第38卷 第11期 计 算 机 工 程 2012年6月
Vol.38 No.11 Computer Engineering June 2012

·安全技术· 文章编号：1000—3428(2012)11—0133—03 文献标识码：A 中图分类号：TP309.2

一个改进的前向安全盲签名方案

何俊杰，王 娟，祁传达

(信阳师范学院数学与信息科学学院，河南 信阳 464000)

摘 要：张席等提出的盲签名方案(武汉大学学报：理学版，2011年第5期)在盲签名生成阶段存在模运算错误，不满足可验证性，攻击者可以生成任意消息的盲签名，不满足不可伪造性。为此，通过优化系统参数、修正模数运算和减少签名数据，提出一种改进的盲签名方案。安全性和效率分析结果表明，改进方案具有不可伪造性、盲性和前向安全性，且计算效率较高。

关键词：盲签名；离散对数；二次剩余；前向安全；不可伪造性；盲性

Improved Forward-secure Blind Signature Scheme

HE Jun-jie, WANG Juan, QI Chuan-da

(College of Mathematics and Information Science, Xinyang Normal University, Xinyang 464000, China)

【Abstract】 In the forward-secure blind signature scheme proposed by Zhang Xi et al, there is an error in module arithmetic in blind signature generation phase, so the scheme does not meet verifiability; the attacker can generate blind signature of any messages, so it does not satisfy unforgeability. This paper proposes an improved blind signature scheme by optimizing the system parameters, modifying the module arithmetic and reducing the signature data. Security and efficiency analysis results show that the improved scheme satisfies unforgeability, blindness and forward-security, and has high calculating efficiency.

【Key words】 blind signature; discrete logarithm; quadratic residues; forward-secure; unforgeability; blindness

DOI: 10.3969/j.issn.1000-3428.2012.11.041

1 概述

随着计算机网络和信息技术的飞速发展，数字签名已经成为保证信息完整性和实现网络身份认证的重要手段。文献[1]为实现不可跟踪的支付系统首次提出了盲签名的概念。使用盲签名技术可以有效地保护用户的隐私，使签名人在不知道被签文件具体内容的情况下对文件进行签名。文献[2]首次提出前向安全的概念。前向安全数字签名要求即使对手盗得当前时段的签名密钥，也不能伪造与密钥被盗前时段相关的数字签名。其本质思想是尽可能减少由于密钥泄露所带来的对系统安全的影响和损失。自文献[2]将前向安全的性质引入数字签名之后，具有前向安全特性的签名方案[3]也相继出现。文献[4]提出了前向安全盲签名方案，它是基于强 RSA 假设的。文献[5]基于文献[6]的主密钥方案和文献[1]的盲签名方案，提出了新的前向安全盲签名方案，其中，密钥是预先设置并存储的，个数与周期 T 相等，存储开销大且增加了泄露的风险。文献[7]基于双线性映射和 Gap Diffie-Hellman 问题，运用树结构构造方法提出了前向安全盲签名方案的另一个思路，但结构的复杂性导致方案非常复杂，难以实现。文献[8]构造了一个基于 Schnorr 盲签名的前向安全盲签名方案，声称其具有不可伪造性、盲性和前向安全性。本文指出，文献[8]的方案存在以下安全缺陷：(1)盲签名生成阶段存在模运算错误，使得方案不满足不可验证性；(2)攻击者能生成任意消息的盲签名，即方案不满足不可伪造性。并对方案进行改进，使其在避免上述安全缺陷的同时，运算效率得到提高。

2 相关知识

2.1 前向安全盲签名

前向安全数字签名的基本思想就是把整个签名的有效时间分成 T 个时段，在不同时段内使用不同的签名密钥产生签名，而用于验证的签名公钥 PK 在整个签名有效时间内都保持不变。每个时段的最后签名以一个单向的模式，从前一时段 $j-1$ 的密钥 SK_{j-1} 得到当前时段 j 的密钥 SK_j，并且安全地删除前一时段的密钥 SK_{j-1}。

一个前向安全盲签名方案是一个密钥进化数字签名方案，主要包括以下4个算法[4]：

(1)密钥生成算法

该算法为概率多项式时间算法。输入安全参数 k 和时间周期数 T 等，输出系统参数 $param$、公钥 PK 和初始私钥 SK_0。

(2)密钥更新算法

该算法为确定性或概率算法。输入前一周期的私钥 SK_{j-1}，输出当前周期的私钥 SK_j。

(3)盲签名生成算法

该算法为用户与签名者之间的交互协议。签名者为概率图灵机，使用当前私钥 SK_j 与用户进行3步交互，最后为用户给出消息 M 的盲签名。用户也为概率图灵机，以消息 M 和公钥 PK 作为输入，与签名者进行交互。在签名完成后，输出时间周期 j、消息 M 及签名 $sig(M)$。$(j, sig(M))$ 即为最终盲签名。

(4)签名验证算法

该过程为确定性过程。输入公钥 PK、消息 M 和签名

基金项目：河南省自然科学基金资助项目(102102210242)；河南省教育厅科学技术研究基金资助重点项目(12A520034)；信阳师范学院青年基金资助项目(2011076)

作者简介：何俊杰(1981－)，男，讲师、硕士，主研方向：信息安全；王 娟，讲师、博士；祁传达，教授、博士

收稿日期：2011-10-09 **E-mail**：hejj99@163.com

$(j, sig(M))$，输出验证通过与否的0/1判断。

2.2 相关数学难题

(1)离散对数难题

设 p 是一个大素数，g 是 Z_p^* 的生成元。已知 $y\in Z_p^*$，求解 $x\in Z_p^*$，使得 $y=g^x \bmod p$ 是困难的。

(2)二次剩余计算难题

在不知道 n 的分解时，已知 $y=x^2 \bmod n$，求 x 是困难的。该数学难题等价于大数分解问题。

3 文献[8]的前向安全盲签名方案

3.1 密钥生成

系统首先选取2个大素数 p、q，其中，$p\geqslant 2^{512}$；$q\geqslant 2^{160}$；$q\mid(p-1)$；$g\in Z_q^*$，且满足 $g^q\equiv 1(\bmod p)$，即 g 是 Z_q^* 的生成元；$H:\{0,1\}^*\rightarrow Z_p^*$ 为安全的哈希函数。

将签名的有效时间划分为 T 个周期 $1,2,\cdots,T$，只有在 T 个周期内，签名者对消息的签名才是有效的。

随机选取初始私钥 $s_0(1<s_0<q)$，计算公钥 $Y=g^{s_0 2^T}$，公开 (H,p,g,T,Y)。

3.2 密钥更新

当时间从前一周期进入当前周期时，签名者根据前一周期密钥更新得到当前周期密钥。设当前周期为 j，签名者按以下步骤更新密钥：(1)若 $j>T$，则 s_j 设为空串，算法终止。(2)若 $1\leqslant j\leqslant T$，则计算 j 周期的密钥 $s_j=s_{j-1}^2 \bmod(p-1)$ 并删除 s_{j-1}。

3.3 盲签名生成

在 j 周期，消息 m 的签名按以下步骤生成：

(1)盲化(Blind)

签名者选择随机数 $k\in Z_p^*$，计算 $R'=g^k \bmod p$，并将 R' 发送给消息 m 的请求者。

用户收到 R' 后，随机选择盲化因子 $\alpha,\beta,\gamma\in Z_p^*$，计算：

$$R=R'^{\alpha}g^{\beta}Y^{\gamma} \bmod p$$

$$e=H(R,m)$$

$$e'=\alpha^{-1}(e-\gamma)\bmod(p-1)$$

并发送 e' 给签名者。

(2)签名(Sign)

签名者收到 e' 后，计算：

$$y'=g^{s_j} \bmod p$$

$$S'=k-e'(s_j^{2^{T-j}}+s_j)\bmod p$$

然后将 (y', S') 发送给用户。

(3)去盲(Umblind)

用户收到 (y', S') 后，计算：

$$y=(y')^{e-\gamma} \bmod p$$

$$S=\alpha S'+\beta \bmod(p-1)$$

则消息 m 的签名为 $sig(m)=(e,S,y)$。

3.4 签名验证

首先判断签名 $(m,j,(e,S,y))$ 是否在签名者的签名有效期内，若 $j>T$，则签名无效，若 $1\leqslant j\leqslant T$，则计算：$R^*=Y^e g^S y \bmod p$，$e^*=H(R^*,m)$。如果等式 $e^*=e$ 成立，则签名 $sig(m)=(e,S,y)$ 有效，否则，签名无效。

4 文献[8]方案存在的问题

文献[8]分析证明了其方案具有不可伪造性、盲性和前向安全性。本文对该方案分析后发现，其中存在的模运算错误影响了盲签名的验证；同时，即使修正盲签名过程中的模运算，方案也不能抵抗伪造攻击，攻击者可以伪造任意消息的盲签名。

4.1 模运算错误

在盲签名过程中，$S'=k-e'(s_j^{2^{T-j}}+s_j)\bmod p$，可设：$S'=k-e'(s_j^{2^{T-j}}+s_j)+xp$，其中，$x\in \mathbf{Z}$。当 $(p-1)\nmid \alpha x$ 时，有：

$$R^*=Y^e g^S y \bmod p=Y^e g^{\alpha S'+\beta}(y')^{e-\gamma} \bmod p=$$

$$Y^e g^{\alpha(k-e'(s_j^{2^{T-j}}+s_j)+xp)+\beta}(y')^{e-\gamma} \bmod p=$$

$$Y^e(g^k)^{\alpha}\left(g^{s_j^{2^{T-j}}}\right)^{-\alpha e'}(g^{s_j})^{-\alpha e'}g^{\alpha xp+\beta}(y')^{e-\gamma} \bmod p=$$

$$Y^e R'^{\alpha}Y^{-e+\gamma}(y')^{-(e-\gamma)}g^{\beta}g^{\alpha xp}(y')^{e-\gamma} \bmod p=$$

$$Y^e R'^{\alpha}Y^{-e}Y^{\gamma}g^{\beta}g^{\alpha xp} \bmod p=$$

$$Rg^{\alpha xp} \bmod p\neq R$$

所以，方案的可验证性不成立。

要使验证等式 $e^*=e$ 成立，即 $e=H(Y^e g^S y \bmod p,m)$，需要将盲签名过程中的参数 S' 修改为：

$$S'=k-e'(s_j^{2^{T-j}}+s_j)\bmod(p-1)$$

4.2 伪造攻击

本文通过分析发现，攻击者可以冒充签名者对任意消息 m 伪造盲签名。伪造方法如下：攻击者任意选取 $\tilde{R}$、$\tilde{S}$，其中，$1<\tilde{R},\tilde{S}<p-1$，计算：

$$\tilde{e}=H(\tilde{R},m)$$

$$\tilde{y}=\tilde{R}Y^{-\tilde{e}}g^{-\tilde{S}} \bmod p$$

则 $(\tilde{e},\tilde{S},\tilde{y})$ 是对消息 m 的有效盲签名。

事实上：

$$\tilde{R}^*=Y^{\tilde{e}}g^{\tilde{S}}\tilde{y} \bmod p=Y^{\tilde{e}}g^{\tilde{S}}\tilde{R}Y^{-\tilde{e}}g^{-\tilde{S}} \bmod p=\tilde{R}$$

$$\tilde{e}^*=H(\tilde{R}^*,m)=H(\tilde{R},m)=\tilde{e}$$

因此，$(m,j,(\tilde{e},\tilde{S},\tilde{y}))$ 可以通过签名验证，是一个有效的盲签名。

5 对文献[8]签名方案的改进

为了抵抗伪造攻击，本文对文献[8]的方案进行了改进，提出了一个新的前向安全的盲签名方案。

5.1 方案描述

(1)密钥生成

文献[8]的方案在生成系统参数时选取了2个大素数 p 和 q，但实际方案中不需要参数 q，所以，本文对其做了修正，省去了大素数 q 的选取。

系统首先选取大素数 $p(p\geqslant 2^{512})$，$g\in Z_p^*$ 是 Z_p^* 的生成元。$H:\{0,1\}^*\rightarrow Z_p^*$ 为安全的哈希函数。

将签名的有效时间划分为 T 个周期 $1,2,\cdots,T$，只有在 T 个周期内，签名者对消息的签名才是有效的。

随机选取初始私钥 $s_0(1<s_0<p-1)$，计算公钥 $Y=g^{s_0 2^T}$，公开 (H,p,g,T,Y)。

(2)密钥更新

与3.2节相同。

(3)盲签名生成

在 j 周期，消息 $m\in Z_p^*$ 的盲签名按如下步骤生成：

1)盲化(Blind)

签名者选择随机数 $k(1<k<p-1)$，计算 $R'=g^k \bmod p$，并将 R' 发送给消息 m 的请求者。

用户收到 R' 后，随机选择盲化因子 α、β、γ，其中，

$1<\alpha,\beta,\gamma<p-1$，计算：

$$R=R'^{\alpha}g^{\beta}Y^{\gamma} \bmod p$$

$$e=H(R,m)$$

$$e'=\alpha^{-1}(e-\gamma)\bmod(p-1)$$

并发送 e' 给签名者。

2)签名(Sign)

签名者收到 e' 后，计算：$s'=k-e's_j^{2^{T-j}} \bmod(p-1)$，并将 s' 发送给用户。

3)去盲(Umblind)

用户收到 s' 后，计算：$s=\alpha s'+\beta \bmod(p-1)$，则消息 m 的签名为 $sig(m)=(e,s)$。

(4)签名验证

首先判断盲签名 $(m,j,(e,s))$ 是否在签名者的签名有效期内，若 $j>T$，则签名无效，若 $1\leqslant j\leqslant T$，则计算：$R^*=Y^e g^s \bmod p$，$e^*=H(R^*,m)$。如果等式 $e^*=e$ 成立，则签名 $sig(m)=(e,S)$ 有效，否则，签名无效。

5.2 方案分析

5.2.1 正确性证明

因为：

$$R^*=Y^e g^s \bmod p=Y^e g^{\alpha s'+\beta} \bmod p=$$

$$Y^e g^{\alpha(k-e's_j^{2^{T-j}})+\beta} \bmod p=$$

$$Y^e (g^k)^{\alpha}\left(g^{s_j^{2^{T-j}}}\right)^{-\alpha e'} g^{\beta} \bmod p=$$

$$Y^e R'^{\alpha} g^{\beta} Y^{\gamma-e} \bmod p=R \bmod p$$

所以：

$$e^*=H(R^*,m)=H(R,m)=e$$

由此证明盲签名 $(m,j,(e,s))$ 是一个有效的签名。

5.2.2 安全性分析

(1)不可伪造性

攻击者试图通过公钥 $Y=g^{s_0 2^T}$ 求解初始私钥 s_0 不可行，因为他会遇到 Z_p^* 上的离散对数难题。

本文方案可以抵抗攻击者的一般性伪造攻击。如果攻击者想伪造签名者对消息 $m\in Z_p^*$ 的一个有效的盲签名，攻击者任意选取 $\tilde{R}(1<\tilde{R}<p-1)$ 可以计算 $\tilde{e}=H(\tilde{R},m)$，但想通过 $g^{\tilde{s}}=\tilde{R}Y^{-\tilde{e}} \bmod p$ 求解出 $\tilde{s}$ 不可行，因为他也会遇到离散对数难题。

(2)盲性

首先，签名者在签名时无法获知所签消息的具体内容。由于签名者是对 e' 进行签名的，而 e' 是用户经过哈希函数变换和盲化因子盲化后的数据，在不知道盲化因子 α、β、γ 的情况下，签名者得不到原始消息的任何信息。

其次，在同一时段内，签名者无法将公布的签名与自己保留的中间结果建立联系，即签名者无法追踪消息的拥有者。假设签名者保留了所有签名的中间结果 (j,k,R',e',s')。当用户公布盲签名 $(m,j,(e,s))$ 后，签名者无法通过：

$$\begin{cases}R=R'^{\alpha}g^{\beta}Y^{\gamma} \bmod p\\ e'=\alpha^{-1}(e-\gamma)\bmod(p-1)\\ s=\alpha s'+\beta \bmod(p-1)\end{cases}$$

计算出 3 个随机数 α、β、γ。因此，签名者无法确定公布的盲签名 $(m,j,(e,s))$ 是由自己保留的哪一组中间结果 (j,k,R',e',s') 生成的签名。但是由于盲签名 $(m,j,(e,s))$ 中含有时段编号 j，如果签名者在每一时段只对一个消息签名，则签名者就可以根据 j 追踪到消息的拥有者，即方案失去了不可追踪性。

(3)前向安全性

在二次剩余求解困难的假设下，方案具有前向安全性。假设攻击者获取了第 j 时段的密钥 s_j，在不知道 $p-1$ 的分解的情况下试图通过 $s_j=s_{j-1}^2 \bmod(p-1)$ 求解前一时段的密钥 s_{j-1} 不可行，因为会遇到二次剩余求解难题。

5.2.3 性能分析

令 T_E、T_I 和 T_M 分别表示一次模幂、模逆和模乘运算所需的时间。将本文方案与文献[8-9]方案在计算效率上进行比较，如表 1 所示，而 3 个方案在密钥更新阶段计算量都为 T_M。可以看出，本文方案相比文献[8-9]的方案分别减少了 1 次和 2 次模幂运算，计算效率更高。

表 1 3 个方案的计算复杂度比较

方案	盲签名阶段	验证阶段	合计
本文方案	$5T_E+T_I+5T_M$	$2T_E+T_M$	$7T_E+T_I+6T_M$
文献[8]方案	$7T_E+T_I+5T_M$	$2T_E+2T_M$	$9T_E+T_I+9T_M$
文献[9]方案	$4T_E+T_I+8T_M$	$4T_P+3T_M$	$8T_E+T_I+11T_M$

6 结束语

本文对文献[8]的基于离散对数的前向安全的盲签名方案进行了改进，使其可以抵抗攻击者的一般性伪造攻击，同时具有盲性和前向安全性。而且与同类方案相比，本文方案的计算效率较高。

参考文献

[1] Chaum D. Blind Signatures for Untraceable Payments[C]//Proc. of CRYPTO'82. New York, USA: Plenum Press, 1983: 199-203.

[2] Anderson R. Two Remarks on Public-key Cryptology[C]//Proc. of the 4th ACM Computer and Communications Security. New York, USA: ACM Press, 1997: 151-160.

[3] Krawczyk H. A Simple Forward-secure Signatures from any Signature Scheme[C]//Proc. of the 7th ACM Conference on Computer and Communication Security. Athens, Greece: ACM Press, 2000: 108-115.

[4] Duc D N, Cheon J H, Kim K. A Forward-secure Blind Signature Scheme Based on the Strong RSA Assumption[C]//Proc. of the 5th International Conference on Information and Communications Security. New York, USA: Springer-Verlag, 2003: 11-21.

[5] Lai Yeu Pong, Chang Chin Chen. A Simple Forward Secure Blind Signature Scheme Based on Master Keys and Blind Signatures[C]//Proc. of the 19th Int'l Conference on Advanced Information Networking and Applications. Washington D. C., USA: IEEE Press, 2005: 139-144.

[6] Koyama K. A Master Key for the RSA Public Key Cryptosystem[J]. IEICE Transactions on Information and Systems, 1982, J65-D(2): 163-170.

[7] Chow S S M, Hui Chi Kwong, Yiu Siu Ming, et al. Forward-secure Multisignature and Blind Signature Schemes[J]. Applied Mathematics and Computation, 2005, 168(2): 895-908.

[8] 张 席，杭欢花. 一种改进的前向安全盲签名方案[J]. 武汉大学学报：理学版，2011, 57(5): 343-348.

[9] 刘亚丽，殷新春，孟纯煜. 一种基于 ElGamal 体制的前向安全强盲签名方案[J]. 微电子学与计算机，2007, 24(10): 95-98.

编辑 张 帆