第 36 卷 第 8 期 计 算 机 工 程 2010 年 4 月
Vol.36 No.8 Computer Engineering April 2010
·安全技术· 文章编号：1000—3428(2010)08—0163—02 文献标识码：A 中图分类号：TP309

一种部分盲签名方案

成 林，亢保元，王国瞻
(中南大学数学科学与计算技术学院，长沙 410075)

摘 要：提出一个基于离散对数的部分盲签名方案，分析其安全性和效率。该方案满足部分盲性、不可追踪性和不可伪造性，可以防止消息提供者滥用签名，保证签名者不能侵犯消息提供者的身份隐私。与基于 Schnorr 签名算法和基于 DSA 变形签名算法的部分盲签名方案相比，该方案效率较高。

关键词：盲签名；部分盲签名；离散对数

Partially Blind Signature Scheme

CHENG Lin, KANG Bao-yuan, WANG Guo-zhan
(School of Mathematical Science and Computing Technology, Central South University, Changsha 410075)

【Abstract】 This paper proposes a partially blind signature scheme based on discrete logarithm and analyzes its security and performance. This scheme is partially blind, untraceable and unforgeable. It prevents user abusing signature and ensures that the identity privacy of message provider can not be infringed by the signer. The scheme is more efficient than the two others based on Schnorr signature algorithm and DSA changed signature algorithm respectively.

【Key words】 blind signature; partially blind signature; discrete logarithm

1 概述

文献[1]首次提出部分盲签名的概念和基于 RSA 的部分盲签名方案。部分盲签名是指在签名时可以加入签名人的信息或签名人与消息提供者(用户)商定的信息，消息提供者得到签名后，不能对签名人加入的消息进行篡改。部分盲签名具有一般数字签名的基本信息，并满足盲签名的 2 个条件：(1)签名人不知所签信息的内容；(2)签名信息是不可追踪的。文献[2]提出基于离散对数的部分盲签名方案，文献[3]对文献[2]方案进行安全性分析[3]，发现敌手可在不被察觉的情况下成功去除该方案中的部分盲特性，并可以伪造部分盲签名的嵌入常数。鉴于此，本文设计一个新的基于离散对数的部分盲签名方案。

2 部分盲签名方案

设 c 为签名人的信息或签名人与用户商定的信息，部分盲因子 c 的长度为 k-2 bit，签名人与用户事先商议好的共同的格式函数为 $\tau_{(c)}=2^{k-1}+2h_1(c)+1$，其中，$h_1(.)$ 是单向函数；$\tau_{(c)}$ 的取值范围是 $2^{k-1}<\tau_{(c)}<2^k$。

当 $c'\neq c$ 时，$\tau_{(c)}$ 与 $\tau_{(c')}$ 不能相互整除。设 p 是一个素数，使得在 z_p 上的离散对数问题是难处理的，设 $g\in z_p^*$ 是一个本原元，待签名的消息为 m，签名人的私钥为 x，相应的公钥为 $y=g^x \bmod p$。设 A 是消息提供者(用户)，B 是签名者，$h(\cdot)$ 是 Hash 函数，$h:\{0,1\}^*\to z_p$。

部分盲签名协议描述如下：

(1)A 与 B 商定信息 c。

(2)B 随机选择 $k\in z_p^*$，计算 $r=g^k \bmod p$，并满足 $\gcd(r,p-1)=1$，B 发送 r 给 A。

(3)A 随机选择 $\alpha,\beta,\delta\in z_p^*$，计算 $r'=r^{\alpha}y^{\delta\tau_{(c)}}g^{\beta} \bmod p$，$m'=(r\alpha)^{-1}(r'm-\delta) \bmod (p-1)$，$A$ 发送 m' 给 B。

(4)B 接收到 m' 后，计算 $s=rm'x\tau_{(c)}-k \bmod (p-1)$，$B$ 发送 s 给 A。

(5)A 计算 $s'=(\alpha s-\beta)[\tau_{(c)}]^{-1} \bmod (p-1)$，并公布 (r',s',c) 作为关于消息 m 和公共信息 c 的部分盲签名，否则输出“ false ”。任何人都可通过检查 $y^{r'm\tau_{(c)}}=r'g^{s'\tau_{(c)}} \pmod p$ 验证签名的有效性。

证明：$s=rm'x\tau_{(c)}-k \bmod (p-1)\Leftrightarrow$

$$s=r\alpha^{-1}r^{-1}(r'm-\delta)x\tau_{(c)}-k \bmod (p-1)\Leftrightarrow$$

$$\alpha^{-1}(s'\tau_{(c)}+\beta)=\alpha^{-1}(r'm'-\delta)x\tau_{(c)}-k \bmod (p-1)\Leftrightarrow$$

$$s'\tau_{(c)}+\beta=(r'm-\delta)x\tau_{(c)}-\alpha k \bmod (p-1)\Leftrightarrow$$

$$r'mx\tau_{(c)}=(\alpha k+\delta x\tau_{(c)}+\beta)+s'\tau_{(c)} \bmod (p-1)$$

因此，$y^{r'm\tau_{(c)}} \bmod p=g^{(\alpha k+\delta x\tau_{(c)}+\beta)+s'\tau_{(c)}} \bmod p=r'g^{s'\tau_{(c)}} \bmod p=g^{r'mx\tau_{(c)}} \bmod p$。

3 安全性分析

3.1 部分盲性

若 (r',s',c) 是一个有效的盲签名，假设用户在获得签名人的签名后，试图将事先协定的消息篡改为 c^*，且能保证签名的有效性，则根据以下验证方程：

$$y^{r'm\tau_{(c^*)}}=r'g^{s'\tau_{(c^*)}} \pmod p \Leftrightarrow$$

$$r'mx\tau_{(c)}=(\alpha k+\delta x\tau_{(c)}+\beta)+s'\tau_{(c)} \bmod (p-1)$$

可知用户欲篡改成功，必须知道 x,k，而由 $y=g^x \bmod p$ 和 $r=g^k \bmod p$ 可知，计算 x 和 k 都要面临有限域上求解离散对

作者简介：成 林(1983－)，男，硕士，主研方向：密码学；亢保元，教授、博士；王国瞻，硕士

收稿日期：2009-12-28 **E-mail：**stonewoods302@163.com

数问题，所以，篡改协定信息 c 是不可行的。

3.2 不可追踪性

在该方案中，B 观察到的信息为 (m',r,s,c)，若 B 存储信息 (m',r,s,c)，则当 A 公开 (m,r',s',c) 后，B 可以通过如下方程：

$$\begin{cases} s' = (\alpha s - \beta)[\tau_{(c)}]^{-1} \bmod (p-1) \\ m' = (r\alpha)^{-1}(r'm - \delta) \bmod (p-1) \\ r' = r^{\alpha} y^{\delta\tau_{(c)}} g^{\beta} \bmod p \end{cases}$$

求解 α,β,δ，从而找出 (m',r,s,c) 和 (m,r',s',c) 的联系，但 B 解出 α,β,δ 必须计算离散对数，因此，在难于计算离散对数的前提下，该方案满足不可追踪性。

3.3 不可伪造性

3.3.1 消息提供者 A 伪造合法盲签名的可能性

签名者在盲消息中置入随机因子，使攻击者不能推测签名者所签消息的具体内容，该随机性可有效抵御选择明文攻击，防止伪造[4]。在安全的签名方案中，用户不能除去签名者的随机因子。

在此方案中，签名者 B 随机选择 $k \in z_p^*$，计算 $r = g^k \bmod p$，并满足 $(r, p-1)=1$，B 发送 r 给 A，A 发送 $m' = (r\alpha)^{-1}(r'm - \delta) \bmod (p-1)$ 给 B，B 发送 $s = rm'x\tau_{(c)} - k \bmod (p-1)$ 给 A。如果攻击者 A 试图去除随机因子 k，则攻击者必须从 $y = g^x \bmod p$ 和 $r = g^k \bmod p$ 计算得到 x 和 k，而解决此类问题要面临有限域上求解离散对数的难题。

3.3.2 签名者伪造合法盲签名的可能性

签名者 B 伪造签名面临 2 大困难：(1)冒充用户 A 将消息盲化，由 $m' = (r\alpha)^{-1}(r'm - \delta) \bmod (p-1)$ 可知，在对 α,δ 未知的情况下，签名者 B 无法完成对消息 m 的盲化。(2)冒充用户 A 对签名脱盲，由 $s' = (\alpha s - \beta)[\tau_{(c)}]^{-1} \bmod (p-1)$ 可知，在 α,β 未知的情况下，B 无法完成对签名 s 的脱盲。解决上述问题时，将面临有限域上求解离散对数的难题。

3.4 效率分析

在进行签名的过程中，指数运算、逆运算、乘法运算和 Hash 运算的耗时比例很大，一般来说，在实际应用中，n 的长度通常取为 1 024 bit 或更长。$|n|$表示 n 的长度，模 n 下的一次指数运算的计算时间是一次乘法运算计算时间的 0.324 6$|n|$倍[5]，逆运算和指数运算的计算时间基本相等，一次 Hash 运算的计算时间不多于一次模乘运算时间[6]。对文献[2]提出的基于 Schnorr 签名算法的部分盲签名方案、基于 DSA 变形签名算法的部分盲签名方案[2]和本文方案进行比较，方案的计算量如表 1 所示，其中，E, I, M,H 分别表示取模意义下的指数运算、逆运算、乘法运算和 Hash 运算。

表 1 计算效率比较

部分盲签名方案	总运算量
基于 Schnorr 签名算法	6E+3I+5M+2H
基于 DSA 变形签名算法	7E+4I+12M
本文方案	6E+2I+15M

由表 1 可知，本文方案的效率高于基于 Schnorr 签名算法和基于 DSA 变形签名算法的部分盲签名方案。

4 结束语

本文提出的方案实现了预期目标，与文献[2]提出的盲签名方案相比，其效率得到提高，具有较高应用价值。

参考文献

[1] Abe M, Fujisaki E. How to Date Blind Signatures[C]//Proc. of Cryptology-Asiacrypt'96. Berlin, Germany: Springer, 1996: 244- 251.

[2] 张 彤, 王育民. 几种部分盲签名的算法设计及其安全性分析[J]. 西安电子科技大学学报, 2004, 31(6): 963-966.

[3] 辛向军, 李发根, 肖国镇. 对几种部分盲签名方案的安全性分析与改进[J]. 西安电子科技大学学报, 2006, 33(6): 953-984.

[4] Ferguson N. Single Term Off-line Coins[C]//Proc. of Cryptology-Eurocrypt'93. Berlin, Germany: Springer, 1994: 318-328.

[5] Chen Chien-Yuan, Chang Chin-Chen, Yang Wei-Pang. Hybrid Method for Modular Exponentiation with Precomputation[J]. Electronics Letters, 1996, 32(6): 540-541.

[6] Simmons G J. Contemporary Cryptology: The Science of Information Integrity[M]. New York, USA: IEEE Press,1992.

编辑 陈 晖

(上接第 162 页)

如上所述，通过上述 2 种方案改进的 adore-ng 模块都可以成功屏蔽卡巴斯基的实时监控。2 次测试中在加载修改过的 adore-ng 模块后，卡巴斯基均无法记录对隐藏文件的操作；而加载未修改的 adore-ng 模块时，卡巴斯基实时监控生成该文件被打开操作的相关记录。

3.4 改进方案比较

实验证明，上述 2 种改进方案均可以有效地屏蔽卡巴斯基的实时监控。但是，作为攻击程序的研究，本身就是在执行环境、访问资源等很多受限情况下进行，因此，上述 2 种方案都存在一定的局限性，对所执行的环境有比较严格的要求。第 1 种方案要求严格控制系统模块的加载顺序，保证修改后的 aodre-ng 模块在卡巴斯基监控模块加载之后加载。具体实现时，攻击者可以通过修改系统启动脚本等方式来控制启动顺序。第 2 种方案在 VFS 层对写文件的内容进行过滤，可能会对系统造成一定的性能损失。因此，在该方案的实现中首先进行严格条件匹配，尽量将文件内容判断的情况减少到最低。

4 结束语

Linux 下 VFS 层 rootkit 隐藏层次深，一般的 rootkit 侦测工具难以发现。本文对 VFS 层 rootkit 的典型应用 adore-ng 进行研究，针对其无法屏蔽内核级实时监控工具的问题提出 2 种改进方案，并加以实现。实验结果表明，改进效果良好，卡巴斯基无法检测到对隐藏文件的访问。

参考文献

[1] Andreas B. Unix and Linux-based Rootkits Techniques and Countermeasures[Z]. (2004-04-30). http://www.first.org/conference/2004/papers/c17.pdf.

[2] Alisa S. Rootkit Evolution[Z]. (2008-08-28). http://www.viruslist.com/en/analysis?pubid=204792016.

[3] Samhain Labs. Detecting Kernel Rootkits[Z]. (2003-06-17). http://www.ists.dartmouth.edu/library/409.pdf.

[4] 庄泗华, 王 剑, 张福新. 检测 Linux 下的 VFS 型内核后门软件[J]. 计算机应用研究, 2005, 22(5): 194-196.

[5] Adore-ng[Z]. (2004-03-25). http://stealth.7350.org/rootkits/adore-ng-0.56.tgz.

编辑 陈 文