几种可转换环签名方案的安全性分析和改进

王化群[①②]　郭显久[①]　于 红[①]　彭玉旭[②]
[①](大连水产学院信息工程学院　大连　116023)
[②](长沙理工大学计算机与通信工程学院　长沙　410076)

摘　要：通过对 Zhang-Liu-He (2006)，Gan-Chen (2004)和 Wang-Zhang-Ma (2007)提出的可转换环签名方案进行分析，指出了这几个可转换环签名方案存在可转换性攻击或不可否认性攻击，即，环中的任何成员都能宣称自己是实际签名者或冒充别的成员进行环签名。为防范这两种攻击，对这几个可转换环签名方案进行了改进，改进后的方案满足可转换环签名的安全性要求。

关键词：环签名；密码分析；可转换性
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2009)07-1732-04

Cryptanalysis and Improvement of Several Convertible Ring Signature Schemes

Wang Hua-qun[①②]　Guo Xian-jiu[①]　Yu Hong[①]　Peng Yu-xu[②]
[①](*School of Information Engineering*, *Dalian Fisheries University*, *Dalian* 116023, *China*)
[②](*College of Computer and Communication Engineering*, *Changsha University of Science & Technology*, *Changsha*, 410076, *China*)

Abstract: The security of the three convertible ring signature schemes proposed by Zhang-Liu-He (2006), Gan-Chen (2004) and Wang-Zhang-Ma(2007) is analyzed, and it is found that these convertible ring signature schemes are susceptible to convertibility attack or non-repudiation attack, i.e., any member in the ring can claim that he is the actual signer or pretend others' identity to sign message. To guard against the attack, these convertible ring signature schemes are improved, which can make the improved schemes satisfy the security requirements for convertible ring signature.

Key words: Ring signature; Cryptanalysis; Convertibility

1　引言

2001年，Rivest，Shamir和Tauman首次正式提出了环签名的概念[1]，并且利用组合函数和对称密码体制给出了一种高效的环签名方案。环签名提出以后引起了广泛的关注，并提出了各种环签名方案[2−5]。后来，Rivest，Shamir和Tauman对近年来环签名的研究进展给予了简单的总结[6]。环签名是一种新的匿名签名技术，因签名中参数根据一定的规则首尾相接组成环状而得名。环签名可以实现无条件匿名，即使攻击者拥有无限的计算能力，也无法追踪签名人的身份。环签名的这种无条件匿名性在对信息需要长期保护的一些特殊环境中非常有用。

环签名是以泄漏秘密的背景提出的，后来被广泛应用于其它环境中，比如，匿名举报等。在匿名举报中，举报人为保护自己，又能够取信于举报中心，可应用环签名来设计电子匿名举报方案[7,8]。在匿名电子举报中，如果举报悬赏时，为获得巨大的利益，在成功举报后，实际举报人将力求证明该举报为自己所为。这样，为满足这种需要，Lü-Wang提出了可验证环签名的概念[9]，随后，一些新的可验证环签名方案被提出[10,11]。2005年，Lee-Wen-Hwang形式化提出了可转换环签名的概念[12]。可转换的环签名的概念不仅保持环签名的所有性质，还能够使得实际签名者将所签名的环签名转换为通常的签名，方法是通过展示一些信息。一个可转换的环签名包括：ring-sign算法，ring-verify算法，ring-convert算法，ring-convert-verify算法。从文献的定义和提出背景分析，Lü-Wang提出了可验证环签名与Lee-Wen-Hwang提出的可转换环签名是同一种签名形式，本文统一称为可转换的环签名。可转换签名的目的就是将具有特定目的的签名转换为通常的签

2008-07-18 收到，2008-11-10 改回
辽宁省教育厅计划(2008140)，大连水产学院科学研究计划(sy2007032)，大连水产学院校人才引进项目(SYYJ200612)，国家自然科学基金(60673070)和长沙理工大学人才引进基金(No.1004151)资助课题

名。目前，具有可转换性质的环签名还包括Gao-Wang-Wang-Xie提出的可控环签名[13]，Wang-Zhang-Ma提出的环签密方案[14]等。因而，可转换环签名的研究得到学者们的广泛关注，而有关于可转换环签名密码分析的文章还比较少见。研究可转换环签名的安全性对于设计安全的可转换环签名方案具有重要的意义。

第2节简要介绍了文献[10]提出的可转换环签名方案，针对该方案提出了不可否认性攻击；第3节简要介绍了文献[11]提出的可转换环签名方案，并提出了不可否认性攻击；第4节简要介绍了文献[14]提出的无证书环签密方案，并提出了不可否认性攻击；第5节分析了上述具有可转换性质的环签名方案存在不可否认性攻击的原因，并给出了一般性的改进方法；第6节对本文进行总结。

2 Zhang-Liu-He[10]基于 Nyberg-Rueppel 的可转换环签名方案及其攻击方法

首先简要给出 Zhang-Liu-He 基于 Nyberg-Rueppel 的可转换环签名方案，然后再给出相应的攻击方法。该方案基于有限域上的离散对数问题，h 为一密码哈希函数。

2.1 Zhang-Liu-He 基于 Nyberg-Rueppel 的可转换环签名方案

设环成员集为 $L=\{U_1,\cdots,U_n\}$，U_i 对应的私钥为 s_i，公钥为 $p_i=\alpha^{s_i} \bmod p$，在下面的可转换环签名方案中，设签名者为 U_s，选取的环成员集为 $L=\{U_1,\cdots,U_n\}$，U_s 计算如下：

签名

(1)初始化　签名者 U_s 取随机值 $a\in Z_q$，计算：$\sigma=\alpha^{-a} \cdot \bmod p$，$c_{i+1}=h(m,\sigma)$；

(2)产生前向环序列　签名者 U_s 取随机值 $y_i\in Z_q,(1\le i\le n,i\ne s)$，其中 $i=s+1,\cdots,n,1,\cdots,s-1$，依次计算 $c_{i+1}=h(m,\alpha^{y_i}P^{c_i} \bmod p)$，其中 $c_{n+1}=c_1$；

(3)计算 $y_s=a+s_sc_s \bmod q$　设 $e_s=c_s$，选择满足 $e_s=x\alpha^{-a} \bmod p$ 的 $x\in Z_p$，签名者 A_s 得到 3 元组 (e_s,y_s,x)，并将 3 元组 (e_s,y_s,x) 保密。这样，关于消息 m 的环签名为 $(p_1,\cdots,p_n;c_1;y_1,\cdots,y_n)$。

验证

(1)验证者计算 $c_{i+1}=h(m,\alpha^{y_i}P_i^{c_i} \bmod p)$，其中 $i=2,3,\cdots,r$；

(2)如果 $c_{r+1}=c_1$，接受；否则，拒绝。

环签名转换和转换验证

签名者 U_s 向验证者出示 3 元组 (e_s,y_s,x)，验证者检测 $x=\alpha^{y_s}P_s^{e_s} \bmod p$ 是否成立。如果成立，接受；否则，拒绝。

2.2 Zhang-Liu-He 可转换环签名方案的可转换性攻击

对于非签名者 U_i，$i\ne s$，接收到关于消息 m 的环签名 $(P_1,\cdots,P_r;c_1;y_1,\cdots,y_r)$ 后，取 $e_i=c_i$，计算：$b=y_i-s_ie_i \cdot \bmod q, e_i=x\alpha^{-b} \bmod p$，则 $x=c_i\alpha^{y_i-S_ie_i}=c_i\alpha^{y_i}P_i^{-c_i} \bmod p$。这样，非签名者 U_i，$i\ne s$，得到 3 元组 (e_i,y_i,x)。从上述计算可知，该 3 元组 (e_i,y_i,x) 满足转换验证方程，因而能够通过转换验证。这样，非签名者 U_i 能够假冒实际签名者 U_s，可验证性不成立。

3 Gan-Chen[11]可转换环签名方案及其攻击方法

先简要给出 Gan-Chen 可验证环签名方案，然后再给出相应的攻击方法。该方案是基于有限域上的 RSA 公钥加密，$h:\{0,1\}^*\to\{0,l\}^l$ 为密码哈希函数，E 为公开的对称加密函数。

3.1 Gan-Chen 可转换环签名方案

设环成员集为 $L=\{U_1,\cdots,U_n\}$，U_i 对应的私钥为 $s_i=(n_i,d_i)$，公钥为 $p_i=(n_i,e_i)$，加密算法为 $f_i(x)=x^{e_i} \bmod n_i$,组合函数如下：

$$C_{k,v}(y_1,y_2,\cdots,y_n)=E_k(y_n\oplus E_k(y_{n-1}\cdots\oplus E_k(y_1\oplus v)))$$

在下面的可转换环签名方案中，设签名者为 U_s，选取的环成员集为 $L=\{U_1,\cdots,U_n\}$，假设请求签名的消息为 m，U_s 计算如下：

签名

(1)计算 $k=h(m)$，随机选取 $r,x_1,\cdots,x_{s-1},x_{s+1},\cdots,x_n\in_R\{0,1\}^b$，计算 $y_i=f_i(x_i)$，$i\ne s$；$v=h(h(r\|\mathrm{ID}_s))$，其中 ID_s 为签名者的身份；

(2)求解组合函数 $C_{k,v}(y_1,\cdots,y_n)=v$，得到 y_s；

(3)利用其 RSA 私钥，计算 $x_s=f_s^{-1}(y_s) \bmod n_s$；

则消息 m 的签名为 $(P_1,\cdots,P_n;v;x_1,\cdots,x_n)$；

验证

(1)计算 $k=h(m)$，计算 $y_i=f_i(x_i)$，$i=1,2,\cdots,n$；

(2)检测 $C_{k,v}(y_1,y_2,\cdots,y_n)=v$ 是否成立，如果成立，接受；否则，拒绝。

Ring-convert 和 Convert-verify：

实际签名者 U_s 公开 $t=h(r\|\mathrm{ID}_s)$，验证者确认 $v\stackrel{?}{=}h(t)$，如果成立，则实际签名者能够被匿名识别。如果实际签名者想公开自己的身份，则公开 (r,ID_s)，验证者确认 $v=h(h(r,\mathrm{ID}_s))$ 是否成立，如果成立，则实际签名者能够被识别。

3.2 Gan-Chen 可转换环签名方案的不可否认性攻击

可转换性要求实际签名者向验证者提供不可否认性的证据，证明签名是自己所为。但是，签名

$(P_1,\cdots,P_n;v;x_1,\cdots,x_n)$ 仅仅表明了 $v=h(h(r,\mathrm{ID}_s))$ 成立，这样，不可否认性不能被保证。任何签名者 $U_i,i\neq s$ 都能随机选取 r，并计算 $v=\ h(h(r,\mathrm{ID}_s))$，然后产生有效的环签名，从而通过提交 (r,ID_s) 给验证者就能够冒充该签名为 U_s 所为，因而，Gan-Chen 可转换环签名方案的不可否认性不能满足。

4 Wang-Zhang-Ma[14]无证书环签密方案及其攻击方法

KGC选取 $s\in_R Z_q^*$ 作为主密钥，计算系统公钥为 $P_0=sP$，系统参数为 $\{G_1,G_2,e,q,P,P_0,H_1,H_2,H_3,H_4,H_5\}$，其中，$H_1:\{0,1\}^*\to G_1^*,H_2:G_2\to\{0,1\}^l$，$H_3:\{0,1\}^l\to\{0,1\}^l$，$H_4:\{0,1\}^*\to\{0,1\}^l,H_5:\{0,1\}^*\to Z_q^*$ 为密码哈希函数。

密钥生成：设用户 U_i 的身份为 ID_i，KGC计算 $D_i=sH_1(\mathrm{ID}_i)=sQ_i$ 作为其部分私钥；用户 U_i 随机选取 $x_i\in_R Z_q^*$ 作为其秘密值，计算其私钥为 $S_i=x_iD_i$，公钥为 $(X_i,Y_i)\ =(x_iQ_i,x_iP_0)$。

4.1 Wang-Zhang-Ma无证书环签密方案

在下面的无证书环签密方案中，设签密者为 U_s，选取的环成员集为 $L=\{U_1,\cdots,U_n\}$，假设请求签名的消息为 m，解密验证者为 U_B，对应的公钥为 (X_B,Y_B)，私钥为 S_B，U_s 计算如下：

(1) 选取 $r_0\in Z_q^*,m_r\in_R M$，计算 $R_0=r_0P,R_0^{'}=e(r_0P_0,X_B),k=H_2(R_0^{'}),c_1=m_r\oplus k$，$c_2=m\oplus H_3(m_r)$；

(2)选取 $r\in\{0,1\}^l$ 并保密，计算 $t=H_4(Y_1,\cdots,Y_{s-1},Y_{s+1},\ \cdots,Y_n,r)$，$k_0=k\oplus t$；

(3)选取 $r_i\in_R Z_q^*$，$i\neq s$，计算 $A_i=r_iP,R_i=e(A_i,P),h_i=H_5(L,m,k_0,R_i)$；

(4)选取 $r_s\in_R Z_q^*$，计算 $A_s=r_sP,R_s=e(A_s,P)\cdot e\left(-P_0,\sum_{i\neq s}h_iX_i\right)$，$h_s=H_5(L,m,k_0,R_s)$，最后，密文为：$\sigma=(L,t,c_1,c_2,\sigma,R_0,R_1,\cdots,R_n,h_1,\cdots,h_n)$。

解密并验证

接收到密文 $\sigma=(L,t,c_1,c_2,\sigma,R_0,R_1,\cdots,R_n,h_1,\cdots,h_n)$ 后，U_B 计算如下：

(1)检测 $e(X_i,P_0)=e(Q_i,Y_i)$，$i=1,2,\cdots,n$ 是否成立，如果成立，继续下一步；

(2)计算 $k'=H_2(e(R_0,S_B))$，$m_r^{'}=c_1\oplus k',m'=c_2\oplus H_3(m_r^{'})$；

(3)计算 $k_0^{'}=k'\oplus t$，h_i=$H_5(L,m',k_0^{'},R_i),i\in\{1,2,\cdots,n\}$，检测

$$e(\sigma,P)=R_1\cdots R_ne\leq\left(P_0,\sum_i h_iX_i\right)$$

是否成立，如果成立，则接受，否则，拒绝。

环签名转换和转换验证

实际签密者 U_s 提交 $\{Y_1,\cdots,Y_{s-1},Y_{s+1},\cdots,Y_n,r\}$，确认者检测 $t=H_4(Y_1,\cdots,Y_{s-1},\ Y_{s+1},\cdots,Y_n,r)$ 是否成立，如果成立，则实际签密者为 U_s，否则，拒绝。

4.2 Wang-Zhang-Ma 无证书环签密方案的不可否认性攻击

可转换性要求实际签名者向验证者提供不可否认性的证据，证明签名是自己所为。但是，签名 $\sigma=(L,t,c_1,c_2,\sigma,R_0,R_1,\cdots,R_n,h_1,\cdots,h_n)$ 仅仅表明了 $t=H_4(Y_1,\cdots,Y_{s-1},Y_{s+1},\cdots,Y_n,r)$ 成立，这样，不可否认性不能被保证。任何签名者 $U_i,i\neq s$ 都能随机选取 r，并计算 $t=H_4(Y_1,\cdots,Y_{s-1},\ Y_{s+1},\cdots,Y_n,r)$，然后产生有效的环签名，从而通过提交 $\{Y_1,\cdots,Y_{s-1},\ Y_{s+1},\cdots,Y_n,r\}$ 给验证者就能够冒充该签名为 U_s 所为，因而，Wang-Zhang-Ma无证书环签密方案的不可否认性不能满足。

5 上述 3 个具有可转换性质的环签名方案的安全性分析及改进

数字签名必须满足3个条件：(1)接收方能够验证发送方所宣称的身份；(2)发送方以后不能否认报文是他发送的；(3)接收方自己不能伪造该报文。环签名方案转换成普通数字签名方案后，也必须满足上述3个条件。因而，可转换环签名中实际签名者用以转换的秘密信息不能被环中其它成员伪造或仿真，否则，转换后的环签名的不可否认性无法保证。Zhang-Liu-He基于Nyberg-Rueppel的可转换环签名方案中，环中任何成员都能够产生类似于实际签名者的秘密信息，能够宣称为自己所签，因而不能保证可转换性。Gan-Chen可转换环签名方案和Wang-Zhang-Ma无证书环签密方案中，实际签名者进行转换的秘密信息能够被环中其它成员仿真，因而环中其它成员就能够冒充实际签名者进行转换。

为满足上述 3 个条件，可转换环签名方案中实际签名者进行转换的秘密信息必须满足下面 2 个条件：(1)不能被环中其它成员进行仿真；(2)在某个消息的具体的可转换环签名产生后，环中其它成员不能产生相应的转换信息通过转换确认。在上述 3 个方案中，我们采用同样的方法进行改进，通过阈下信道传递秘密信息，即，转换信息。我们传递的秘密信息将是环签名中实际签名者对同一信息的安全的普通签名 $\mathrm{sign}(m)$，并将其与实际签名者的身份 ID_s 作用于某一密码哈希函数 H，得到 $r'=H(\mathrm{sign}(m),\mathrm{ID}_s)$。

在 Zhang-Liu-He 基于 Nyberg-Rueppel 的可转换环签名方案中，环签名过程改为：签名者 U_s 选取 $a\in_R Z_q$，$y_i\in_R Z_q,(1\leq i\leq n,i\neq s)$，先计算 $\sigma=$

$\alpha^{-a} \bmod p$，$c_{i+1} = h(r', m, \sigma)$；再依次计算，$c_{i+1} = h(r', m, \alpha^{y_i} P^{c_i} \bmod p)$，$i = s+1, \cdots, n, 1, \cdots, s-1$，其中 $c_{n+1} = c_1$；最后计算 $y_s = a + s_s c_s \bmod q$，关于消息 m 的环签名为 $(r', p_1, \cdots, p_n; c_1; y_1, \cdots, y_n)$。确认过程改为：验证者计算 $c_{i+1} = h(r', m, \alpha^{y_i} P_i^{c_i} \bmod p)$，其中 $i = 2, 3, \cdots, r$；如果 $c_{r+1} = c_1$，接受；否则，拒绝。环签名转换和转换验证改为：签名者 U_s 向验证者出示 $(\mathrm{sign}(m), \mathrm{ID}_s)$，验证者检测 $\mathrm{Verify}(\mathrm{sign}(m)) = "T"$ 是否成立。如果成立，接受；否则，拒绝。

在 Gan-Chen 可转换环签名方案和 Wang-Zhang-Ma 无证书环签密方案中，将 $r' = H(\mathrm{sign}(m), \mathrm{ID}_s)$ 代替其中的 t 即可，实际签名者的秘密信息为 $(\mathrm{sign}(m), \mathrm{ID}_s)$。

改进方案的安全性分析：由于 H 为密码哈希函数，在某个消息的具体的可转换环签名产生后，由于无法得到 $r' = H(\mathrm{sign}(m), \mathrm{ID}_s)$ 的原像，环中其它成员不能产生相应的转换信息通过转换确认。又由于 $\mathrm{sign}(m)$ 是安全的，$(\mathrm{sign}(m), \mathrm{ID}_s)$ 不能被环中其它成员仿真或伪造。所以，改进的可转换环签名(密)方案的可转换性能够得到保证。

6　结束语

本文对文献[10,11,14]提出的可转换环签名(密)方案进行了分析，给出了可转换性攻击和不可否认性方法。通过对上述 3 个方案的分析，总结了原方案存在缺陷的原因，并给出了安全的可转换环签名方案需满足的两个条件。针对原方案出现的缺陷，对原签名方案进行了改进，使得改进后的可转换环签名(密)方案是安全的。

参 考 文 献

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

[2] Masayuki abe, Miyako ohkubo, and Koutarou suzuki. 1-out-of-n signatures from a variety of keys. *IEICE Trans. on Fundamentals*, 2004, E87-A: 131–140.

[3] Liu Y W, Liu J K, Mu Y, Susilo W, and Wong S. Revocable ring signature. *Journal of Computer Science and Technology*, 2007, 22(6): 785–794.

[4] Au M H, Liu J K, Susilo W, and Yuen T H. Certificate based (linkable) ring signature. ISPEC 2007, Berlin: Springer-Verlag, 2007, LNCS 4464: 79–92.

[5] Zhang Lei, Zhang Futai, and Wu Wei. A provably secure ring signature scheme in certificateless cryptography. ProvSec 2007, Berlin: Springer-Verlag, LNCS 4784: 103–121.

[6] Rivest R L, Shamir A, and Tauman Y. How to leak a secret : Theory and Applications of Ring Signatures. Essays in Memory of Shimon Even 2006: 164–186.

[7] 范安东, 孙琦, 张杨松. 基于环签名的匿名电子投票方案. 四川大学学报(工程科学版), 2008, 40(1): 113–117.
Fan An-dong, Sun Qi, and Zhang Yang-song. The scheme of anonymous electronic voting based on ring signature. *Journal of Sichuan University* (*Engineering Science Edition*), 2008, 40(1): 113–117.

[8] 苗付友, 王行甫, 苗辉, 熊焰. 一种支持悬赏的匿名电子举报方案. 电子学报, 2008, 36(2): 320–324.
Miao Fu-you, Wang Xing-fu, Miao Hui, and Xiong Yan. An anonymous e-prosecution scheme with reward support. *Acta Electronica Sinica*, 2008, 36(2): 320–324.

[9] Lü Jiqiang and Wang Xinmei. Verifiable ring signature. The 9th International Conference on Distribted Multimedia Systems, USA, 2003: 663–667.

[10] Zhang Changlun, Liu Yun, and He Dequan. A new verifiable ring signature scheme based on Nyberg-Rueppel scheme. ICSP2006, Beijing 2006, 4: 16–20.

[11] Gan Zhi and Chen Kefei. A new verifiable ring signature scheme. *Acta Scientiarum Naturalium Universitatis Sunyatseni*, 2004, 143, Suppl1(2): 132–134.

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

[13] Gao Wei, Wang Guilin, Wang Xueli, and Xie Dongqing. Controllable ring signatures. WISA 2006, Berlin: Springer-Verlag, 2007, LNCS4298: 1–14.

[14] Wang Lingling, Zhang Guoyin, and Ma Chunguang. A secure ring signcryption scheme for private and anonymous communication. 2007 IFIP International Conference on Network and Parallel Computing–Workshops, Harbin, 2007: 107–111.

王化群：　男，1974年生，博士，副教授，硕士生导师，主要研究方向为信息安全.

郭显久：　男，1963年生，博士，教授，硕士生导师，主要研究方向为图像处理.

于　红：　女，1968年生，博士，教授，硕士生导师，主要研究方向为可信计算.

彭玉旭：　男，1977年生，博士，讲师，主要研究方向为移动通信、无线传感器网络.