第 37 卷 第 24 期
Vol.37 No.24

计 算 机 工 程
Computer Engineering

2011 年 12 月
December 2011

• 安全技术 •

文章编号：1000—3428(2011)24—0106—03 文献标识码：A 中图分类号：TP309

一种改进的前向安全环签名方案

黄明军，杜伟章

(长沙理工大学计算机与通信工程学院，长沙 410114)

摘 要：对已有前向安全环签名方案进行安全性分析，指出其不具备前向安全性，存在多种安全隐患。为此，提出一种改进的前向安全环签名方案。通过改变环签名算法，将密钥更新和环签名相结合，克服原方案中用常量进行环签名的缺陷。安全性与效率分析表明，改进方案具有前向安全性、无条件匿名性、抗伪造性，且签名效率较高。

关键词：前向安全；环签名；离散对数问题；密钥更新算法

Improved Forward-security Ring Signature Scheme

HUANG Ming-jun, DU Wei-zhang

(College of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410114, China)

【Abstract】This paper analyzes the existing security of the forward secure ring signature scheme, points out that the scheme exists security omission because of lacking forward security. Aiming at these problems, it proposes an improved forward-security ring signature scheme. The defect that the original scheme is signed with constant is overcome by changing the algorithm of ring signature. The algorithm combines the updating secret key and ring signature. The analysis of security and efficiency shows that the improved scheme has forward security, unconditional anonymity and resisting forging attack, as well as higher signing efficiency.

【Key words】forward-security; ring signature; Discrete Logarithm(DL) problem; secret key evolution algorithm

DOI: 10.3969/j.issn.1000-3428.2011.24.035

1 概述

前向安全[1]的本质是对数字签名风险的控制，因此，在前向安全特性提出后，如何改进前向安全特性并将其更好地应用到各类数字签名中，成为信息安全领域研究的热点。文献[2]在匿名泄漏秘密的背景下提出环签名的概念[2]。随后，许多学者在标准模型下展开了对环签名体制的研究，设计出了不少在标准模型下可证安全的环签名方案。文献[3]针对环签名的密钥泄漏问题，将前向安全特性和环签名结合，提出前向安全的环签名和密钥封装的环签名。文献[4]提出标准模型下基于双线性对的前向安全环签名方案(Forward-secure Ring Signature Scheme based on Bilinear Pairing, FSRS-BP)，然而该方案并不真正具备前向安全性。本文指出其不具备前向安全性的根本原因并进行了改进，提出一种改进的前向安全环签名方案，改进方案的安全性基于离散对数(Discrete Logarithm, DL)问题和模平方剩余问题。

2 FSRS-BP 方案的安全性分析

2.1 FSRS-BP 方案

设环中有 n 个成员 $U=\{U_1,U_2,\cdots,U_n\}$，方案步骤如下：

(1)系统设置算法(SET-BP)：选择双线性对 $e:G\times G\to G_T$，$|G|=|G_T|=N$，N 为合数，且 $G=\langle P\rangle=\langle R\rangle$。选择单向哈希函数 $H_i(.):\{0,1\}^*\to Z_N^*$，$1\leqslant i\leqslant n$。签名密钥的有效期分为 T 个时段。系统公共参数为 $\{e,P,R,H_1,\cdots,H_n,T\}$。

(2)初始密钥生成算法(IKG-BP)：用户 U_i 任选 $x_{i,0},y_{i,0}\in_R Z_N^*$，计算 $u_i=x_{i,0}^{2^T}R$、$v_i=y_{i,0}^{2^T}R$。U_i 的验证公钥为 $PK_i=\{u_i,v_i\}$，初始私钥为 $SK_{i,0}=\{x_{i,0},y_{i,0}\}$。

(3)密钥更新算法(KE-BP)：系统一旦进入 $j(1\leqslant j\leqslant T)$ 时段，用户 U_i 使用第 $j-1$ 时段的私钥 $SK_{i,j-1}=\{x_{i,j-1},y_{i,j-1}\}$，计算 $x_{i,j}=x_{i,j-1}^2 \bmod N$、$y_{i,j}=y_{i,j-1}^2 \bmod N$。此时，立刻从系统中删除第 $j-1$ 时段的私钥 $SK_{i,j-1}$。系统在第 j 时段的签名密钥对为 $(SK_{i,j},PK_i)$。

(4)环签名算法(SIG-BP)：用户 U_s 代表群体对消息 m 进行签名。系统现在进入第 j 时段。用户 U_s 执行如下操作：

1)对于 $i\in\{1,2,\cdots,n\}\setminus s$，选择 $z_i\in_R Z_N^*$，计算 $\sigma_i=z_iR$；

2)对于 $i\in\{1,2,\cdots,n\}$，选择 $r_i\in_R Z_N^*$，通过以下式计算：

$$P=W+[\sum_{i\in\{1,2,\cdots,n\}\setminus s}z_i\cdot(u_i+H_i(m)R+r_iv_i)]$$

3)通过 $SK_{i,j}=\{x_{i,j},y_{i,j}\}$ 计算：

$$\sigma_s=(1/(x_{s,j}^{2^{T-j}}+H_s(m)+r_sy_{s,j}^{2^{T-j}}))W$$

输出环签名 $\{(\sigma_1,r_1),(\sigma_2,r_2),\cdots,(\sigma_n,r_n)\}$。

(5)签名验证算法(VER-BP)：接收方收到消息 m 的环签名 $\{(\sigma_1,r_1),(\sigma_2,r_2),\cdots,(\sigma_n,r_n)\}$，用 n 个成员的公钥验证等式：$\prod_i^n[e(\sigma_i,(u_i+H_i(m)R+r_iv_i))]=e(P,R)$，若等式成立则接受签名，否则拒绝。

2.2 安全性分析

FSRS-BP 方案安全性分析如下：

(1)该方案不具备前向安全性。对于用户 U_s 而言，第 $j(1\leqslant j\leqslant T)$ 时段的签名 $\sigma_s=(1/(x_{s,j}^{2^{T-j}}+H_s(m)+r_sy_{s,j}^{2^{T-j}}))W$，

作者简介：黄明军(1986－)，男，硕士研究生，主研方向：密码学；杜伟章，教授、博士后

收稿日期：2011-06-27 **E-mail：**huangmingjun2008@163.com

根据密钥更新算法 $x_{s,j}=x_{s,0}^{2^j}\Rightarrow x_{s,j}^{2^{T-j}}=x_{s,0}^{2^T}$、$y_{s,j}=y_{s,0}^{2^j}\Rightarrow y_{s,j}^{2^{T-j}}=y_{s,0}^{2^T}$，可以得到 $\sigma_s=(1/(x_{s,0}^{2^T}+H_s(m)+r_s y_{s,0}^{2^T}))W$，$x_{s,0}^{2^T}$ 和 $y_{s,0}^{2^T}$ 是与时段 j 无关的常量，而 $W=P-[\sum_{i\in\{1,2,\cdots,n\}\setminus s}z_i(u_i+H_i(m)R+r_iv_i)]$ 也与时段 j 无关，因此，用户 U_s 生成的环签名 $\{(\sigma_1,r_1),(\sigma_2,r_2),\cdots,(\sigma_n,r_n)\}$ 与时段 j 无关，即任一时段生成的环签名在整个有效周期内都是有效的，这违背了前向安全性的原则。

(2)该方案的安全隐患如下：

1)攻击者可以欺骗验证者。假设当前时段为第 j 时段，攻击者截获用户第 j 时段的环签名 $\{(\sigma_1,r_1),(\sigma_2,r_2),\cdots,(\sigma_n,r_n)\}$，然后转发给验证者，并声称这是第 $i(1\leqslant i<j)$ 时段的签名，或将第 i 时段的签名发给验证者，声称这就是第 j 时段的签名，而验证者却察觉不了，从而欺骗成功。

2)密钥更新不但没有意义，反而给了敌手更多的机会。只要用户 U_s 任一时段 $j(1\leqslant j\leqslant T)$ 的密钥 $SK_{s,j}$ 泄漏了，攻击者便可求出用户 U_s 的真正签名密钥 $SK_s=(x_{s,0}^{2^T},y_{s,0}^{2^T})$，从而伪造用户 U_s 的签名。

3 改进方案及其安全性分析

3.1 改进方案

设环中有 n 个成员 $U=\{U_1,U_2,\cdots,U_n\}$，其中，U_i 对应身份为 ID_i。改进方案步骤如下：

(1)系统设置算法(SET-BP)：定义群 G_1 为加法循环群，G_2 为乘法循环群(阶数均为素数 N)，双线性对 $e:G_1\times G_1\to G_2$，P 是 G_1 的生成元，选择单向哈希函数 $H:\{0,1\}^*\times\{0,1\}^*\times\{0,1\}^*\times\{0,1\}^*\times G_2\to Z_N^*$，签名密钥的有效期分为 T 个时段，计算 $g=\{P,P\}$，发布系统公共参数 $\{e,P,g,H,T\}$。

(2)初始密钥生成算法(IKG-BP)：用户 U_i 任选 $x_{i,0}\in Z_N^*$，计算公钥 $PK_i=x_{i,0}^{2^T}P\bmod N$，初始私钥为 $SK_{i,0}=x_{i,0}$。

(3)密钥更新算法(KE-BP)：系统在第 $j(1\leqslant j\leqslant T)$ 时段，用户 U_i 使用第 $j-1$ 时段的私钥 $SK_{i,j-1}=x_{i,j-1}$，计算 $SK_{i,j}=x_{i,j}=x_{i,j-1}^2\bmod N$，然后从系统中删除第 $j-1$ 时段的私钥 $SK_{i,j-1}$。第 j 时段的签名密钥对为 $\{SK_{i,j},PK_i\}$，其中，$SK_{i,j}=x_{i,j}=x_{i,0}^{2^j}\bmod N$；$PK_i=x_{i,0}^{2^T}P\bmod N$。

(4)环签名算法(SIG-BP)：用户 U_s 希望代表群体对消息 m 进行签名，系统进行到第 j 时段，用户 U_s 执行如下操作：

1)对于 $i\in\{1,2,\cdots,n\}/s$，选择秘密随机数 $r_i\in Z_N^*$，计算 $R_i=g^{r_i}\bmod N$；

2)选择秘密随机数 k、r_s、$\mu\in Z_N^*$，计算：

$$\omega=SK_{s,j}k^{\mu}\bmod N=x_{s,j}k^{\mu}\bmod N$$

$$h_i=H(m\|\omega\|ID_i\|PK_i\|R_i)\bmod N(i\in\{1,2,\cdots,n\}\setminus s)$$

$$R_s=g^{r_s}\prod_{i\in\{1,\cdots,n\}\setminus s}e(\omega^{-2^{T-j}}P,PK_i)^{-h_i}\bmod N$$

若 $R_s=1_{G_2}$ 或 $R_s=R_i(s\neq i)$，只需重新选择 r_s 避免冲突；

3)计算：

$$h_s=H(m\|\omega\|ID_s\|PK_s\|R_s)\bmod N$$

$$v=(\sum_{i=1}^{n}r_i+h_sk^{-2^{T-j}\mu})\bmod N$$

4)输出关于消息 m 的环签名：$\sigma=\{\omega,v,R_1,R_2,\cdots,R_n,j\}$。

(5)签名验证算法(VER-BP)：接收方收到关于消息 m 的环签名 $\sigma=\{\omega,v,R_1,R_2,\cdots,R_n,j\}$，根据公钥集 $PK=\{PK_1,PK_2,\cdots,PK_n\}$，执行下列算法：

1)计算 $h_i=H(m\|\omega\|ID_i\|PK_i\|R_i)\bmod N(1\leqslant i\leqslant n)$；

2)用等式 $\prod_{i=1}^{n}R_ie(\omega^{-2^{T-j}}P,PK_i)^{h_i}\bmod N=e(vP,P)\bmod N$ 对签名进行验证，若等式成立则接受签名，否则拒绝。

3.2 改进方案的安全性分析

3.2.1 正确性分析

方案的正确性分析如下：

$$\prod_{i=1}^{n}R_ie(\omega^{-2^{T-j}}P,PK_i)^{h_i}\bmod N=R_se(\omega^{-2^{T-j}}P,PK_s)^{h_s}\times\prod_{i\in\{1,2,\cdots,n\}\setminus s}R_ie(\omega^{-2^{T-j}}P,PK_i)^{h_i}=$$

$$e(\omega^{-2^{T-j}}P,PK_s)^{h_s}(g^{r_s}\prod_{i\in\{1,\cdots,n\}\setminus s}e(\omega^{-2^{T-j}}P,PK_i)^{-h_i})\times\prod_{i\in\{1,2,\cdots,n\}\setminus s}g^{r_i}e(\omega^{-2^{T-j}}P,PK_i)^{h_i}\bmod N=$$

$$(\prod_{i}^{n}g^{r_i})e(\omega^{-2^{T-j}}P,PK_s)^{h_s}\bmod N=$$

$$e(\sum_{i=1}^{n}r_iP,P)e(h_sk^{-2^{T-j}\mu}P,P)\bmod N=$$

$$e((\sum_{i=1}^{n}r_i+h_sk^{-2^{T-j}\mu})P,P)\bmod N=$$

$$e(vP,P)\bmod N$$

因此，本环签名是正确的，即 $\sigma=\{\omega,v,R_1,R_2,\cdots,R_n,j\}$ 为有效的前向安全环签名。

3.2.2 前向安全性分析

从签名参数 $\omega=x_{s,j}k^{\mu}\bmod N$ 中可以看出本方案的实际签名私钥不再是常量，而是随时段 j 不断更新的 $SK_{s,j}=x_{s,j}$，做到了将密钥更新和环签名真正结合起来，从而改进后的环签名方案具有前向安全性。

3.2.3 无条件匿名性分析

仅从改进方案的环签名 $\sigma=\{\omega,v,R_1,R_2,\cdots,R_n,j\}$ 来看，任何成员的地位都是一样的，因此，无法确定具体签名人。从环签名算法来看，对于 $i\in\{1,2,\cdots,n\}\setminus s$，$R_i=g^{r_i}\bmod N$，因为 r_i 是随机选取的，所以 R_i 是随机的。而 $\omega=x_{s,j}k^{\mu}\bmod N$ 和随机数 μ 相关，$R_s=g^{r_s}\prod_{i\in\{1,\cdots,n\}\setminus s}e(\omega^{-2^{T-j}}P,PK_i)^{-h_i}$ 和随机数 r_s 相关，$v=(\sum_{i=1}^{n}r_i+h_sk^{-2^{T-j}\mu})\bmod N$ 和随机数 μ 相关，所以 ω、R_s、V 可以看作是随机的，攻击者得不到签名者 U_s 的任何信息，猜对真正签名者的概率为 $1/n$，因此，改进后的方案满足无条件匿名性。

3.2.4 不可伪造性分析

下面通过一个定理证明改进后的方案可抵抗自适应选择消息攻击下的存在性伪造。

定理 在随机预言机模型下，设 A 是自适应选择消息和身份攻击下的超级攻击者[5]，如果在时间 t 内，至多做 q_U 次生成用户询问，q_H 次 H 询问，q_{PK} 次公钥询问，q_x 次私钥询问，q_σ 次签名询问后，能以不可忽略的概率 ε 攻破改进后的方案，那么存在一个算法 B，在时间：

$$t'\leqslant 2(t+q_Ut_U+q_Ht_H+q_{PK}t_{PK}+q_xt_x+q_\sigma t_\sigma)$$

内解决 DL 问题，其中，t_U、t_H、t_{PK}、t_x、t_σ 分别表示一次生成用户询问、H 询问、公钥询问、私钥询问和签名询问所用的时间。

证明：令 B 是加法循环群 G_1 上的 DL 问题解决者，给定一个 DL 问题的随机实例 $(P,X=aP\bmod N)$，B 的目标是计算

出 a。A 的攻击的目标身份是 ID^*，最终他能在时间 t 内，以不可忽略的概率 ε，伪造出关于消息 m 的合法环签名 $\sigma=\{\omega,v,R_1,R_2,\cdots,R_n,j\}$。下面将证明 B 可利用 A 的能力，在 t' 时间内以不可忽略的概率 ε' 解决给定的 DL 问题。

建立系统参数：B 把系统参数 $\{e,P,g,H,T\}$ 发送给 A。

攻击：B 把哈希函数 H 作为随机预言机，A 可以作生成用户询问、哈希 H 询问、公钥询问、私钥询问和签名询问，假设 A 的询问都是不同的。模拟机询问如下：

(1)生成用户询问：B 保持一个列表 $L_1=\{ID_i,x_{i,0}\}$，初始为空，设 ID_i 是 A 的第 i 次询问。当收到 A 的生成用户询问，B 判断 $ID_i=ID^*$ 是否成立，若 $ID_i=ID^*$，则终止，若 $ID_i\neq ID^*$，则查表 L_1，若 ID_i 在表 L_1 中，则返回相应的 $(ID_i,x_{i,0})$ 给 A，否则随机选择 $x_{i,0}\in Z_N^*$（$x_{i,0}$ 以前未出现在表 L_1 中），返回 $(ID_i,x_{i,0})$ 给 A 并将其添加到表 L_1 中，$i\in\{1,2,\cdots,q_U\}$。

(2)私钥询问：假设当前前向安全环签名时段为第 j 时段，B 保持一个列表 $L_2=\{ID_i,x_{i,j}\}$，初始为空。当收到 A 的私钥询问，B 判断 $ID_i=ID^*$ 是否成立，若 $ID_i=ID^*$，则终止，若 $ID_i\neq ID^*$，则查表 L_2，若 ID_i 在表 L_2 中，则返回相应的 $(ID_i,x_{i,j})$ 给 A，否则查表 L_1，得到相应的 $x_{i,0}$，计算 $x_{i,j}=x_{i,0}^{2^j}\bmod N$，返回 $(ID_i,x_{i,j})$ 给 A 并将其添加到表 L_2 中。

(3)公钥询问：B 保持一个列表 $L_3=\{ID_i,PK_i\}$，初始为空。当收到 A 的公钥询问，B 判断 $ID_i=ID^*$ 是否成立，若 $ID_i=ID^*$，则令 $PK_{ID^*}=X=aP\bmod N$，将 (ID^*,PK_{ID^*}) 返回给 A 并将其添加到表 L_3 中，若 $ID_i\neq ID^*$，B 查表 L_1 获得相应的 $x_{i,0}$，计算 $PK_i=x_{i,0}^{2^T}P\bmod N$，返回 (ID_i,PK_i) 给 A，并将其添加到表 L_3 中。

(4) H 询问：B 保持一个列表 $L_4=\{ID_i,h_i\}$，初始为空。当收到 A 的 H 询问，B 查表 L_4，若 ID_i 在表 L_4 中，返回相应的 h_i 给 A，否则，随机选择 $h_i\in Z_N^*$（h_i 以前未出现在表 L_4 中），返回 (ID_i,h_i) 给 A，并将其添加到表 L_4 中。

(5)签名询问：当 B 收到 A 的签名询问时，B 先从表 L_3 中获得成员的公钥，接下来按如下步骤回答：

1)任选 $s\in\{1,2,\cdots,n\}$，对任意的 $i\in\{1,2,\cdots,n\}\setminus s$，随机选取 $r_i\in Z_N^*$，计算 $R_i=g^{r_i}\bmod N$，任选 $\omega\in Z_N^*$，计算 $h_i=H(m\|\omega\|ID_i\|PK_i\|R_i)\bmod N$；

2)任选 v，$h_s\in Z_N^*$，计算：

$$R_s=e((v-\sum_{i\in\{1,2,\cdots,n\}\setminus s}r_i)P,P)\prod_{i=1}^{n}e(\omega^{-2^{T-j}}P,PK_i)^{-h_i}$$

若 $R_s=1_{G_2}$ 或 $R_s=R_i(s\neq i)$，只需重新选择 v 避免冲突。置 $h_s=H(m\|\omega\|ID_s\|PK_s\|R_s)$；

3)输出环签名 $\sigma=\{\omega,v,R_1,R_2,\cdots,R_n,j\}$。

伪造：A 能在 t' 时间内以不可忽略的概率 ε' 输出用户身份为 ID^*，关于消息 m 的有效环签名 $\sigma=\{\omega,v,R_1,R_2,\cdots,R_n,j\}$，由分叉引理可知，$A$ 能够生成消息 m 另一个有效环签名 $\sigma'=\{\omega,v',R_1,R_2,\cdots,R_n,j\}$，不妨设 $PK_s=PK_{ID^*}=aP\bmod N$，其中 $h_s\neq h_s'$，$h_i=h_i'$ $(i\in\{1,2,\cdots,n\}\setminus s)$。这样就得到了 2 个有效的环签名，于是有：

$$e(vP,P)\bmod N=\prod_{i=1}^{n}R_i e(\omega^{-2^{T-j}}P,PK_i)^{h_i}\bmod N=$$
$$R_s e(\omega^{-2^{T-j}}P,PK_{ID^*})^{h_s}\times\prod_{i\in\{1,2,\cdots,n\}\setminus s}R_i e(\omega^{-2^{T-j}}P,PK_i)^{h_i}\bmod N$$
$$e(v'P,P)\bmod N=\prod_{i=1}^{n}R_i e(\omega^{-2^{T-j}}P,PK_i)^{h_i'}\bmod N=$$
$$R_s e(\omega^{-2^{T-j}}P,PK_{ID^*})^{h_s'}\times\prod_{i\in\{1,2,\cdots,n\}\setminus s}R_i e(\omega^{-2^{T-j}}P,PK_i)^{h_i'}\bmod N$$

两式相除得：

$$e((v-v')P,P)\bmod N=e(\omega^{-2^{T-j}}P,PK_{ID^*})^{h_s-h_s'}\bmod N\Leftrightarrow$$
$$e((v-v')P,P)\bmod N=e(a\omega^{-2^{T-j}}(h_s-h_s')P,P)\bmod N\Leftrightarrow$$
$$(v-v')\bmod N=a\omega^{-2^{T-j}}(h_s-h_s')\bmod N\Leftrightarrow$$
$$a=(v-v')\omega^{2^{T-j}}(h_s-h_s')^{-1}\bmod N$$

这样 B 利用 A 就求出了椭圆曲线上 DL 问题的一个解，出现矛盾。因此，改进方案在随机预言机模型下可抵抗敌手 A 的自适应选择消息攻击下的存在性伪造。

4 改进方案的效率分析

下面就计算代价和是否具备前向安全特性 2 个方面对改进方案和原方案进行比较，其中，E、M、A、H 分别代表方案中模素数 N 的双线性运算、幂运算、乘法运算和哈希运算。2 种方案的性能比较如表 1 所示。

表 1 2 种方案的性能比较

方案	签名运算量	验证运算量	总运算量	前向安全性
原方案	2M+(4n-2)A+nH	(n+1)E+2nA+P+nH	(n+1)E+2M+(6n-2)A+2nH	无
本文方案	E+(n+2)M+2A+nH	2E+M+nA+nH	3E+(n+3)M+(n+2)A+2nH	有

可以看出，与原方案相比，本文方案在运算量上最显著的一个特征就是减少了双线性运算，原方案用到了 n+1 个双线性运算，改进方案只用到了 3 个，而最费时的就是双线性运算，所以当成员数 n 越大时，本文签名方案的效率优势就越明显。

5 结束语

本文针对文献[4]的基于双线性对的前向安全环签名方案提出一种改进方案，解除了原方案的安全隐患，简化了签名过程，提高了签名效率。下一阶段的重点是研究新的算法，将密钥更新和环签名过程更好地结合，从而设计出更安全且具有实用性的前向安全环签名方案。

参考文献

[1] Anderson R. Two Remarks on Public Key Cryptology[C]//Proc. of ACM Conference on Computer and Communications Security. Zurich, Switzerland: [s. n.], 1997.

[2] Rivest R L, Shamir A, Tauman Y. How to Leak a Secret[C]//Proc. of Cryptology-ASIACRYPT'01. Berlin, Germany: [s. n.], 2001.

[3] Liu J K, Wong D S. Solutions to Key Esposure Problem in Ring Signature[J]. International Journal of Network Security, 2008, 6(2): 170-180.

[4] 王玲玲, 张国印, 马春光. 标准模型下基于双线性对的前向安全环签名方案[J]. 电子与信息学报, 2009, 31(2): 448-452.

[5] 王 颖, 肖 俊, 王蕴红. 数字水印原理与技术[M]. 北京: 科学出版社, 2007.

编辑 顾姣健