输入真实签名者泄露的秘密信息，输出真实签名者的身份。此算法由验证者完成。

3.2 无证书的可验证环签名方案的安全特性

无证书的可验证的环签名方案一般具有以下安全特性：

(1)正确性(correctness)：如果是按照正确的签名步骤得到对消息 m 的签名 σ，并且签名 σ 在传播的过程中也没有被篡改，那么签名就应该满足签名验证等式。

(2)签名者的匿名性(signer-ambiguity)：环成员之外的人猜出谁是真正的签名者的概率不会超过 $1/n$(n 是环成员的个数)，环成员之内除真实签名者外的人猜出谁是真正的签名者的概率不会超过 $1/(n-1)$。

(3)不可伪造性(unforgeability)：1 个环成员才可产生 1 个合法的无证书的可验证的环签名方案，任何攻击者想伪造一个合法的无证书的可验证环签名的概率是可忽略不计。

(4)签名者身份的不可伪造性(signer-unforgeability)：如果签名者愿意透露自己的身份，他(她)可以使验证者确信谁是真正的签名者。任何攻击者(包括环内的其他人)，想伪造秘密信息证实自己是真实签名者的概率是可以忽略不计的。

4 无证书的可验证的环签名方案

(1)系统参数生成算法(CL-VRSGen)

设 G_1 是由它的一个生成元 P 生成的阶为素数 q 的加法群，G_2 是阶为 q 的乘法群，$e: G_1 \times G_1 \to G_2$ 是双线性对。H_1, H_2 是 2 个安全的哈希函数，其中，$H_1: \{0,1\}^* \to z_q^*$，$H_2: \{0,1\}^* \to G_1$。可信中心的私钥是 $s_0 \in z_q^*$，公钥是 $P_0 = s_0 P$，$L = \{ID_i\}$，$(i = 1, 2, \cdots, n)$ 表示签名人的身份集合。系统保密私钥 s_0，公布系统参数 $para = \{q, e, G_1, G_2, P, P_0, H_1, H_2\}$。

(2)部分私钥提取算法(CL-VRSEet-Par-Key)

对于身份为 ID_i 的环成员(也简记为 ID_i)，可信中心为其计算部分私钥 $D_i = sQ_i$，其中，$Q_i = H_2(ID_i)$，然后通过安全信道把它传给 ID_i $(i = 1, 2, \cdots, n)$。

(3)秘密值生成算法(CL-VRSSet-Sec-Val)

ID_i 选择 $x_i \in_R z_q^*$ 作为秘密值。

(4)密钥生成算法(CL-VRSSet-Pri- Key)

ID_i 计算其密钥 $S_i = x_i D_i = x_i s Q_i$。

(5)公钥生成算法(CL-VRSSet-Pub- Key)

ID_i 计算并公开其公钥 $(X_i, Y_i) = (x_i Q_i, x_i P_0)$ $(i = 1, 2, \cdots, n)$。

(6)签名的生成算法(CL-VRSSign)

对于消息 m，真实的签名者 ID_k (不妨设为第 k 个人)：

1) ID_k 选择 $r \in \{0,1\}^*$，计算 $t = H_1(X_k, Y_k, r)$，保密 r；

2) ID_k 选择 $r_i \in_R z_q^*$，计算 $U_i = r_i X_i$ (若 U_i 中有相同的，则重新选择 r_i)，$h_i = H_1(m \| L \| U_i)$ $(i \neq k)$；

3) ID_k 选择 $r_k \in_R z_q^*$，计算 $U_k = r_k X_k - \sum_{i \neq k} (r_i + h_i) X_i$，若 U_k 与 U_i 有相同，则重新选择 r_k，$h_k = H_1(m \| L \| U_k)$，$V = (r_k + h_k) S_k$。

签名为 $\sigma=(m,U_1,U_2\cdots U_n,V,t)$。

(7)签名的验证算法(CL-VRSVer)

1)验证者通过 $e(X_i,P_0)=e(Q_i,Y_i)$ 验证公钥的合法性，若等式成立再计算 $h_i=H_1(m\|L\|U_i)(i=1,2,\cdots,n)$；

2)验证 $e(P_0,\sum_{i=1}^{n}(U_i+h_iX_i))=e(P,V)$，如果等式成立，则认为签名是正确的，否则认为签名无效。

(8)真实签名者身份验证算法(CL-VRSIdVer)

如果真实签名者 ID_k 愿意泄露自己的身份，他(她)透露出秘密信息 (X_k,Y_k,r)，验证者验证等式 $t=H_1(X_k,Y_k,r)$ 是否成立，如果等式成立，则可以确定真实签名者的身份就是与公钥 (X_k,Y_k) 对应的 ID_k。

5 安全性分析

以下从无证书的可验证的环签名方案的安全性需求的几个方面证明其安全性。

定理 1 提出的无证书的可验证的环签名方案是正确的。

证明：如果 $\sigma=(m,U_1,U_2,\cdots,U_n,V,t)$ 是签名者对消息 m 的数字签名，则有：

$$e(P_0,\sum_{i=1}^{n}(U_i+h_iX_i))=e(P_0,U_k+h_kX_k+\sum_{i\neq k}(U_i+h_iX_i))=$$
$$e(P_0,r_kX_k-\sum_{i\neq k}(r_i+h_i)X_i+h_kX_k+\sum_{i\neq k}(U_i+h_iX_i))=$$
$$e(P_0,r_kX_k-\sum_{i\neq k}(U_i+h_iX_i)+h_kX_k+\sum_{i\neq k}(U_i+h_iX_i))=$$
$$e(P_0,(r_k+h_k)X_k)=e(sP,((r_k+h_k)x_kQ_k)=$$
$$e(P,(r_k+h_k)x_ksQ_k)=e(P,(r_k+h_k)S_k)=$$
$$e(P,V)$$

定理 2 提出的无证书的可验证的环签名方案满足签名者的匿名性。

证明：在一个合法的签名 $\sigma=(m,U_1,U_2,\cdots,U_n,V,t)$ 中，$U_i=r_iX_i(i\neq k)$，$U_k=r_kX_k-\sum_{i\neq k}(r_i+h_i)X_i$，$V=(r_k+h_k)S_k$。因为 r_i 是随机选择的，所以无论谁是真正的签名者，$(U_1,U_2,\cdots,U_n,V)$ 在 G_1 上都是均匀分布的；同时由于 $t=H_1(X_k,Y_k,r)$ 中的 r 是随机选择并且是保密的，由哈希函数 H_1 的单向性知，t 也不会泄露真实签名者的身份。综上所述，环成员之外的任何人猜出真实签名者的身份的概率不会超过 1/n，环之内除真实签名者外的成员猜出真正签名者的概率不会超过 1/(n-1)。

定理 3 提出的无证书的可验证的环签名方案在 CDHP 困难假设下满足不可伪造性。

证明：令 $P_0=aP,X_j=bP$，假设敌手 A 能成功伪造真实的签名者 U_k 的一个有效的无证书的可验证的环签名：$(m,U_1,U_2,\cdots,U_n,h_1,h_2,\cdots,h_n,V,t)$，由于本文方案也可看成一般的环签名方案，则由环签名分叉引理[7]可知，存在 1 个算法 A'，能以不可忽略的概率输出 2 个无证书的可验证的环签名方案：$(m,U_1,U_2,\cdots,U_n,h_1,h_2,\cdots,h_n,V,t)$ 和 $(m,U_1,U_2,\cdots,U_n,h_1',h_2',\cdots,h_n',V',t)$，其中，$h_i=h_i',i\in\{1,2,\cdots,n\}\backslash\{j\}$，而 $h_j\neq h_j'$。由于 2 个签名均有效，因此都满足签名验证方程，可得：

$$e(P_0,\sum_{i=1}^{n}(U_i+h_iX_i))=e(P,V)$$

$$e(P_0,\sum_{i=1}^{n}(U_i+h_i'X_i))=e(P,V')$$

由以上 2 个等式得：

$$e(P_0,(h_j-h_j')X_j)=e(P,V-V')$$

即：

$$e(aP,(h_j-h_j')bP)=e(P,V-V')$$

则有：

$$(h_j-h_j')abP=V-V'$$

因此，$abP=(h_j-h_j')^{-1}(V-V')$，即解决了 CDHP 的一个实例。而由 CDHP 是一个困难性问题知，上述假设是错误的，因此，提出的方案是不可伪造的。

定理 4 真实的签名者的身份是不可伪造的。

证明：在提出的方案中，任何的非真实签名者均无法证明他(她)是签名者，这是因为他(她)要证明自己是真实的签名者，就要从 $t=H_1(X_k,Y_k,r)$ 中解出秘密信息 (X_k,Y_k,r)，而由哈希函数 H_1 的单向性知，上述计算是困难的，因此，只有真实的签名者才能证明其签名者的身份。

6 结束语

本文给出一个无证书的可验证的环签名方案，由于方案是基于无证书的密码体制，可信中心只向用户提供部分私钥，用户的私钥是由自己选的秘密信息和部分私钥构成，而在基于身份的密码体制中用户的私钥完全由可信中心生成，因此克服了基于身份的密码体制的密钥托管问题。用户的公钥不再根据自己的身份来计算，而是用户利用公开参数和秘密信息来产生，这就避免了基于证书密码体制的公钥存储和管理问题。该方案不但具有一般的环签名的性质(签名者的匿名性、签名的不可伪造性)，还具有可验证性：只要真实签名者愿意，可以向验证者证明自己的身份。本文在 *CDHP* 困难问题假设下，证明了它的不可伪造性。在某些特定的场合(如泄密者想领奖)，该方案有重要的实用价值。

参考文献

[1] Rivest R, Shamir A, Tauman M. How to Leak a Secret[C]//Proc. of AsiaCrypt'01. [S. l.]: Springer-Verlag, 2001.

[2] Lv Jiqian, Wang Xinmei. Verifiable Ring Signature[C]//Proc. of the 9th International Conference on Distributed Multimedia Systems. Miami, USA: [s. n.], 2003.

[3] Shamir A. An Identity-based Cryptosystems and Signature Scheme[C]//Proc. of Crypto'84. [S. l.]: Springer-Verlag, 1984.

[4] Zhang Fanguo, Kim K. ID-based Blind Signature and Ring Signature from Pairings[C]//Proc. of AsiaCrypt'02. [S. l.]: Springer-Verlag, 2002.

[5] Al-Riyami S S, Paterson K G. Certificateless Public Key Cryptography[C]//Proc. of AsiaCrypt'03. [S. l.]: Springer-Verlag, 2003.

[6] 王玲玲，张国印，马春光. 一种基于双线性的可验证无证书的环签密方案[J]. 计算机应用, 2007, 27(9): 2167-2169.

[7] Saez H G. Forking Lemmas for Ring Signature Scheme[C]//Proc. of IndoCrypt'03. [S. l.]: Springer-Verlag, 2003.

编辑　顾姣健