对两种基于离散对数代理盲签名的分析

秦宝东
QIN Bao-dong

西南科技大学 计算机科学与技术学院,四川 绵阳 621010
College of Computer Science & Technology,Southwest University of Science & Technology,Mianyang,Sichuan 621010,China
E-mail:bd_qin@yahoo.com

QIN Bao-dong.Cryptanalysis of two proxy blind signatures based on DLP.Computer Engineering and Applications,2009,45(3):104-105.

Abstract:This paper presents a security analysis of two DLP-based proxy blind signature schemes proposed recently by Gao et al and Yu et al respectively and point out that both of the two schemes are insecure against the proxy signer's linkability attacks as well as the user's forgery attacks.Gao et al's scheme is an improved scheme of Tan et al's.However,it is still vulnerable to the proxy signer's linkability attacks.Yu et al's scheme is also insecure against the proxy signer's linkability attacks.In addition,the user can deduce the proxy signature private key by using a valid proxy signature,and then instead of the proxy signer he can forge a valid proxy signature of a message m.He also can directly forge a valid proxy signature which related to the valid signature received from the proxy signer.This paper presents an improved scheme that can against the proxy signer's linkability attacks.

Key words:discrete logarithm problem;proxy blind signature;cryptanalysis

摘 要:高炜等人和 Yu Bao-zheng 等人分别提出了两种基于离散对数的代理盲签名方案。对这两种方案进行了安全性分析。研究表明,这两种方案存在以下不足之处:高炜等人的代理盲签名方案是对谭等方案的改进,新的方案仍然具有可连接性,即代理签名者可以从一个合法的代理盲签名中恢复出此签名的中间值从而跟踪消息的拥有者。Yu Bao-zheng 等人的代理盲签名方案同样具有可连接性的缺点。除此之外,用户可以通过自己持有的代理盲签名信息恢复出代理签名私钥,从而可以冒充代理签名者伪造消息 m 的代理盲签名或者直接利用一个合法的代理盲签名伪造出其它消息的合法代理盲签名。为了避免上述不足之处,给出了一个防止代理签名者连接性攻击的改进方案。

关键词:离散对数;代理盲签名;密码分析
DOI:10.3778/j.issn.1002-8331.2009.03.030 **文章编号**:1002-8331(2009)03-0104-02 **文献标识码**:A **中图分类号**:TP309

1 引言

数字签名技术是一种用于证明签名者身份信息的密码技术。近年来人们又提出了一些新的与数字签名相关的概念,主要包括 1983 年 Chaum[1]提出的盲签名概念,1996 年 Mambo 等[2]提出的代理签名概念和 2000 年 Lin 等[3]结合盲签名和代理签名所提出的代理盲签名概念。盲签名和代理盲签名主要具有以下特征:(1) 正确性,即任何人都可以利用签名者和/或代理签名者的公钥验证签名是否正确;(2) 不可伪造性,即除签名者和/或指定的代理签名者外,其他人不能伪造消息的有效签名;(3) 非关联性,即用户在公开自己的签名后,签名者和/或代理签名者不能够对自己所签消息的拥有者进行跟踪。除此之外,代理盲签名还具有:(4) 可区分性,即人们能区分出代理盲签名和一般签名;(5) 代理签名者身份不可伪造性,即除原始签名者指定的代理签名者外,其他人不可以冒充代理签名者身份。

近年来,一些基于离散对数问题的代理盲签名方案不断被提出。2007 年高炜等[4]提出了一个改进的基于离散对数问题的代理盲签名方案。改进的方案解决了谭等[5]方案中的可伪造及可连接等[6]不足之处。2007 年 Yu 等[7]提出了一个新的基于离散对数问题的代理盲签名方案。研究表明,在这两种代理盲签名方案中仍存在以下不足之处:(1) 高等改进的代理盲签名方案仍然具有可连接性,即代理签名者可以从一个合法的代理盲签名中恢复出此签名的中间值从而跟踪消息的拥有者;(2) Yu 等人的代理盲签名方案同样具有可连接性的缺点。除此之外,用户可以通过自己持有的代理盲签名信息恢复出代理签名私钥,从而可以冒充代理签名者伪造消息 m 的代理盲签名或者直接利用一个合法的代理盲签名伪造出其它消息的合法代理盲签名。为了避免上述不足之处,给出了部分改进方案。

2 符号说明

为便于叙述,在本文中对以下符号定义如下:

A 为原始签名者;B 为代理签名者;R 为签名的接受者,即用户;p、q 为两个大素数其离散对数问题在 Z_p 上是难处理的,

作者简介:秦宝东(1982-),男,助教,主要研究方向为公钥密码体制、计算数论和信息安全。
收稿日期:2008-01-04 修回日期:2008-04-24

且 $q|p-1$;g 为环 Z_p^* 上阶为 q 的本原元 ;m 为待签名的消息 ;$H(\cdot)$ 为无碰撞的哈希函数。

3 高等和 Yu 等代理盲签名方案及其安全性分析

3.1 高等代理盲签名方案及其安全性分析

3.1.1 高等代理盲签名方案

(1) 系统参数

$x_A, x_B \in Z_p^*$ 分别为 A 和 B 的私钥 ;$y_A = g^{x_A} \bmod p$ 和 $y_B = g^{x_B} \bmod p$ 分别为 A 和 B 的公钥。

(2) 代理阶段

A 随机选择 $\bar{k} \in Z_p^*$,计算 $\bar{r} = g^{\bar{k}} \bmod p$,$\bar{s} = x_A \bar{r} + \bar{k} \bmod q$。$A$ 通过安全信道把 $(\bar{r}, \bar{s})$ 发送给代理 B。

B 验证 $g^{\bar{s}} = \bar{r} y_A^{\bar{r}} \bmod p$ 是否成立。若成立,B 接受并计算 $s' = \bar{s} + x_B \bmod q$。$s'$ 为 B 的代理秘钥。计算 $T = g^{s'} = y_B^{\bar{r}} y_A^{\bar{r}} \bmod p$。

(3) 签名阶段

①B 随机选择 $k \in Z_p^*$,计算 $t = g^k \bmod p$,然后发送 $(\bar{r}, t, T)$ 给接收者 R。

②R 随机选择 $a, b, w, n \in Z_p^*$,计算 :

$r = t g^{-H(\bar{r})} y_B^{-(a+b)} \bmod p$,$e = H(r \| m) \bmod q$,$e^* = e + a + b \bmod q$,$M = (a+b)\, w + n \bmod q$,$N = a + b \bmod q$,$u = (\bar{r} y_A^{\bar{r}})^{-1} y_A^{w} \bmod p$,$T^* = (uT)^N y_A^n \bmod p$。

如果 $r=0$,R 重新选择满足 $r \neq 0$ 的 $a, b \in Z_p^*$。R 传送 e^* 给代理 B。B 收到 e^* 后计算 $s'' = k - x_B e^* \bmod q$。$B$ 将 s'' 发送给 R。

(4) 签名提取阶段 R 收到 s'' 后,计算 $s = s'' - H(r) \bmod q$。代理签名为六元组 (m, M, N, T^*, s, e)。

(5) 签名验证 $T^* = y_A^M y_B^N \bmod p$ 成立则说明 A 和 B 存在代理关系,$e = H(g^s y_B^e \| m)$ 成立说明签名有效。

3.1.2 安全性分析

高等代理盲签名方案虽然是对谭等方案的改进,但是仍然具有可连接性,也就是说代理签名六元组 (m, M, N, T^*, s, e) 与代理签名者 B 所知道的中间值 $\bar{r}, t, T, e^*$ 存在一定联系,即已知签名,B 可以求解到中间值。这是因为,当 R 公布自己的代理签名六元组 (m, M, N, T^*, s, e) 后,B 可以通过计算 $N + e \bmod q$ 获得该签名所对应的中间值 e^*,这是因为 $e^* = N + e \bmod q$。由于 B 保留了所有签名消息的中间值,B 可以找到与 $N + e \bmod q$ 相匹配的 e^*, 从而跟踪用户。对于不同的消息其中间值 e^* 可能相等,概率为 $1/q$,因此代理签名者跟踪用户失败的概率仅为 $1/q$。由于 q 为大素数,因此失败的概率是可以忽略的。

3.1.3 改进的方案

在上述代理盲签名方案中,代理签名六元组 (m, M, N, T^*, s, e) 中的参数 M 和 N 的作用主要是用来验证 $T^* = y_A^M y_B^N \bmod p$ 是否成立,以此判断 A 和 B 是否存在代理关系,而与签名有效性验证所需的参数 s 和 e 之间无必然联系。也就是说,参数 M 和 N 的选取可以是任意的。下面给出高等方案的一个改进方案,以避免前面提到的可连接性攻击。

在高等原有方案的基础上,只需要对签名阶段②中的部分参数主要包括 M,N 和 T^* 的计算值作如下修改 :

R 随机选择 $a, b, c, w, n \in Z_p^*$,计算 $r = t g^{-H(\bar{r})} y_B^{-(a+b)} \bmod p$,$e = H(r \| m) \bmod q$,$e^* = e + a + b \bmod q$,$M = (a+b+c)\, w + n \bmod q$,$N = a + b + c \bmod q$,$u = (\bar{r} y_A^{\bar{r}})^{-1} y_A^{w} \bmod p$,$T^* = (uT)^N y_A^n \bmod p$。

此时, 仍然可以利用 $T^* = y_A^M y_B^N \bmod p$ 是否成立来判断 A 和 B 是否存在代理关系,这是因为 $T^* = (uT)^N y_A^n = (\bar{r} y_A^{\bar{r}})^{-N} y_A^{wN} (y_B^{\bar{r}} \bar{r} y_A^{\bar{r}})^N y_A^n = y_A^M y_B^N \pmod p$。

在改进的方案中 $e^* \neq e + N \pmod q$,从而避免了原方案的可连接性的缺点。

3.2 Yu 等代理盲签名方案及其安全性分析

3.2.1 Yu 等代理盲签名方案

Yu 等方案的系统参数建立和代理阶段与高等方案的 (1) 和 (2) 阶段一致,不同的是在阶段 (2) B 并不计算 T 的值。

(1) 消息盲化阶段

R 选择一盲化因子 t,计算 $M = mt \pmod q$。R 把 M 发送给 B。

(2) 盲签名阶段

B 随机选取 $k \in Z_p$,计算 $r = g^k \pmod p$,$\varphi = k^{-1} s' \pmod q$,$\bar{s} = M - s' r \pmod q$。

B 把 $(M, \bar{s}, r, \bar{r}, \varphi)$ 发送给 R。R 验证 $g^M = y_A^{\bar{r}r} y_B^{\bar{r}r} \bar{r}^{\bar{r}} r^{\bar{s}} \pmod p$,若成立则 R 相信盲消息 M 的签名来自 B,否则拒绝接受。

(3) 签名提取阶段

R 计算 $s = \bar{s} t^{-1} + \varphi r (r^{-1} - 1) \pmod q$,则消息 m 的代理签名为 $(m, s, r, \bar{r})$。

(4) 签名验证

任何人可以通过验证 $g^m = r^s y_A^{\bar{r}r} y_B^{r\bar{r}} \pmod p$ 来确定签名的有效性。

3.2.2 安全性分析

在 Yu 等上述代理签名方案中存在以下三点不足之处 :

(1) 该方案最终的代理签名为 $(m, s, r, \bar{r})$,即签名提取阶段 (3) R 公布的结果。在该代理签名中,参数 r 是阶段 (2) 代理签名者 B 计算的一个中间值。对于不同的消息 m,r 的值应该是随机的。如果 B 保留这些 r 的值,那么 B 就可以根据签名接受者 R 公布的签名参数 $(m, s, r, \bar{r})$ 找到与 m 对应的 M 的值,这就失去了代理盲签名方案应具有的非关联性。

(2) 在 Yu 等代理签名方案阶段 (2),代理签名者 B 把 $(M, \bar{s}, r, \bar{r}, \varphi)$ 发送给用户 R。那么用户通过已知的信息 $\varphi, \bar{s}, r$ 和 M 可以计算出 $k = (\bar{s} + r\varphi)^{-1} \cdot M \pmod q$ 以及代理秘钥 $s' = (\bar{s} + r\varphi)^{-1} \cdot \varphi M \pmod q$。用户 R 一旦获得了代理签名秘钥 S',那么 R 就完全可以充当代理签名者的角色并按照步骤 (2) 的方式对其它消息进行签名。若该方案用于安全的电子支付系统中,那么将是非常危险的,因为 R 完全可以通过上述攻击方式,为自己生成大量合法的电子货币。由此看,Yu 等代理盲签名方案不具有不可伪造性,是不安全的,更不能在实际中应用。

(下转 112 页)

且 $X_0(t_0)=X'_0(t_0)$，$g(\cdot)=0$，同样使用的反馈微扰同步法，同样采用数值分析法，得到的非时变参数系统试与时变参数的驱动系统的同步时误差曲线，如图 9 所示。$x\sim x'$的同步相图，如图 10 所示。

图 9 和图 10 表明，此时窃密（响应）系统与驱动系统存在相当大的误差，而无法实现同步通信。因为，驱动参数实际上是动态时变的，窃密方的参数失配必然远大于正常通信的响应系统，即使不计噪声等因素的干扰 $g(\cdot)=0$ 和初始条件完全相同 $X_0(t_0)=X'_0(t_0)$，窃密方与驱动系统达成动态同步或广义动态同步的可能性也是极小的，从而表明时变参数的混沌系统同步系统，具有极强的抗攻击能力。而利用混沌映射的子密钥序列控制混沌系统参数的方法，不仅适应于四阶 Lorenz 超混沌同步系统，也适用于其他类混沌系统。

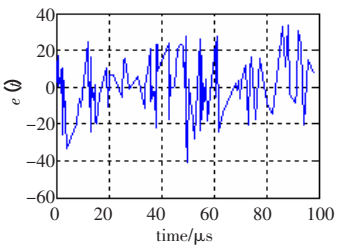

图 9 非时变参数与系统的同步误差图

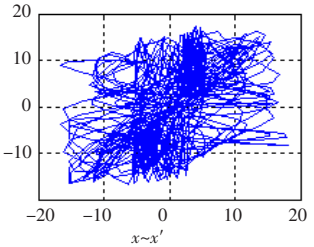

图 10 非时变参数与时变参数系统的同步相图

4 总结

在对改进的自治四阶 Lorenz 系统进行分析的基础上，提出了数值混沌序列进行二次处理的新算法，并将该算法应用于改进的四阶 Lorenz 混沌同步系统，控制系统参数，实现了系统在混沌与超混沌状态之间不断切换情况下的同步。从仿真的结果中可以看到，该算法在提高了系统保密性的同时，保证了系统良好的鲁棒性。限于篇幅上的原因，该算法使用的数字混沌序列和密钥算法还较简单，实际应用中，可在该算法的基础上随时变更 M 序列，或变更控制数值、或采用多个参数同时控制等方法，使窃密方没有足够的时间和信量来破译系统，实现混沌同步保密通信。

参考文献：

[1] 高远，翁甲强，罗晓曙，等.超混沌电路的广义同步[J].电子与信息学报，2002，6(24)：855-959.

[2] 冯久超，鲁瑞华.一种基于神经网络策略的自适应混沌解调器[J].计算机科学，2000，6(27)：101-103.

[3] Guang L，Steve B.Radzal basis function network eonflgu ratlon using mutual informarzon and the orthogonal least square algorlthm[J].Neural Networks，1996，9(9)：1619-1637.

[4] Grassi G，Miller D A.Theory and experimental realization of observer-based diserete-time hyperehaos synehronization[J].IEEE Trans Cireuits and Systems，2002，49(3)：373-377.

[5] Lv J H，Chen G R，Cheng D Z，et al.Bridge the gap between the Lorenz system and the Chen system [J].International Journal of Bifurcation and Chaos，2002，12：2917-2926.

[6] Rossler O E.An equation for hyperchaos[J].Phys Lett A，1979：71-155.

[7] 王光义，郑艳，刘敬彪.一个超混沌吸引子及其电路实现[J].物理学报，2007，6(56)：3114-3120.

[8] 杨涛，邵惠鹤.一类混沌系统的同步方法[J].物理学报，2002，4(51)：742-748.

[9] 陈滨.混沌在时变参数保密通信及雷达波形设计中的应用基础研究[D].成都：电子科技大学，2007.

[10] 厉小润，赵辽英，赵光宙.一种具有结构或参数失配的混沌保密通信系统[J].电路与系统学报，2003，8(3)：44-49.

[11] 张勇，陈天麒，陈滨.跃变参数混沌同步及其应用[J].物理学报，2007，56(1)：55-56.

[12] 杨承辉，周宇鹏，徐超.改进的耦合同步罗仑兹混沌遮掩保密通信电路[J].苏州科技学院学报：自然科学版，2008，2(25)：70-73.

[13] Eckmann J P，Kamphorst S O，Ruelle D.Lyapunov exponents from time series[J].Phys Rev A，1986，34：4971-4979.

（上接 105 页）

(3) 用户 R 也可以直接在签名提取阶段 (3) 伪造出一系列合法的签名，若 R 想获得另一消息$\hat{m}$（假设 $gcd(\hat{m},M)=1$）的代理盲签名，方法是：R 首先利用欧几里德算法计算 $\hat{t}=\hat{m}^{-1}\cdot M \bmod q$，再计算$\hat{s}=\bar{s}\hat{t}^{-1}+\varphi r(r^{-1}-1)\pmod q$，则消息$\hat{m}$的代理盲签名为 $(\hat{m},\hat{s},r,\bar{r})$。该签名可以通过签名验证，是有效的签名。这再次说明 Yu 等代理盲签名方案是不安全的。

从上述不足之处可以看出，Yu 等方案在代理签名阶段的设计上存在缺陷。要提高方案的安全性，可以改变签名有效性验证的方式，减少一些敏感参数的泄漏。具体如何去改进 Yu 等方案的不足之处是一个有待解决的问题。

4 结束语

主要分析了高等和 Yu 等两种基于离散对数的代理盲签名方案的安全性，指出它们的不足之处，并给出了高等方案的改进方案。如何提高 Yu 等方案的安全性还需要作进一步的研究。

参考文献：

[1] Chaum D.Blind signature for untraceable payments[C]//Proceedings of CRYPTO'82.Berlin：Plenum Press，1993：199-203.

[2] Mambo M，Usuda K，Okamoto E.Proxy signatures for delegating signing operation[C]//Proc of 3rd ACM Conference on Computer and Communication Security，1996：48-57.

[3] Lin W D，Jan J K.A security personal learning tools using a proxy blind signature scheme[C]//Proc of Int'l Conference on Chinese Language Computing，2000：273-277.

[4] 高炜，刘焕平.对基于离散对数的代理盲签名方案的改进[J].哈尔滨师范大学自然科学学报，2007，23(1)：56-59.

[5] 谭作文，刘卓军，唐春明.基于离散对数的代理盲签名[J].软件学报，2003，11：1931-1935.

[6] 王蜀洪，王桂林，鲍丰，等.对一个基于离散对数代理盲签名的密码分析[J].软件学报，2005，5：911-915.

[7] Yu Bao-zheng，Xu Cong-wei.A proxy blind signature scheme based on DLP[J].Wuhan University Journal of Natural Sciences，2007，12(1)：83-86.