DOI: 10.3969/j.issn.1003-0972.2014.03.035

一个前向安全盲签名方案的分析与改进

孙 芳[1a*],张雪峰[2],袁小转[1b]

(1. 信阳师范学院 a. 计算机与信息技术学院; b. 数学与信息科学学院,河南 信阳 464000;
2. 信阳农林学院 计算机科学系,河南 信阳 464000)

摘 要: 对何俊杰等人提出的基于二次剩余的前向安全盲签名方案进行安全性分析,指出方案不满足前向安全性,并提出了一种改进方案. 分析结果表明,在二次剩余的平方根计算和 2^l 次根计算困难的假设下,改进方案具有前向安全性; 其不可伪造性则依赖于离散对数难题和二次剩余的 2^l 次根计算难题.

关键词: 盲签名; 前向安全性; 二次剩余; 离散对数

中图分类号: TP309 **文献标志码:** A **文章编号:** 1003-0972(2014)03-0444-03

Cryptanalysis and Improvement of a Forward-Secure Blind Signature Scheme

Sun Fang[1a*], Zhang Xuefeng[2], Yuan Xiaozhuan[1b]

(1a. College of Computer and Information Technology, b. College of Mathematics and Information Science, Xinyang Normal University, Xinyang 464000, China;
2. Department of Computer Science, Xinyang College of Agriculture and Forestry, Xinyang 464000, China)

Abstract: Cryptanalysis of the forward-secure blind signature scheme proposed by He Junjie et al. showed that the scheme does not satisfy forward security. An improved forward-secure blind signature scheme was proposed. Analysis results showed that the improved scheme has forward security under the assumption which make solving the square root and 2^l-th root of a quadratic residue hard, and its unforgeability dependends on the hardness of discrete logarithm problems and the problems of computing 2^l-th root of a quadratic residue.

Key words: blind signature; forward security; quadratic residue; discrete logarithm

0 引言

1982 年,Chuam [1] 为实现不可跟踪的支付系统首次提出了盲签名的概念. 与一般的数字签名相比,盲签名加入了对签名使用者隐私的保护,即签名者对用户要求的信息进行签名,但却不能获得信息的具体内容. 盲签名可以满足人们对个人隐私的要求,被广泛地用于电子现金、电子拍卖、电子选举等场合. 1997 年,Anderson [2] 为了减小私钥泄露给系统带来的威胁,首次提出了前向安全的概念. 在前向安全密码体制中,用户的签名私钥是随着时间段变化的,并且由当前时间段的私钥很难推出此前的任意时间段的私钥. 这样,即使某一个时间段的私钥泄露,攻击者也不能获得破坏系统此前各该时间段的安全性的能力.

2003 年 Duc 等人 [3] 将盲签名和前向安全技术结合起来,提出了前向安全盲签名方案. 此后,很多学者基于不同的数学难题和基本签名方案提出了大量前向安全盲签名方案. 如,2005 年,Lai 等人 [4] 基于 Koyama 主私钥方案和 Chaum 盲签名方案, Chow 等人 [5] 基于双线性映射和 GDH 问题分别提出了前向安全盲签名方案. 2007 年,Huang 等人 [6] 基于 Chaum 的经典盲签名方案,刘亚丽等人 [7] 基于 EIGamal 体制也分别提出了前向安全盲签名方案.

2011 年,张席等人 [8] 构造了一个基于 Schnorr 盲签名的前向安全盲签名方案. 但何俊杰等人 [9] 指出文献 [8] 方案不满足可验证性和不可伪造性,并对其进行了改进. 本文对文献 [9] 提出的改进的前向安全盲签名方案进行分析,指出方案不满足前向安全性,并对其进行了改进. 在二次剩余的平方根计算和 2^l 次根计算困难的前提下,改进方案具有不可伪造性和前向安全性.

1 预备知识

(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

收稿日期: 2013-09-04; 修订日期: 2013-12-06; * . 通信联系人,E-mail: ivy_xynusf@126.com
基金项目: 国家自然科学基金项目(61272465); 河南省自然科学基金项目(122400550189,142300410320,142400410486)
作者简介: 孙芳(1981-),女,河南信阳人,讲师,硕士,主要研究领域为信息安全.

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

满足 $y=g^x \bmod p$ 的 $x\in Z_p^*$ 是困难的.

(2) 二次剩余的平方根计算难题

在不知道 n 的分解时,已知 $y=x^2 \bmod n$,求 x 是困难的. 该问题的难度等价于大数分解难题.

(3) 二次剩余的 2^l 次根计算难题[10]

在不知道 n 的分解时,已知 $y=x^{2^l} \bmod n$,求 x 是困难的.

2 文献[9]方案回顾

2.1 私钥生成

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 个时段 $1,2,\cdots,T$,只有在 T 个时段内,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).

2.2 私钥更新

当时间从前一时段进入当前时段时,签名者根据前一时段私钥更新得到当前时段私钥. 设当前时段为 j,签名者按以下步骤更新私钥:

(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 时段的私钥 $s_j=s_{j-1}^2 \bmod (p-1)$,并删除 s_{j-1}.

2.3 盲签名生成

在 j 时段,消息 $m\in Z_p^*$ 的盲签名按如下步骤生成:

(1) 盲化: 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). 用户收到 R' 后,随机选择盲化因子 $\alpha、\beta、\gamma$,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: 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: 用户收到 s' 后,计算

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

则消息 m 的签名为 $sig(m)=(e,s)$.

2.4 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.

3 文献[9]方案的安全缺陷

文献[9]方案中,私钥的进化基于模合数的二次剩余的平方根计算难题,难度等价于大数分解问题,具有较好的前向安全性. 但在盲签名生成算法中,私钥以 $s_j^{2^{T-j}}$ 的形式出现在签名方程中,而

$$s_j^{2^{T-j}}=(s_{j-1}^2)^{2^{T-j}}=s_{j-1}^{2^{T-j+1}}=\cdots=s_0^{2^T}$$

是一个常数,与时段 j 无关. 所以,攻击者在获得第 j 时段的私钥后就可以利用 $s'=k-e's_j^{2^{T-j}} \bmod (p-1)$ 生成 s',进而去盲得到 s,并声称是任意时段 $i(i\neq j)$ 的签名数据. 由于

$$s'=k-e's_j^{2^{T-j}} \bmod (p-1)=k-e's_i^{2^{T-i}} \bmod (p-1),$$

所以验证者无法判别该签名到底是利用时段 j 的私钥 s_j 生成还是用时段 i 的私钥 s_i 生成. 因此方案不满足前向安全性.

4 改进方案

为了消除文献[9]方案的安全缺陷,本文对其进行了改进,改进方案描述如下.

4.1 系统生成

系统首先选取两个大素数 $p,q(p,q\geqslant 2^{512})$,且满足 $p=2p_1+1$,$q=2q_1+1$,其中 p_1,q_2 也为素数; 计算

$$n=pq,\varphi(n)=(p-1)(q-1)=4p_1q_1,$$

任意选择 $g\in Z_n^*$; 选取安全的哈希函数 $H:\{0,1\}^*\rightarrow Z_n^*$. 将签名的有效期划分为 T 个时段,只有在 T 个时段内,签名者对消息的签名才是有效的. 随机选取初始私钥 $s_0(1<s_0<n-1)$,计算公钥 $Y=s_0^{2^T} \bmod n$,公开参数为$(H,n,\varphi(n),g,T,Y)$.

4.2 私钥更新

第 j 时段的私钥按以下步骤更新: 若 $j>T$,则 s_j 设为空串,算法终止; 若 $1\leqslant j\leqslant T$,则计算第 j 时段的私钥 $s_j=s_{j-1}^2 \bmod n$,并删除 s_{j-1}.

4.3 盲签名生成

在第 j 时段,签名者和请求者(用户)按如下步骤生成消息 $m\in Z_n^*$ 的盲签名.

(1) 承诺: 签名者选择随机数 k,其中 $1<k<\varphi(n)$,计算 $R'=g^k \bmod p$,并将 R' 发送给用户.

(2) 盲化: 用户收到 R' 后,随机选择盲化因子 $\alpha、\beta$,其中,$1<\alpha,\beta<\varphi(n)$,计算

$$R=R'^{\alpha}g^{\beta} \bmod n,e=H(R,m,j),$$

$$e'=\alpha^{-1}e \bmod \varphi(n),$$

并发送 e' 给签名者.

(2) 签名: 签名者收到 e' 后,选择随机数 $u\in Z_{\varphi(n)}^*$,计算

$$U=s_j g^u \bmod n,s'=k+2^{T-j}e'u \bmod \varphi(n),$$

并将 U 和 s' 发送给用户.

(4) 去盲(Unblind): 用户收到 U 和 s' 后,计算

$$s=\alpha s'+\beta \bmod \varphi(n),$$

则消息 m 的签名为 $sig(m)=(j,U,e,s)$.

4.4 签名验证

验证者收到消息 m 的盲签名 $sig(m)=(j,U,e,s)$ 后,首先判断其是否在签名有效期内,若 $j>T$,则签名无效; 若 $1\leqslant j\leqslant T$,则计算

$$R^*=(YU^{-2^{T-j}})^e g^s \bmod n,e^*=H(R^*,m,j),$$

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

如果等式 $e^* = e$ 成立,则签名 $sig(m) = (j, U, e, s)$ 有效,否则,签名无效.

5　改进方案的分析

5.1　有效性

由于 $s_j = s_{j-1}^2 \bmod n = s_{j-2}^{22} \bmod n = \cdots = s_0^{2j} \bmod n$,所以

$$R^* = (YU^{-2^T-j})^{e'} g^s \bmod n =$$
$$(s_0^{2^T} (s_j g^u)^{-2^T-j})^{\alpha e'} g^{\alpha s'+\beta} \bmod n =$$
$$(s_0^{2^T} (s_0^{2j})^{-2^T-j} g^{-2^T-ju})^{\alpha e'} g^{\alpha(k+2^T-je'u)+\beta} \bmod n =$$
$$(s_0^{2^T} s_0^{-2^T-j2j})^{\alpha e'} g^{-2^T-ju\alpha e'} g^{\alpha k} g^{2^T-j\alpha e'u} g^{\beta} \bmod n =$$
$$R^{\alpha} g^{\beta} \bmod n = R,$$

从而 $e^* = H(R^*, m) = H(R, m) = e$,说明盲签名 $sig(m) = (j, U, e, s)$ 是一个有效的签名.

5.2　不可伪造性

攻击者试图通过公钥 $Y = s_0^{2^T} \bmod n$ 求解初始私钥 s_0 不可行,因为他会遇到二次剩余的 2^l 次根计算难题.

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 $m \in Z_n^*$ 的一个有效的盲签名,攻击者任意选取 $\tilde{R}, \tilde{U}(1 < \tilde{R}, \tilde{U} < n)$,可以计算 $\tilde{e} = H(\tilde{R}, m)$,但想通过 $g^{\tilde{s}} = (\tilde{Y}U^{-2^T-j})^{-\tilde{e}} \tilde{R} \bmod n$ 求解出 $\tilde{s}$ 不可行,因为他会面对离散对数难题. 同理,攻击者任意选取 $\tilde{R}(1 < \tilde{U} < n)$ 和 $\tilde{s}(1 < \tilde{s} < \varphi(n))$,想通过 $\tilde{U}^{-2^T-j} = (\tilde{R}g^{-\tilde{s}})^{e^{-1}} Y^{-1} \bmod n$ 计算 $\tilde{U}$ 或 $\tilde{U}^{-1}$ 不可行,因为他会遇到二次剩余的 2^l 次根计算难题.

5.3　前向安全性

在二次剩余的平方根计算和 2^l 次根计算困难的假设下,方案具有前向安全性.

假设攻击者获取了第 j 时段的私钥 s_j,在不知道 n 的分解的情况下试图通过 $s_j = s_{j-1}^2 \bmod n$ 求解前一时段的私钥 s_{j-1} 不可行,因为会遇到二次剩余求解难题. 所以改进方案中,签名私钥是前向安全的.

另一方面,假设攻击者获取了第 j 时段的私钥 s_j,试图生成之前任意时段(不妨设为第 i 时段,其中 $1 \leqslant i < j \leqslant T$)的签名也不可行. 首先,由于签名私钥是前向安全的,所以无法获得第 i 时段的私钥 s_i 伪造签名. 其次,签名数据 $U = s_j g^u \bmod n$ 直接与第 j 时段的私钥 s_j 有关,且签名验证中,等式 $R^* = (YU^{-2^T-j})^{e'} g^s \bmod n$ 与时段序号 j 直接相关,所以攻击者无法利用第 j 时段的私钥 s_j 来生成可以通过验证的之前任意时段的盲签名.

5.4　弱盲性

由于签名者只知道 e',而 e' 是用户经过盲化因子盲化后的数据,在不知道盲化因子的情况下,签名者不能获得原始消息 m 的任何信息. 但是,签名数据中含有签名者已知的 U,使得签名者可以将公布的盲签名与自己保留的某次签名中间数据联系起来,所以改进方案是可追踪. 所以改进方案满足弱盲性.

6　结语

本文对文献[9]提出的前向安全盲签名方案进行了安全性分析,指出方案不满足前行安全性,并提出了一种改进的方案. 对改进方案做了安全性分析,指出方案具有不可伪造性、前向安全性、弱盲性.

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] 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.

[4] Lai Y P, Chang C C. *A simple forward secure blind signature scheme based on master keys and blind signatures* [C] // Proc of the 19th International Conference on Advanced Information Networking and Applications. Washington D C, USA: IEEE Press, 2005: 139-144.

[5] Chow S S M, Hui L C K, Yiu S M, et al. *Forward-secure multisignature and blind signature schemes* [J]. Applied Mathematics and Computation, 2005, 168(2): 895-908.

[6] Huang H F, Chang C C. *A new forward-secure blind signature scheme* [J]. Journal of Engineering and Applied Sciences, 2007, 2(1): 230-235.

[7] 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.

[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): 434-438.

[9] 何俊杰, 王娟, 祁传达. 一个改进的前向安全盲签名方案 [J]. 计算机工程, 2012, 38(11): 133-135.

[10] 柴震川, 董晓蕾, 曹珍富. 利用二次剩余构造的基于身份的数字签名方案 [J]. 中国科学·F 辑: 信息科学, 2009, 2(2): 199-204.

责任编辑: 郭红建

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net