前向安全的代理盲签名方案

张 席,杭欢花
ZHANG Xi,HANG Huan-hua

深圳大学 计算机软件学院,广东 深圳 518060
Computer Software Institute,Shenzhen University,Shenzhen,Guangdong 518060,China
E-mail:hanghuanhua@tom.com

ZHANG Xi, HANG Huan-hua.Forward secure proxy blind signature scheme.Computer Engineering and Applications, 2010,46(24):101-103.

Abstract: The valid signer may take the consequences caused by the disclosure of the private signature key,and the loss will be invaluable.To solve this problem,forward secure scheme has been suggested.This paper proposes a new forward secure proxy blind signature scheme on the basis of the concept of forward security and proxy blind signature.In the new scheme,even if an adversary has gotten the current proxy signature key in a time,it could not forge proxy signature pertaining to the past,that is,previous generated proxy signatures retain valid.Finally,this paper analyzes the correctness and security of the scheme.

Key words: cryptography;forward security;proxy blind signature;security analysis

摘 要: 密钥泄露问题对数字签名系统带来的后果是系统的崩溃,具有前向安全特性的数字签名体制就是针对密钥泄露问题提出的。基于前向安全性思想和代理盲签名理论,提出了一种新的具有前向安全性的代理盲签名方案。在该方案中,即使某一时刻代理签名者的密钥泄露,以前时段所产生的代理盲签名依然有效。对所提方案的正确性和安全性做了分析与讨论。

关键词: 密码学;前向安全;代理盲签名;安全分析
DOI:10.3778/j.issn.1002-8331.2010.24.030 **文章编号:**1002-8331(2010)24-0101-03 **文献标识码:** A **中图分类号:**TP309

1 引言

1982年Chaum首次提出了盲签名的概念[1],盲签名是指签名者并不知道所签文件的具体内容(即对签名者而言,消息被盲化处理过),而文件的拥有者又能从签名人关于盲化后消息的签名中得到签名人关于真实文件的签名。

1996年,Mambo、Usuda和Okamoto[2]提出代理签名的概念。代理签名是指在原始签名者不在或不方便做出签名时,将签名权委派给其他人,一个被指定的代理签名者可以代表原始签名者生成有效的签名。

随着电子现金和匿名选举技术的不断发展,在现实社会里,人们经常需要把自己的签名权委托给可靠的代理人,让代理人代表本人行使这种权力,所以,需要将以上所提的两种数字签名相结合。2000年,Lin和Jan提出了代理盲数字签名的概念[3],并给出了解决这个问题的一种方法。代理盲签名是代理签名中的一种特殊形式,这种方案在代理签名方案的基础上又兼有盲签名的性质。

然而,大部分代理签名方案都需要一个安全的信道来传送代理签名密钥,而在实际应用中,一个真正安全的信道是很难找到的,因此,当签名人的签名密钥泄露后,这些方案都不能提供任何保护,之前所产生的签名将变成无效。如何减少由于密钥泄露所带来的对系统安全的影响,一直是人们十分关注的研究课题。

1997年,R.Anderson首次提出了前向安全的概念[4]。前向安全的基本思想就是:把整个有效时间分成若干个周期,在每个周期内使用不同的签名密钥产生签名,而验证签名的公钥在整个有效时间内都保持不变,即使当前周期的签名密钥被泄露,也并不影响此周期前签名的有效性,从而大大减少了由于签名密钥泄露而对系统带来的影响。

将前向安全的概念引入到代理签名体制,受到了业界普遍的关注。目前,已经提出了多种前向安全的签名方案、前向安全的代理签名方案[5-7]。本文基于前向安全的代理签名方案[6-7]、Schnorr盲签名方案[8]、Schnorr代理盲签名方案[9-10],将前向安全引入代理盲签名中,并做相应的改进,提出了一种新的前向安全的代理盲签名方案。

2 前向安全签名的基本概念

一个前向安全数字签名方案由4个算法组成:

$FS-SIG=(Gen, Upd, Sign, Verf)$

基金项目: 国家自然科学基金(the National Natural Science Foundation of China under Grant No.60903178)。
作者简介: 张席,男,副教授,研究方向:信息安全;杭欢花(1985-),女,硕士研究生,研究方向:信息安全。
收稿日期:2009-11-27 **修回日期:**2010-04-19

(1)密钥生成算法*Gen*:概率算法。该算法输入安全参数k(一般记为1^k)与时间周期总数T,输出(SK_0, PK),作为初始的私钥与公钥。

(2)私钥更新算法*Upd*:确定性算法。输入当前时间段j的私钥SK_j,通过单向函数输出下一时间段$j+1$的私钥SK_{j+1},删除SK_j。

(3)签名算法*Sign*:概率算法。以当前周期的私钥SK_j与待签名的消息m为输入,然后输出(j,σ),作为在第j个周期对消息m的签名。

(4)验证算法*Verf*:确定性算法。以公钥PK、消息m及给定签名(j,σ)为输入,然后输出1当且仅当(j,σ)为一个有效签名,否则就输出0。

3 方案具体实施步骤

3.1 初始化阶段

设A是原始签名人,B是代理签名人:

(1)系统首先选择$n=p_1p_2=(2qp'_1+1)(2qp'_2+1)$和一个阶为$q$的生成元$g\in Q_{R_n}$(即$g^q=1 \bmod n$),且$p_1=p_2=3 \bmod 4$,其中$p_1$、$p_2$、$p'_1$、$p'_2$、$q$都为安全的大素数,$Q_{R_n}$为模$n$的平方剩余集合,然后,选择一对整数$(e,d)$,满足$\gcd(e,\varphi(n))=1$,$\varphi(n)=(p_1-1)(p_2-1)$,$ed=1 \bmod \varphi(n)$,最后,选择一个安全的单项散列函数$h$,公布$(n,q,g,h,e)$。

(2)系统选择随机数$x_A\in Z^*_{R_n}$作为原始签名人A的私钥,计算$y_A=g^{x_A} \bmod n$作为其公钥,并通过安全通道发送(x_A,y_A)给用户A,公布A的公钥y_A。

(3)系统选择随机数$x_B\in Z^*_{R_n}$作为代理签名人B私钥,计算$y_B=g^{x_B} \bmod n$作为其公钥,并通过安全通道发送(x_B,y_B)给用户B,公布B的公钥y_B。

(4)原始签名人A制定代理授权书m_w,其中主要包括A和B的身份标识、时间周期$1,2,\ldots,T$、代理终止时间$\tilde{t}$、代理签名消息的范围等内容,公布m_w。

3.2 代理授权阶段

(1)原始签名人A选择随机数$k_A\in Z^*_{R_n}$,计算

$$r_A=g^{k_A} \bmod n,\sigma=k_Ar_A+x_Ah(m_w,r_A) \bmod q$$

这样,(r_A,σ)相当于对m_w的数字签名,A通过安全通道将(r_A,σ)秘密发送给代理签名者B。

(2)B收到(r_A,σ)后,验证等式

$$g^{\sigma}=r_A^{r_A}y_A^{h(m_w,r_A)} \bmod n$$

若等式成立,则B计算

$$\sigma_0=\sigma+x_B \bmod q,y_T=\left(\sigma_0^{2^{T+1}}\right)^{-e} \bmod n$$

将σ_0、y_T分别作为代理签名的私钥和公钥,公布y_T。

3.3 密钥更新阶段

在每个周期的开始,代理签名人B根据前一周期的密钥计算出此周期的密钥:$\sigma_j=\sigma_{j-1}^2 \bmod n$,其中,$\sigma_{j-1}$为第$j-1$周期的代理密钥,$\sigma_j$为第$j$周期的密钥,$j=1,2,\ldots,T$。然后,代理签名人立即删除前一个周期的密钥$\sigma_{j-1}$。

3.4 前向安全的代理盲签名产生阶段

设C为待签名消息m的拥有者,B和C通过交互共同产生消息m的代理盲签名:

(1)B选择随机数$k_1,k_2\in Z^*_{R_n}$,计算

$$t=\left(g^{k_1}\right)^{2^{T+1-j}} \bmod n,w=g^{k_2} \bmod n$$

将(t,w)通过安全通道秘密发送给消息拥有者C。

(2)盲化:C收到(t,w)后,选择盲化因子$\alpha,\beta\in Z^*_{R_n}$,计算

$$r=ty_T^{-\beta}\left(g^{-\alpha}w^{-\beta}\right)^{2^{T+1-j}} \bmod n$$

若$r=0$则重新选择α、β,否则计算

$$u=h(j\|r\|w\|m\|m_w),u'=u+\beta \bmod q$$

将u'通过安全通道秘密发送给B。

(3)盲签名:B收到u'后计算

$$z=\sigma_j^{u'} \bmod n,s'=k_1-k_2u' \bmod n$$

将盲签名(z,s')通过安全通道秘密发送给C。

(4)去盲:C收到(z,s')后,验证等式

$$t=\left(g^{s'}z^ew^{u'}\right)^{2^{T+1-j}}y_T^{u'} \bmod n$$

是否成立,若成立则计算

$$s=s'-\alpha \bmod q$$

则$\sigma(m)=(s,z,w,u)$,所以,$[j,(s,z,w,u),m,m_w]$即为消息m的代理盲签名。

3.5 前向安全的代理盲签名的验证

(1)首先,验证者判断代理签名权是否在$\tilde{t}$有效期内,即如果当前周期$>\tilde{t}$,则代理签名无效,否则,转(2)验证。

(2)计算$r'=\left(g^sz^ew^u\right)^{2^{T+1-j}}y_T^u \bmod n$,验证等式

$$u=h(j\|r'\|w\|m\|m_w)$$

是否成立,若成立则代理盲签名有效,否则无效。

4 安全模型

4.1 盲性

如果不存在多项式时间内的敌手能以不可忽略的优势赢得以下游戏,则称一个签名方案在适应性选择密文攻击下具有盲性。该游戏在敌手A(A是可控制签名的任何敌手,而非用户)和挑战者C之间进行,以及两个诚实的用户U_0、U_1。

(1)挑战者C生成密钥对(sk_u,pk_u),保密sk_u,并将pk_u发送给敌手A;

(2)询问:敌手A进行多项式次数的适应性签名询问,即A选择一个消息$m\in M$和拥有消息m的用户U,询问C关于m的签名结果$\sigma(m)$,作为回答,C将$\sigma(m)$发送给A;

(3)A产生两个明文$m_0,m_1\in M$和任意一个私钥sk_s。挑战者C选择数$b\in_R\{0,1\}$,消息$\{m_b,m_{1-b}\}$等同于$\{m_0,m_1\}$;

(4)敌手A与拥有消息m_b、m_{1-b}的用户U_0、U_1合作对消息进行签名,最后,用户得到签名$\sigma(m_b)$和$\sigma(m_{1-b})$,并将其发送给A作为挑战密文;

(5)猜测:A执行多项式次数的询问。最后,输出一个值b'作为对b的猜测。如果$b'=b$,则A赢得游戏。A的优势定义为

$\left|\Pr[b'=b]-\frac{1}{2}\right|$。

4.2　不可伪造性

如果不存在多项式时间内的敌手能以不可忽略的优势赢得以下游戏，则称一个签名方案在适应性选择密文攻击下具有不可伪造性。该游戏在敌手F(F是可控制的任何用户的敌手，而非签名者)和挑战者C之间进行。

(1)挑战者C生成密钥对(sk,pk)，保密sk，并将pk发送给敌手F；

(2)敌手F进行多项式次数的适应性签名询问(每次询问依赖于以前询问的结果)：F选择一个消息$m\in M$和盲化因子，询问C关于m的签名结果，作为回答，C将$\sigma(m)$发送给A；

(3)最后A输出一个集合$\{(m_1,\sigma(m_1))(m_2,\sigma(m_2))\cdots(m_j,\sigma(m_j))\}$($j>1$)，如果对于$(m_i,\sigma(m_i))(1\le i\le j)$满足签名验证条件且都不是直接由签名预言机产生的，则F赢得了游戏。

4.3　前向安全性

在不同的密码学方案中，前向安全有不同的定义，它依赖于方案的安全目标。在盲签名中，前向安全是指，即使当前的签名密钥被泄露，之前时间段的签名仍然是有效的，具有不可伪造性。

5　方案安全性分析

5.1　正确性

证明等式$t=\left(g^{s'}z^{e}w^{u'}\right)^{2^{T+1-j}}y_T^{u'}\bmod n$的正确性：

$$\left(g^{s'}z^{e}w^{u'}\right)^{2^{T+1-j}}y_T^{u'}\bmod n=\left(g^{k_1-k_2u'}\sigma_j^{u'e}g^{k_2u'}\right)^{2^{T+1-j}}\sigma_0^{-2^{T+1}eu'}\bmod n=$$
$$\left(g^{k_1}\right)^{2^{T+1-j}}\bmod n=t$$

证明等式$u=h(j\|r'\|w\|m\|m_w)$的正确性：

$$r'=\left(g^{s}z^{e}w^{u}\right)^{2^{T+1-j}}y_T^{u}\bmod n=\left(g^{s'-\alpha}z^{e}w^{u'-\beta}\right)^{2^{T+1-j}}y_T^{u'-\beta}\bmod n=$$
$$\left(g^{s'}z^{e}w^{u'}\right)^{2^{T+1-j}}y_T^{u'}\left(g^{-\alpha}w^{-\beta}\right)^{2^{T+1-j}}y_T^{-\beta}\bmod n=$$
$$t\left(g^{-\alpha}w^{-\beta}\right)^{2^{T+1-j}}y_T^{-\beta}\bmod n=r$$

因为$r'=r$，所以$u=h(j\|r'\|w\|m\|m_w)$。

5.2　盲性

在敌手A和挑战者C之间进行盲性游戏，假设A得到来自用户的对m_0、m_1的两个签名

$$(i,\sigma(m_b))=(i,(s_b,z_b,w_b,u_b))$$
$$(i,\sigma(m_{1-b}))=(i,(s_{1-b},z_{1-b},w_{1-b},u_{1-b}))$$

由签名者和用户之间的交互可知，(u',z,s')为共享数据，即对于签名者来说(u',z,s')是可见的。因此，对于任何给定的(u',z,s')和签名$(i,\sigma(m),m)$存在着唯一的盲化因子，这就防止了签名者确定给定的(u',z,s')相应的签名，因为盲化因子是随机的。

盲化因子α、β只能通过(u',z,s')和$(i,\sigma(m),m)$来计算，由算法可知$\beta=u'-u$，而α要通过$r=ty_T^{-\beta}\left(g^{-\alpha}w^{-\beta}\right)^{2^{T+1-j}}\bmod n$计算，但这是一个基于离散对数的不可解问题，因此，任何敌手A都不可能得到有用的消息来得到$b'=b$，他对b成功猜测的概率为1/2，即该方案具有盲性。

5.3　不可伪造性

在敌手F和挑战者C之间进行不可伪造性游戏，假设F选择盲化因子α、β询问C关于m的签名，得到盲签名结果(z,s')，如果F要伪造消息m_i的签名(z_i,s'_i)，根据算法，F可任取$k_{1i},k_{2i}\in Z_{R_n}^*$，计算

$$t_i=\left(g^{k_{1i}}\right)^{2^{T+1-j}}\bmod n,w_i=g^{k_{2i}}\bmod n$$

接着可取相同的α、β，计算

$$r_i=t_iy_T^{-\beta}\left(g^{-\alpha}w_i^{-\beta}\right)^{2^{T+1-j}}\bmod n,u_i=h(j\|r_i\|w_i\|m_i\|m_w)$$
$$u'_i=u_i+\beta\bmod q,s'_i=k_{1i}-k_{2i}u'_i\bmod n$$

但是$z_i=\sigma_j^{u'_i}\bmod n$，即便根据$z=\sigma_j^{u'}\bmod n$，由于大合数因式分解的困难问题，$\sigma_j$也不可计算，因此也无法得知$z_i$，又根据等式

$$t_i=\left(g^{s'_i}z_i^{e}w_i^{u'_i}\right)^{2^{T+1-j}}y_T^{u'_i}\bmod n,r_i=\left(g^{s_i}z_i^{e}w_i^{u_i}\right)^{2^{T+1-j}}y_T^{u_i}\bmod n$$

求z_i也大合数因式分解问题，是不可解的，所以，F就不可能伪造m_i的签名，因此，该方案具有不可伪造性。

5.4　前向安全性

方案的前向安全性是基于强RSA假定和模合数平方剩余难题，即当n为合数时，企图通过$\sigma_j=\sigma_{j-1}^2\bmod n$求$\sigma_{j-1}$是一个困难问题，因此，即使攻击者已获得当前周期$j$的代理签名密钥$\sigma_j$，他也无法求出周期$j$之前的代理密钥$\sigma_i(i<j)$。所以，即使当前的签名密钥被泄露，之前时间段的签名仍然是有效的，具有不可伪造性。

5.5　代理授权安全性

(1)根据$\sigma_0=\sigma+x_B\bmod q$，伪造者无法伪造$\sigma_0$，因为$\sigma$和B的私钥$x_B$对伪造者都是无法得到的。

(2)根据公布的公钥y_T，攻击者无法得到σ_0，这是因为$y_T=\left(\sigma_0^{2^{T+1}}\right)^{-e}\bmod n$，要求解$\sigma_0$，必须计算$\left(2^{T+1}\right)^{-1}\bmod\varphi(n)$，则需要对大合数$n$进行因式分解，这是个难解问题，所以攻击者不可能通过计算y_T伪造σ_0。

(3)A也不可能伪造B的代理签名，虽然A可得到σ，却无法得到B的私钥x_B，所以A也是不可能得到σ_0，总之，除了B，任何人都无法得到σ_0，也就不能伪造A的代理签名。

5.6　可区分性、可识别性

从代理签名的形式中可以看出代理签名和原始签名形式不同，即代理签名和原始签名是容易区分的；在代理签名中含有授权书m_w，m_w中包含原始签名者和代理签名者的身份，故任何人都可以确定代理签名者的身份。

6　结束语

目前，代理盲签名方案仍是数字签名理论的研究热点之一，如何减少由于代理签名密钥泄露所造成的损失是一个急待解决的问题。在代理盲签名体制的基础上引入前向安全数字签名思想，在一定程度上减少了签名密钥泄露的危害。然而，前向安全不能保证密钥泄漏以后时间段签名的安全性，敌

(下转145页)

表2　两种复合树的对代词的消解结果

	召回率/(%)	准确率/(%)	F值/(%)
LMSPT	81.2	69.1	74.6
RMSPT	81.2	71.0	75.8

MT树时，系统的性能最好，无论是准确率，还是召回率都有相应的提升。这也说明了中文的句子比英文复杂，而且经常存在多个名词连接在一起，子句之间也缺少明确的主从关系，所以中文需要更多的节点来表达照应语和先行词在句子中的结构，而英文只需要用MT树，保留其直接祖先节点就可以大致表达其结构。通过实验表明，合适的裁剪方式能显著提高中文的代词消解性能，采用RMSPT树，在NWIRE上F值达到了75.8%。

5　总结与展望

使用树核函数来进行指代消解，取得了不错的结果。相比于其他方法，通过树核来自动挖掘句法信息，从而免于手工提取规则和确定语义特征。通过对不同裁剪策略的考察表明，使用树核函数能有效地解决中文代词的消解。

从实验结果看，系统的准确率仍有待提高。下一步工作是考虑如何在现有的句法树基础上，在尽量不丢失结构信息的前提下裁剪冗余信息。对于不同的指代模式需要的子树也各不相同，如何去寻找一种自动的裁剪策略也是下一步要考虑的问题。将继续构建一个完整的中文指代消解平台，以便考虑所有短语的指代，而不仅仅局限于ACE2005提供的实体。此外，还可以尝试在句法树特征的基础上加入一些平面特征，而不是只通过规则来强制过滤。

参考文献：

[1] Soon W M，Ng H T，Lim D C Y.A machine learning approach to coreference resolution of noun phrase[J].Computational Linguistics，2001，27(4)：521-544.

[2] Ng V，Cardie C.Improving machine learning approaches to coreference resolution[C]//Proceedings of the 40th Annual Meeting of the Association for Computational Linguistics，2002.

[3] Yang X F，Zhou G D，Su J，et al.Coreference resolution using competition learning approach[C]//ACL'2003，Sapporo，Japan，7-12 July 2003：176-183.

[4] Yang X F，Su J，Zhou G D，et al.Improving pronoun resolution by incorporating coreferential information of candidates[C]//ACL'2004，Barcelona，Spain，21-26 July 2004：127-134.

[5] Yang X F，Su J，Tan C L.Improving pronoun resolution using statistics-based semantic compatibility information[C]//ACL'2005，Univ of Michgan-Ann Arbor，USA，25-30 June 2005：165-172.

[6] 王厚峰.指代消解的基本方法和实现技术[J].中文信息学报，2002(6)：9-17.

[7] 王厚峰.鲁棒性的汉语人称代词消解研究[J].软件学报，2005，16(5).

[8] 王厚峰.汉语中人称代词的消解研究[J].计算机学报，2001(2)：136-143.

[9] 王小斌.基于语篇表述理论的汉语人称代词的消解研究[J].厦门大学学报，2004(1)：31-35.

[10] 李国臣，罗云飞.采用优先选择策略的中文人称代词的指代消解[J].中文信息学报，2005(4).

[11] Hobbs J.Resolving pronoun references[J].Lingua，1978，44：339-352.

[12] Lappin S，Leass H.An algorithm for pronominal anaphora resolution[J].Computational Linguistics，1994，20(4)：525-561.

[13] Zelenko D，Aone C，Richardella A.Kernel methods for relation extraction[J].Journal of Machine Learning Research，2003(2)：1083-1106.

[14] Zhang M，Zhang J，Su J，et al.A composite kernel to extract relations between entities with both flat and structured features[C]//ACL'2006，Sydney，July 2006：825-832.

[15] Yang X F，Su J，Tan C L.Kernel-based pronoun resolution with structured syntactic knowledge[C]//ACL'2006，Sydney，July 2006：41-48.

(上接103页)

手的入侵到密钥泄漏被检测到可能需要一段时间，只有密钥泄漏被检测到才能进行密钥撤销的操作，这就意味着密钥泄漏之后到密钥撤销之前，可能有多个时间段的签名是不安全的，入侵者完全可以伪造这些时间段内的签名，所以，对于密钥泄漏以后时间段签名的安全性保证显得尤其重要。这将成为以后数字签名研究的热点问题和方向。

参考文献：

[1] Chaum D.Blind signatures for untraceable payments[C]//Advances in Cryptology Crypto'82.[S.l.]：Springer-Verlag，1983：199-203.

[2] Mambo M，Usuda K，Okamoto E.Proxy signatures for delegating signing operation[C]//Proc 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]//Proceedings of International Conference on Chinese Language Computing，Illinois，USA，2000：273-277.

[4] Anderson R.Two remarks on public key cryptology[C]//The Fourth ACM Computer and Communication Security.New York：ACM Press，1997：151-160.

[5] 王晓明，陈火炎，付方伟.前向安全的代理签名方案[J].通信学报，2005，26(11)：38-42.

[6] 王亮，贾小珠.基于离散对数的前向安全代理签名方案[J].青岛大学学报：自然科学版，2007，20(2)：46-49.

[7] 夏祥胜，洪帆，崔国华.一个前向安全的代理签名方案的分析与改进[J].微电子学与计算机，2008，25(10)：172-174.

[8] Okamoto T.Provable secure and practical identification schemes and corresponding digital signature schemes[C]//Crypto'92.New York：Springer Verlag，1992：3-52.

[9] Tan Z，Liu Z，Tang C.A proxy blind signature scheme based on DLP[J].Journal of Software，2003，14(11)：1931-1935.

[10] 谷利泽，张胜，杨义先.代理盲签名方案及其在电子货币中的应用[J].计算机工程，2005，31(16)：11-13.