基于身份的可链接和可转换环签名

王少辉[①] 郑世慧[②] 展 涛[①]
[①](山东大学数学与系统科学学院密码技术与信息安全教育部重点实验室 济南 250100)
[②](北京邮电大学网络与交换技术国家重点实验室 信息安全中心 北京 100876)

摘 要：环签名是提供匿名发布信息的巧妙方法，该文首次给出了基于身份的可链接环签名和可链接可转换环签名的概念与安全的形式化定义。以 Zhang 和 Kim 的环签名方案为例，给出了为某些基于身份环签名添加可链接性的方法。并分别提出了高效的基于身份的可链接环签名和可链接可转换环签名方案，方案除满足完备匿名性和适应性选择消息攻击下的不可伪造性外，还分别满足可链接性和对非签名者的不可转换性。

关键词：环签名；基于身份环签名；基于身份可链接环签名；基于身份可链接可转换环签名；双线性对
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2008)04-0995-04

Identity-Based Linkable and Convertible Ring Signature

Wang Shao-hui[①] Zheng Shi-hui[②] Zhan Tao[①]
[①](*Key Laboratory of Cryptologic Technology and Information Security*, *Ministry of Education*, *Shandong University*, *Jinan* 250100, *China*)
[②](*Information Security Center*, *State Key Laboratory of Networking and Switching Technology*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)

Abstract: In this paper, the concepts of identity-based linkable ring signature and linkable convertible ring signature are proposed. Taken Zhang and Kim's scheme as an example, a general method is given to add linkability and convertibility to some identity-based ring signatures. Then two efficient schemes are given for the first time, besides the complete anonymity and unforgeability under adaptively chosen message attack, one satisfying linkability, and the other satisfying both linkability and convertibility.

Key words: Ring signature; ID-based ring signature; ID-based linkable ring signature; ID-based linkable convertible ring signature; Bilinear pairs

1 引言

1984 年，Shamir 提出了基于身份密码系统的概念[1]。在此密码系统中，用户的公钥是与其身份紧密相关的字符串，如电子邮件地址、姓名等；由 PKG(Private Key Generator)负责给每个用户发放与其身份相对应的私钥。从而，避免了 PKI 体制花费大量时间管理和验证公钥证书的问题。文献[1]中提出了基于身份的签名方案，2001 年，Boneh 和 Franklin[2]利用双线性对给出了第一个可行的基于身份的加密系统。

环签名由 Rivest, Shamir 和 Tauman[3]在 2001 年正式提出，以实现对消息的完全匿名签名。接收方只能确认签名来自于某个群体，而不能确认具体签名者。考虑到应用环境的具体需要，人们对基本的环签名做了适当扩展，如基于身份的环签名[4−6]，可链接环签名[7, 8]，可转换环签名[9]，门限环签名[10]等。文献[7–9]均是在 PKI 体制下设计，并且文献[7]基于离散对数的可链接环签名方案只能满足计算匿名性，而不满足环签名所要求的完备匿名性。

目前，基于身份的可链接环签名和可转换环签名还没有提出相关的方案，这也是文献[11]提出的公开问题之一，本文研究了这两个方案的实现问题。首先利用文献[7]的设计思想，提出了为基于身份环签名添加可链接性的方法，然后利用该方法将文献[5]转化为基于身份的可链接环签名，将文献[4]转化为同时满足可链接性和可转换性的基于身份环签名，本文的方案可满足完备匿名性。

下文首先简单介绍相关的预备知识；然后给出了基于身份可链接环签名和可转换环签名的概念和安全形式化定义；第 4 部分首先提出了为某些基于身份环签名添加可链接性的方法，然后分别提出了两个高效的方案；所提方案的安全性分析在第 5 部分给出；最后是结束语。

2 预备知识

设方案的安全参数为 k，即 1^k 是算法的默认输入。我们称函数 $\varepsilon(k)$ 是可忽略的，如果对于任意的正多项式 $P(k)$，当 k 足够大时，都有 $\varepsilon(k)<1/P(k)$；如果存在某个 $P(k)$，满足 $\varepsilon(k)>1/P(k)$, $\forall k\in N$，则称其为不可忽略的。

2007-04-09 收到，2007-09-20 改回
国家 973 项目(2007CB807903)和国家杰出青年基金(60525201)资助课题

近年来，双线性对在密码学中得到了广泛的应用，已经成为设计各种密码体系的重要工具之一。设 G_1 和 G_2 分别是阶为大素数 q 的循环加法群和乘法群， P 是 G_1 的生成元。 $a,b,c \in Z_q$ 是随机数，假设离散对数问题在 G_1 和 G_2 中都是难解的。

定义 1 我们称映射 $e: G_1 \times G_1 \to G_2$ 为一个双线性对，如果满足：

(1) 双线性： $\forall Q,R,S \in G_1$ ，有 $e(Q+R,S)=e(Q,S)\cdot e(R,S)$ ， $e(Q,R+S)=e(Q,S)e(Q,R)$ ；

(2)非退化性： $\exists Q,R \in G_1$ ，使得 $e(Q,R) \neq 1$ ；

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

在群 G_1 上，我们可以定义以下几个密码学困难问题：(1) 计算 Diffie-Hellman(CDH)问题：给定 (aP,bP) ，计算 abP ；(2)决策 Diffie-Hellman(DDH)问题：给定 (aP,bP,cP) ，判断是否满足 $c=ab$ ；(3)Gap Diffie-Hellman (GDH)问题：一类 CDH 问题困难而 DDH 问题容易的问题。

3 基于身份的可链接和可转换签名的形式化定义

基于身份的密码体系中，给定双线性对系统 (G_1,G_2,e,q,P) ，PKG 随机选择 $s \in Z_q^*$ 作为其主私钥，计算 $P_{\text{pub}}=sP$ 作为其主公钥。给定哈希函数 H_1 和 H_2 ， $H_1:\{0,1\}^* \to G_1$ ，而 $H_2:\{0,1\}^* \to Z_q$ ，则系统的公开参数 $\text{params}=\{G_1,G_2,e,q,P,P_{\text{pub}},H_1,H_2\}$ 。用户将身份 $\text{ID} \in \{0,1\}^*$ 送 PKG，PKG 设定用户公钥 Q_{ID} 为 $H_1(\text{ID})$ ，私钥 S_{ID} 为 sQ_{ID} ，PKG 通过安全信道将私钥送给用户。

简单地说，可链接性就是验证者可确认不同签名来自同一签名者，但并不能确认签名者的身份；而可转换性则是签名者可在公布一定信息后，将所签的环签名转化成为一般的签名。文献[7]和文献[9]分别给出了一般可链接环签名和可转换环签名的形式化定义，这里我们将其扩展到基于身份的环境中。

定义 2 (**基于身份可链接环签名**) 基于身份可链接环签名由 Setup, Extract, Sign 和 Verify 4 个算法组成：Setup, Extract 和 Sign 都是概率多项式时间算法，Verify 是一个确定性算法。其中 Setup 输入安全参数 1^k ，输出公共参数 params 和主私钥 s ； Extract 输入 params ，用户身份 ID ，输出用户私钥 S_{ID} ； Sign 输入消息 m ， params ，用户私钥 S_{ID} 和公钥列表 $L=\{\text{ID}_i\}_{i=0}^{n-1}$ ，输出签名 σ ； Verify 输入 params ，公钥列表 L 和签名 σ ，通过验证输出 1，否则输出 0。

基于身份的可链接环签名应满足完备性、适应性选择消息攻击下的不可伪造性、签名匿名性和可链接性。

定义 3 (**完备性**) 合法签名者正确执行签名方案输出的签名 σ ，通过 Verify 算法验证的概率为 1。

定义 4 (**不可伪造性**) 令 $\text{SO}(\text{params},L',m')$ 是一个输入 params ，消息 m' 和公钥列表 L' ，生成相应签名 σ' 的预言， $\text{EO}(\text{params,ID})$ 是输入用户 ID ，输出该用户私钥 S_{ID} 的预言。我们称方案满足适应性选择消息攻击下的不可伪造性是指对于任意的概率多项式算法 A ，通过适应性的访问哈希函数和预言 $\{H_1,H_2,\text{SO},\text{EO}\}$ ，输出 (L,m,σ) ，满足 $\text{Verify}(\text{params},L,m,\sigma)=1$ 的概率是可忽略的，而且要求 A 不曾向 EO 询问 L 中成员的私钥，也不曾向 SO 询问 m 的签名。

定义 5 (**签名匿名性**) 令 $L=\{\text{ID}_i\}_{i=0}^{n-1}$ 为公钥列表，方案称为完备匿名的，如果对任意消息 m ，以及随机选择的成员(私钥为 sk)，和环签名 $\sigma=\text{Sign}(\text{params},L,m,\text{sk})$ ，对于任意算法 $A(\text{params},L,m,\sigma)$ 输出 sk 的概率恰为 $1/n$ ；如果算法 A 是概率多项式时间算法，则方案称为计算匿名的。

定义 6 (**可链接性**) 如果对不同消息 m_1 和 m_2 ，签名者可生成合法签名 σ_1 和 σ_2 (可选择不同的公钥列表)，存在概率多项式算法 F ，得出 $(\text{params},L,m_1,m_2,\sigma_1,\sigma_2)$ 是同一人签名的概率是不可忽略的；而如果两个签名不是由同一个用户签署，则对任意的概率多项式算法 F ，得出是同一签名人签署的概率是可忽略的，则称方案为可链接的。

基于身份的可链接可转换环签名的定义和上述基本类似，除了上述安全需求，还应满足对非签名者的不可转换性：

定义 7 (**对非签名者的不可转换性**) 如果非签名者将方案转换成一般签名方案的概率是可忽略的，则称方案是对非签名者不可转换的，也就是说非签名者不能证明自己是真正的签名者。

4 方案描述

文献[7]设计了基于离散对数的可链接环签名，签名者的私钥是 x_k ，如果签名者要链接两个不同消息的签名，则其选择相同的公钥列表 L ，并计算 $y'=H(L)^{x_k}$ ，利用该值作为链接两个签名的标识；然后在生成环阶段和封闭环阶段构造了一个知识证明，证明签名者的公钥和标识的离散对数是相等的。利用这个思想，在基于身份的环签名方案中，签名者可选择参数 t ，利用 $P'=tP$ 或者 $H'=tH_1\cdot(\text{ID}_k)$ 作为签名链接的标识，从而为原方案添加可链接的性质。

4.1 基于身份的可链接环签名方案

下边首先以 Zhang 和 Kim[4]的方案为例，说明如何为一般基于身份环签名添加可链接性，改进方案签名长度是原签名的两倍，运算量也过大，效率不高。这里，我们只描述 Sign 和 Verify 算法。通常，签名算法在发布签名前，要进行 3 步操作：初始化阶段；为非签名者生成环序列；将环封闭。

Sign 算法：

(1)初始化：随机选择 $t\in Z_q^*$ 和 G_1 中元素 A，计算 $P'=tP$ 和 $c_{k+1}=H_2(L\,||\,m\,||\,e(A,P)\,||\,e(A,P))$；

(2)对非签名者生成环序列：对 $i=k+1,\cdots,n-1,0,\cdots,k-1$，随机选择 G_1 中元素 R_i 和 T_i，计算 $c_{i+1}=H_2(L\,||m||\,e(R_i,P)e(c_iH_1(\mathrm{ID}_i),P_{\mathrm{pub}})\,||\,e(T_i,P)e(c_iH_1(\mathrm{ID}_i),P'))$；

(3)封闭环：计算 $R_k=A-c_kS_{\mathrm{ID}_K}$ 和 $T_k=A-c_ktH_1(\mathrm{ID}_k)$，实际上有 $e(R_k,P)e(c_kH_1(\mathrm{ID}_k),P_{\mathrm{pub}})=e(A-c_kS_{\mathrm{ID}_k},P)e(c_kS_{\mathrm{ID}_k},P)=e(A,P)$，而 $e(T_k,P)e(c_kH_1(\mathrm{ID}_k),P')=e(A-c_ktH_1(\mathrm{ID}_k),P)\ e(c_kH_1(\mathrm{ID}_k),\ tP)\ =e(A,P)$；

(4)发布签名：输出签名 $\sigma=(P',c_0,R_0,R_1,\cdots,R_{n-1},T_0,T_1,\cdots,T_{n-1})$。

Verify 算法：

对于 $i=0,1,\cdots,n-1$，计算 $c_{i+1}=H_2(L\,||\,m\,||\,e(R_i,P)\cdot e(c_iH_1(\mathrm{ID}_i),P_{\mathrm{pub}})\,||\,e(T_i,P)e(c_iH_1(\mathrm{ID}_i),P'))$，如果 $c_n=c_0$，则验证通过，否则拒绝。

上述方案虽然可以提供可链接性，但是效率远低于原方案。实际上，上述方案的改进方法可应用于其它某些基于身份的环签名方案中。文献[5]采用的是和文献[4]不同的设计思路，下边给出对文献[5]的改进方案，新方案的效率与原方案等同，比上述方案效率大大提高。

Sign 算法：

(1)初始化：随机选择 $t\in Z_q^*$ 和 G_1 中元素 A，计算 $P'=tP$；

(2)对非签名者生成环序列：对于 $i=k+1,\cdots,n-1,0,\cdots,k-1$，随机选择 G_1 中元素 R_i，计算 $r_i=e(R_i,P')$ 和 $c_i=H_2(L\,||\,m\,||\,r_i)$；

(3)封闭环：首先计算 $U=\sum_{i\in\{0,\cdots,n-1\}\backslash\{k\}}\{c_iH_1(\mathrm{ID}_i)\}$，然后计算 $r_k=e(A,P')e(-P_{\mathrm{pub}},U)e(-P',U)$ 和 $c_k=H_2(L||m||\cdot r_k)$，最后计算 $V=c_kS_{\mathrm{ID}_k}+c_ktH_1(\mathrm{ID}_k)+t\left(A+\sum_{i\in\{0,\cdots,n-1\}\backslash\{k\}}\{R_i\}\right)$；

(4)发布签名：输出签名 $\sigma=(P',r_0,r_1,\cdots,r_{n-1},V)$。

Verify 算法：

对 $i=0,1,2,\cdots,n-1$，计算 $c_i=H_2(L\,||\,m\,||\,r_i)$，如果 $e(P,V)=\prod_{i=0}^{n-1}\{r_i\}e\left(P_{\mathrm{pub}},\sum_{i\in\{0,1,\cdots,n-1\}}\{c_iH_1(\mathrm{ID}_i)\}\right)\cdot e\left(P',\sum_{i\in\{0,1,\cdots,n-1\}}\{c_iH_1(\mathrm{ID}_i)\}\right)$，则验证通过，否则拒绝。

4.2 基于身份的可链接可转换环签名方案

本文基于文献[4]给出了基于身份可链接可转换环签名方案，这里选择 $H'=tH_1(\mathrm{ID}_k)$ 作为标识，相当于签名者对自己的身份做了盲化，新方案的效率与文献[4]等同。

Sign 算法：

(1)初始化：随机选择 $t\in Z_q^*$ 和 G_1 中元素 A，计算 $H'=tH_1(\mathrm{ID}_k)$ 和 $c_{k+1}=H_2(L\,||\,m\,||\,e(A,P))$；

(2)对非签名者生成环序列：对于 $i=k+1,\cdots,n-1,0,\cdots,k-1$，随机选择 G_1 中元素 R_i，计算 $c_{i+1}=H_2(L\cdot||m||e(R_i,P)e(c_iH',P_{\mathrm{pub}}))$；

(3)封闭环：计算 $R_k=A-c_ktS_{\mathrm{ID}_K}$，实际有 $e(R_k,P)\cdot e(c_kH',P_{\mathrm{pub}})=e(A-c_ktS_{\mathrm{ID}_k},P)e(c_ktH_1(\mathrm{ID}_k),P_{\mathrm{pub}})=e(A-c_kt\cdot S_{\mathrm{ID}_k},P)\ e(c_ktS_{\mathrm{ID}_k},P)=e(A,P)$；

(4)发布签名：输出签名 $\sigma=(H',c_0,R_0,R_1,\cdots,R_{n-1})$。

Verify 算法：

对于 $i=0,1,\cdots,n-1$，计算 $c_{i+1}=H_2(L\,||\,m\,||\,e(R_i,P)\cdot e(c_iH',P_{\mathrm{pub}}))$，若 $c_n=c_0$，则验证通过，否则拒绝。

5　方案安全性分析

5.1 基于身份的可链接环签名方案

本文以基于文献[4]的改进方案为例说明安全性。这里选择 $P'=tP$ 作为签名者链接签名的标识，这与用户的私钥秘密和用户的身份信息是独立的，在生成环和环封闭阶段，构造了两个知识证明，一个证明签名者了解私钥信息，另一个证明签名者知道 P' 的离散对数。下边分别就方案所满足的匿名性、不可伪造性和可链接性进行简单讨论。

(1)匿名性　文献[7]中，如果攻击者能够求解离散对数问题，则签名者的身份也就泄露了，也就是说文献[7]所满足的匿名性是计算匿名而不是完备匿名，其匿名性是针对概率多项式时间的攻击者成立。而本文的方案能够实现完备匿名性，因为即便能够求解出参数 t，一方面 P' 的生成没有用到签名者身份信息 $H_1(\mathrm{ID}_k)$，另一方面在公式 $R_k=A-c_kS_{\mathrm{ID}_K}$ 和 $T_k=A-c_ktH_1(\mathrm{ID}_k)$ 中，攻击者能获得信息 (R_k,c_k,T_k,t)，而未知的元素有 3 个，并不能求解出未知参数的值。而每一个非签名者能等概率地生成 P'，进而能等概率地完成整个签名方案，不同签名者的签名是完全不可区分的，从而方案满足完备匿名性。

(2)适应性选择消息下的不可伪造性　可以看出新方案中对签名预言的询问同原方案一样，并不能提供额外的信息。攻击者可以与 SO 或者 EO 进行交互，获得某些消息的签名或者某些用户的私钥，然后选择好固定的公钥列表 L，攻击者可以随机选择 t'，生成相应的 $P'=t'P$，其中 P' 不是 SO 的输出，虽然攻击者知道 t' 的信息，从而能控制 c_{i+1} 的后半部分的封闭，但是如果攻击者寻找到合适的 $\sigma=\{P',c_0,R_0,R_1,\cdots,R_{n-1},T_0,T_1,\cdots,T_{n-1}\}$ 通过 Verify 算法的验证，由 Hash 函数的随机性，攻击成功相当于攻击者能够找到封闭第一个知识证明的算法，也就是找到了破解文献[4]的方法；而另一方面，攻击者选择 SO 输出的 P'，因为选择的参数 t，必须参与封闭环的操作，由 Hash 函数的随机性，如果在不知道 t 的时候，存在适应性选择消息下的伪造攻击，则存在相应的算法解决离散对数问题和破解文献[4]。

(3)可链接性　如果签名者希望链接自己签署的不同消

息 m_1 和 m_2，则通过签名算法选择相同的 $P'=tP$，得到签名 $\sigma=\{P',c_0,R_0,\cdots,R_{n-1},T_0,\cdots,T_{n-1}\}$ 和 $\sigma'=\{P',c_0',R_0',\cdots,R_{n-1}',T_0',\cdots,T_{n-1}'\}$，验证者验证两个签名的合法性，并断定两个消息由同一个用户签署，这里并不要求选择相同的公钥列表。由于完成封闭环这步操作，必须使用参数 t，任意的非签名者在不知道 t 时，伪造合法签名的概率是可忽略的。从而，在假设离散对数问题难解的条件下，σ 和 σ' 来自不同签名者的概率是可忽略的，方案满足可链接性。

5.2 基于身份的可链接可转换环签名方案

同满足可链接性方案相比，该方案只构造了一个知识证明，虽然这里将 $H'=tH_1(\mathrm{ID}_k)$ 作为标识，应用了签名者的身份信息，但是对攻击者而言，$H_1(\mathrm{ID}_k)$ 本身是未知的，通过 t 的盲化实现完备匿名性。可链接性和适应性选择消息下的不可伪造性不再具体讨论。

对非签名者的不可转化性 如果签名者想让外界知道消息确实是自己所签，则可以公布参数 t，由于 $R_k=A-c_ktS_{\mathrm{ID}_K}$，公布 t 后仍然存在两个未知参数，并不会泄露私钥信息，验证者很容易验证等式 $P'=tH_1(\mathrm{ID}_k)$ 是否成立；而对于非签名者 i，其要寻找 t'，满足 $tH_1(\mathrm{ID}_k)=t'H_1\cdot(\mathrm{ID}_i)$ 是困难的。

6 结束语

对环签名和满足一些特殊要求的环签名的研究是当前数字签名领域的研究热点之一。本文提出了基于身份的可链接环签名和可链接可转换环签名的概念和安全形式化定义，提供了为一般的基于身份环签名添加可链接性和可转换性的方法，并分别设计了两个高效的签名方案。对于设计更高效和满足其他性质的环签名方案，如可分性，还有待进一步的研究。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes. Advances in Cryptology——Crypto 1984, LNCS 196: 47–53.

[2] Boneh D and Franklin M. Identity-based encryption from the weil pairing. Advances in Cryptology——Crypto 2001, LNCS 2139: 213–229.

[3] Rivest R, Shamir A, and Tauman Y. How to leak a secret. In: Advances in Cryptology ——AsiaCrypt'01, Berlin: Springer-Verlag, 2001, LNCS 2248: 552–565.

[4] Zhang Fangguo and Kim Kwangjo. ID-based blind signature and ring signature from pairings. Advances in Cryptology——AsiaCrypt 2002, LNCS 2501: 533–547.

[5] Herranz J and Saez G. New identity-based ring signature schemes. International Conference on Information and Communications Security——ICICS 2004, LNCS 3269: 27–39.

[6] Chow S S M, Yiu S M, and Hui L C K. Efficient identity based ring signature. Applied Cryptography and Network Security——ACNS 2005, LNCS 3531: 499–512.

[7] Liu J K, Wei V K, and Wong D S. Linkable spontaneous anonymous group signature for Ad-hoc groups (Extended Abstract). In: ACISP'04, Berlin: Springer-Verlag, 2004, LNCS 3108: 325–335.

[8] Mao Ho Au, Chow S S M, Susilo W, and Tsang P P. Short linkable ring signatures revisited. In: EuroPKI 2006, Berlin: Springer-Verlag, 2006, LNCS 4043: 101–115.

[9] Lee K C, Wen H A, and Hwang T. Convertible ring signature. *IEE Proc-Commun.*, 2005, 152(4): 411–414.

[10] Bresson E, Stern J, and Szydlo M. Threshold ring signatures and applications to Ad-hoc group. In: Crypto 2002, Berlin: Springer-Verlag, 2002, LNCS 2442: 465–480.

[11] Chow S S M, Liu R W C, Hui L C K, and Yiu S M. Identity-based ring signature: why, how and what next. In: EuroPKI 2005, Berlin: Springer-Verlag, 2005, LNCS 3545: 144–161.

[12] Abe M, Ohkubo M, and Suzuki K. 1-out-of-n signatures from a variety of keys. Advances in Cryptology ——AsiaCrypt 2002, LNCS 2501: 415–432.

[13] Gao Wei, Wang Guilin, Wang Xueli, and Xie Dongqing. Controllable ring signatures. The 7th International Workshop on Information Security Applications (WISA 2006), Springer-Verlag, 2006, LNCS 4298: 1–14.

王少辉： 男，1977 年生，博士生，研究领域为数字签名、公钥密码理论.

郑世慧： 女，1979 年生，博士后，研究领域为密码分析和公钥理论.

展 涛： 男，1963 年生，教授，博士生导师，主要研究领域为解析数论、群签名与电子钱币.