广西科学院学报
Journal of Guangxi Academy of Sciences

2008,24(2):106～109
Vol. 24,No. 2 May 2008

一种改进的无需可信任第三方的时控代理签名方案
An Improved Time Stamped Proxy Signature Scheme without a Trusted Party

赖永东[1,2],钟 诚[1]
LAI Yong-dong[1,2],ZHONG Cheng[1]

(1.广西大学计算机与电子信息学院,广西南宁 530004;2.广西壮族自治区社会保险事业局,广西南宁 530022)
(1. School of Computer and Electronics and Information, Guangxi University, Nanning, Guangxi, 530004, China; 2. Social Insurance Bureau of Guangxi, Nanning, Guangxi, 530022, China)

摘要:应用现实生活中"分权"的思想和 (t,n) 门限群签名技术,提出一种改进的无需可信任第三方的时控代理签名方案.该方案在对签名时间验证服务上,不再由一个可信的第三方来提供,而是由一个群体(t 个人)来对代理签名时间和待签名的消息实行二级签名,能够避免 (t,n) 门限群签名时消息浏览权被扩大化和防止消息被泄密,除了满足代理签名的所有性质外,还能确定代理人签名的准确时间,当代理权被滥用时,授权人还可以将代理权撤销.

关键词:代理签名 门限群签名 可信中心 时间标志
中图法分类号:TN918 **文献标识码**:A **文章编号**:1002-7378(2008)02-0106-04

Abstract:By the concept of decentralized power in real life and (t,n) threshold multi signature, an improved time stamped proxy signature scheme without a trusted party is presented. In this paper, the verification server of time stamped is offered not by a trusted party but by (t,n) threshold multi signature. In the meantime, to avoid the messages are read by non authorization, the time-stamped and messages are signed on two levels. First, the time stamped is signed by the threshold multi-signature scheme. Then the messages with time stamped are signed by proxy. This presented scheme satisfies all the security requirements for proxy signature. A verifier also can ascertain the proxy time. Moreover, the original signer can revoke delegations whenever necessary.

Key words:proxy signature,threshold multi-signature,trusted authority, time stamp

自从 Mambo,Usuda 和 Okamoto[1]提出代理签名概念以来,如何防止和处理代理权被滥用的问题一直为学者们所关注.一般而言,要对代理人实施有效控制,避免代理人滥用代理权,必须解决三个问题:一是如何防止代理权被滥用,二是代理权被滥用或代理期限失效后如何撤销代理权;三是如何防止代理人否认其在代理有效期内签名.文献[2]提出具有授权证书的部分代理签名和门限代理签名方案,通过在授权信息中包含代理有效期的方法来实现对代理签名期限的限制.由于无法能知道代理人签名的确切时间,因而该方案不是一个十分有效的方法.文献[3]基于前向安全技术,利用可信第三方(TTP)来生成签名时间和对签名时间进行验证,提出一种签名接收方可查的时控代理签名方案.文献[4]提出具有跟踪接收者的时间戳代理签名方案,通过可信第三方提供时间戳来保证被签文件的顺序,从而防止伪造签名.文献[5,6]利用第三方提供时间戳服务实现代理权的可撤销问题.利用一个可信或不可信的第三方提供时间戳服务,不仅会给系统带来性能瓶颈的问题,而且一旦第三方被攻击也会给系统带来不可估量的损失.文献[7]提出一种没有第三方参与的时控代理签名方案,但是该方案并不安全[8].文献[9]提出需要可信任中心和无需可信任中心的 $(t,$

收稿日期:2008-03-18
修回日期:2007-09-27
作者简介:赖永东(1968-),男,硕士研究生,高级工程师,主要从事网络信息安全和计算机应用技术研究。

n) 门限群签名方案.但是,无需可信任中心的(t,n)门限群签名方案存在着签名伪造攻击问题[10].因此,我们在前人的基础上,给出一种改进的无需可信第三方的时控代理签名方案.

1 方案的基本思路

方案在对签名时间验证服务上,不再由一个可信的第三方来提供,而是由一个群体(t 个人)来共同对签名时间进行验证和签名;同时,为了避免(t,n)门限群签名时消息浏览权被扩大化和防止消息被泄密,方案利用现实生活中"分权"的思想,将代理签名分成二级签名,首先由(t,n)门限群签名负责代理签名时间的验证签名,然后代理人再对消息和代理签名时间进行签名.

2 方案的描述

2.1 系统初始化

系统初始化分为确定系统参数集和群公钥及分存秘密的生成两个部分.

2.1.1 授权人确定系统参数集

系统参数集(p,q,α,$H(x,y)$)中,p和q是两个大素数,且$q|(p-1)$,$2^{511}<p<2^{512}$,$2^{159}<q<2^{160}$,α是$GF(p)$中阶为q的元素,$H(x,y)$是单向Hash函数.授权人的私钥为x_A,其公钥为$y_A=\alpha^{x_A}\bmod p$;代理人的私钥为x_B,其公钥为$y_B=\alpha^{x_B}\bmod p$.

2.1.2 群公钥及分存秘密的生成

方案要求文献[9]无需可信任中心的(t,n)门限群签名方案中的成员i在广播$\{x_i,y_i\}$的同时,也广播x_i'.这样,其他成员$j(j=1\sim n,j\neq i)$可以利用x_i'来验证y_i.通过各成员间的相互验证,保证所有的$y_i(i=1\sim n)$不能被伪造.设群体N共有n个成员,每个成员$i(i\in N)$随机选择一个次数不超过($t-1$)的多项式$f_i(x)$,并随机选择两个整数,x_i,$k_i(1\leq x_i,k_i\leq p-1)$,其中$x_i$代表成员$i$的身份.然后计算:

$y_i=\alpha^{a_i \bmod q}\bmod p$,其中$a_i=f_i(0)$.

$x_i'=\alpha^{k_i\cdot a_i \bmod q}\bmod p=y_i^{k_i}\bmod p$.

成员i将$\{x_i,x_i',y_i\}$作为公钥向其他成员$j(j=1\sim n,j\neq i)$广播,并将多项式$f_i(x)$作为秘密参数保存.当成员j收到成员i发送来的$\{x_i,x_i',y_i\}$后,验证$x_i'\overset{?}{\equiv}y_i^{k_i \bmod q}\bmod p$是否成立,若成立,则成员$j$接受成员$i$的$\{x_i,x_i',y_i\}$.

当所有成员都广播了$\{x_i,x_i',y_i\}$并互相得到验证后,就可以决定群公钥:

$$y=\prod_{i\in N}y_i\bmod p=\alpha^{\sum_{i\in N}f_i(0)\bmod q}\bmod p.$$

在生成群签名后,成员i向其他成员$j(j\in N,j\neq i)$秘密分发分存秘密:

$u_{ij}=g_{ij}+f_i(x_j)\bmod q$,$1\leq g_{ij}\leq q-1$,

$y_{ij}=\alpha^{u_{ij}}\bmod p$,

$z_{ij}=\alpha^{g_{ij}}\bmod p$.

成员j接收到后u_{ij},y_{ij},z_{ij},公开y_{ij},z_{ij}.

2.2 授权

2.2.1 对代理权的生效时间L_B进行(t,n)门限群签名

授权人将代理权的生效时间L_B传递给N中的成员,当N中的t个成员(设这些成员构成集合T)同意对L_B进行签名时,每个成员$i(i\in T)$随机选择$k_i(1\leq k_i\leq q-1)$,计算$r_i=\alpha^{k_i}\bmod p$,并将r_i广播给T中其他成员.各成员$i(i\in T)$获得所有的$r_j(j\in T)$后,计算自己的部分签名s_i:

$$R=\prod_{i\in T}r_i\bmod p=\alpha^{\sum_{i\in T}k_i \bmod q}\bmod p,$$

$$E=H(L_B,R)\bmod p,$$

$$s_i=f_i(0)+\sum_{j\in N,j\notin T}\left(u_{ji}\cdot\prod_{l\in T,l\notin\{i\}}\frac{0-x_l}{x_i-x_l}\right)+k_i\cdot E \bmod q.$$

随后,成员$i(i\in T)$将$\{L_B,x_i,r_i,s_i\}$发送给一个既定的签名合成成员DC(Designated Combiner,该成员为授权人).签名合成成员DC根据

$$\alpha^{s_i}\overset{?}{\equiv}\left(y_i\cdot\left(\prod_{j\in N,j\notin T}y_{ji}\right)^{\prod_{l\in T,l\notin\{i\}}\left(\frac{x_l}{x_i-x_l}\right)\bmod q}\right)\cdot r_i^E\bmod p,\quad\forall i\in T$$

验证每个签名是否正确.若每个成员$i(i=1\sim t)$的$\{L_B,x_i,r_i,s_i\}$都正确,则签名合成成员DC就可以生成群签名$\{L_B,B,R,S\}$,其中$S=\sum_{i\in T}s_i \bmod q$,然后验证群签名$\{L_B,B,R,S\}$的有效性.验证者首先计算$E$和$F$:

$$E=H(L_B,R)\bmod p,$$

$$F=\prod_{i\in T}\left(\left(\prod_{j\in N,j\notin T}z_{ji}\right)^{\prod_{l\in T,l\notin\{i\}}\left(\frac{0-x_l}{x_i-x_l}\right)}\right)\bmod p.$$

然后判断$\alpha^S\overset{?}{\equiv}y\cdot F\cdot R^E\bmod p$是否成立[9].如果成立就认为群签名$\{L_B,B,R,S\}$是有效的.

2.2.2 授权人生成授权证书

授权证书c_A包括授权说明、代理人身份、代理权生效时间L_B以及代理权失效时间L_E等信息.授权人生成授权证书c_A,并将c_A广播.

2.2.3 生成代理权

授权人随机选取$k_A(1\leq k_A\leq p-1)$,并计算:

$r_A = \alpha^{k_A} \bmod p$,

$\sigma_A = k_A + x_A H(c_A, r_A) \bmod q$,

然后,授权人将$\{c_A, r_A, \sigma_A\}$传送给代理人.

2.2.4 代理人验证$\{c_A, r_A, \sigma_A\}$

代理人收到$\{c_A, r_A, \sigma_A\}$之后,验证$\alpha^{\sigma_A} \stackrel{?}{\equiv} r_A y_A^{H(c_A, r_A)} \bmod p$是否成立,若不成立,则要求授权人重发或终止协议;如果成立,代理人就可以生成代理私钥σ_p和代理公钥y_p:

$\sigma_p = \sigma_A + x_B H(c_A, r_A) \bmod q$,

$y_p = \alpha^{\sigma_p} = r_A y_B y_A^{H(c_A, r_A)} \bmod p$.

由于本方案是将代理人身份(包含在授权证书中)和代理人私钥x_B以及公钥y_B嵌入生成代理私钥σ_p和代理公钥y_p的算式中,然后用代理私钥σ_p对消息签名,所以验证者就可以验证签名确为代理人所为.

2.3 代理签名

代理人生成签名时间L_n,将L_n传递给N中的成员,当N中的t个成员同意对L_n进行签名时(判断$L_B < L_n < L_E$是否成立,如成立则表示同意),则开始对L_n进行(t,n)门限群签名,签名过程类似于对L_B进行(t,n)门限群签名过程,所不同的是签名合成成员DC由代理人担任.这样,代理人就得到了签名时间L_n的门限群签名$\{L_n, B, R, S\}$,然后随机选取$g(1 \leqslant g \leqslant p-1)$,并计算:

$U = \alpha^g \bmod p$,

$V = g + \sigma_p H(m, U) \bmod q$,

$\{m, c_A, r_A, U, V, L_n, B, R, S\}$就表示对消息$m$的代理签名.

2.4 签名验证

验证者首先验证签名时间L_n的有效性(验证过程类似于对L_B进行验证的过程),如果L_n有效,那么验证者计算$y_p = r_A y_B y_A^{H(c_A, r_A)} \bmod p$,然后验证$\alpha^V \stackrel{?}{\equiv} U \cdot y_p^{H(m,U)} \bmod p$是否成立,若成立,验证者就可以认为代理签名$\{m, c_A, r_A, U, V, L_n, B, R, S\}$是有效的.这是因为$\alpha^V = \alpha^{(g+\sigma_p H(m,U)) \bmod p} \bmod p = \alpha^g \cdot \alpha^{\sigma_p H(m,U)} \bmod p = U \cdot y_p^{H(m,U)} \bmod p$.

2.5 代理权的撤销

当授权人需要撤销代理人的代理权时,首先生成代理权失效时间L_E,然后采取与对L_B进行(t,n)门限群签名相同的方式对L_E进行(t,n)门限群签名,并将(c_A, L_B, L_E)在群体N内广播.如果代理人在L_E之后申请L_n的(t,n)门限群签名,那么由于$L_n > L_E$,所以L_n就无法通过(t,n)门限群签名验证,从而实现授权人在L_E时间点撤销代理权.

3 方案的安全性分析

应用现实生活中"分权"的思想,以及(t,n)门限群签名技术改进的无需可信任第三方的时控代理签名方案,除了满足代理签名的所有性质外,还能确定代理人签名的准确时间,当代理权被滥用时,授权人还可以将代理权撤销,具有较高的安全性.

3.1 无需可信任第三方

本方案在没有可信第三方参与下,利用(t,n)门限群签名技术提供对代理签名时间进行控制,不仅可以解决代理权被滥用问题,也解决了因使用一个第三方参与带来的系统性能瓶颈和一旦第三方被攻击给系统带来损失的问题.

3.2 可验证性

本方案的代理签名$\{m, c_A, r_A, U, V, L_n, B, R, S\}$中包含授权证书$c_A$和由授权人生成的$r_A$,验证者能够相信授权人认同了这份签名.另外,验证者通过检查$L_B < L_n < L_E$,可以确信签名的时间是在有效期限内.

3.3 不可伪造性

由于在签名时使用了代理人的私钥,因此,除代理人之外,任何人也无法伪造有效的签名.

3.4 可识别性

在授权证书c_A中包含了代理人的身份标识,因此从代理签名中可以确定代理人的身份.

3.5 强不可否认性

因为在签名时使用了代理人的私钥,所以代理人就不能否认他所做的签名,同时,在没有可信第三方参与下,使用(t,n)门限群签名就可以验证签名时间的有效性,使得代理人无法否认其在代理有效期内的签名.

3.6 防止滥用性

方案不仅在授权证书中对代理人签名行为进行限制,还通过(t,n)门限群签名技术对签名时间进行验证,确保了代理签名是在限定的范围和限定的时间内进行.

3.7 代理权的可撤销性

一旦授权人发现代理权被滥用,授权人就发布经过(t,n)门限群签名的代理失效时间L_E,这样,当代理人申请的签名时间L_n超过代理失效时间L_E时,L_n就无法通过(t,n)门限群签名验证,从而实现授权人在L_E时间点撤销代理权的功能.

参考文献:

[1] Mambo M,Usuda K,Okamoto E. Proxy signature for delegating signing operation: proceedings of the 3rd ACM Conference on Computer and Communications Security [M]. New Delhi, India, New York: ACM Press,1996:48-57.

[2] Zhang K. Threshold proxy signature schemes: proceedings of the 1st International Workshop on Information Security [C]. Berlin: Springer-Verlag, 1997:191-197.

[3] 吴克力,郝鹃,刘凤玉. 签名接收方可查的时控代理签名方案[J]. 计算机应用,2003,23(6):38-39.

[4] Sun H M. Design of time-stamped proxy signatures with traceable receivers [J]. IEE Proc-Comput Digit Tech,2000,147(6):462-466.

[5] Lu E J L, Hwang M S,Huang C J. A new proxy signature scheme with revocation [J]. Applied Mathematics and Computation,2005,161(3):799-806.

[6] 宋夏,戚文峰. 基于双线性映射的可撤销代理权的代理签名[J]. 信息工程大学学报,2006,7(4):330-335.

[7] 甘元驹,黎群辉,施荣华. 一种可追踪接收者的时控代理签名方案[J]. 计算机工程与应用,2004,40(10):140-141.

[8] 谢琪. 对可追踪接收者的时控代理签名的改进[J]. 计算机工程与应用, 2005,41(4):134-135.

[9] Li C T, Hwang T,Lee N. Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders: proceedings of Eurocrypt'94, LNCS 950 [C]. Berlin: Springer-Verlag, 1995: 194-204.

[10] 王贵林,王明生,季庆光,等. LHL 门限群签名方案的安全缺陷[J]. 计算机学报,2001,24(9):897-902.

(责任编辑:邓大玉)

(上接第 105 页)

打印功能。首先用 CommonDialog 控件调出显示打印选项,然后打印 Picture 中的内容。

窗体中的雨量图形文件也可以另存为别的文件名,实现的过程也是利用 CommonDialog 控件调出"文件另存为"的对话框,然后另外保存图形。

利用 Surfer7.0 绘制出来的广西自动气象站雨量图(图 2)既清晰又直观,对比图中的色标,广西各自动气象站雨量的大小和空间分布一目了然。

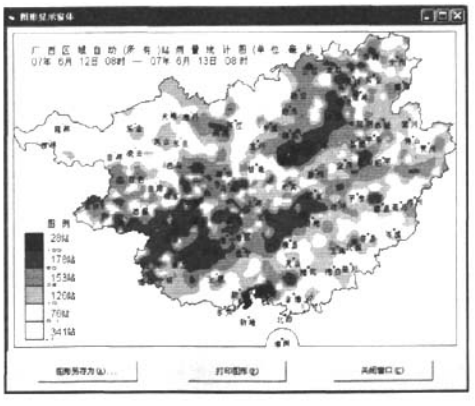

图 2 广西自动气象站雨量图形显示窗体

3 结束语

利用 Visual Basic 6.0 结合 Surfer7.0,通过数据处理、图形绘制、图形显示输出 3 个模块,可以方便快捷地完成广西自动气象站雨量图的绘制工作,而且绘制出来的图形清晰直观。在日常业务中,它有利于预报员及时了解各地天气细微变化,提高预报的准确率。在暴雨、洪涝天气时,它有利于各级领导随时掌握广西各地降雨情况,及时采取正确的防灾措施。另外,只要修改数据调用参数,也可以完成自动气象站其它要素的图形显示。

参考文献:

[1] 何瀚原,李清华,史源香. 利用 Sufer 软件绘制山西区域气象要素图[J]. 科技情报开发与经济,2007,17(4):234-235.

[2] 林伙海,吴陈锋. 基于 Surfer8.0 实现雨量图形可视化[J]. 气象,2006,32(7):115-118.

[3] 王志春,杨军,胡桂杰. 基于 Surfer Automation 接口的气象等值线图的绘制[J]. 内蒙古气象,2006(3):31-33.

[4] 文雅,郭治兴. 应用 Win-Surfer 软件绘制降水等值线图[J]. 土壤与环境,2002,11(4):360-362.

(责任编辑:韦廷宗)