基于身份的代理签名方案

李 沛[1],王天芹[2]
(1.河南农业大学 河南 郑州 450002;2.河南大学 计算机与信息工程学院,河南 开封 475004)

摘 要:代理签名具有丰富的密码特性,在代理签名中原始签名人可以将签名权利下放给代理签名人,从而将自己从"繁琐"的签名事务中解放出来。随着对双线性映射的研究和应用,人们发现使用双线性映射可以有效简化传统的基于"证书"密钥管理和密钥分发技术。文中以双线性映射和Schnorr签名方案为基础,合理融入代理签名机制,提出一种基于身份的代理签名方案。对新方案进行安全性分析,证明在CDHP问题难解性前提下,具有不可伪造性、密钥依赖性等特性。

关键词:基于身份;双线性映射;代理签名;可证明安全
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2011)05-0155-03

ID-Based Proxy Signature Scheme from Bilinear Pairings

LI Pei[1], WANG Tian-qin[2]
(1. Henan Agriculture University, Zhengzhou 450002, China;
2. Computer & Information College, Henan University, Kaifeng 475004, China)

Abstract: Proxy singature has rich password characteristics. In the proxy signature, original signer's signature right transferred to proxy signer, thus theirself liberated from "trival" signature affairs. Along with bilinear map of research and application, people found using bilinear map can effectively simplified traditional "certificate" based key management and key distribution technology. In this paper, a new proxy is proposed which reasonable into proxy signature mechanism and based on bilinear map and Schnorr signature scheme. Finally on the new scheme, gave a security analyses, and proofed that under the CDHP difficult problem, this scheme has the non-forgeability, key dependence and other properties.

Key words: identity-based; bilinear map; proxy signature; proven safety

0 引 言

1996年Mambo等人首次提出了代理签名方案[1],在该方案中原始签名人可以将自己的签名权利委托给"合法的"代理签名人进行签名,使自己从"繁琐的"签名事务中解放出来。该方案提出了代理委托协议,决了签名权利委托的问题。由于代理签名具有丰富的密码特性,可以广泛应用到电子商务、电子政务等领域,使得代理签名成为信息安全领域的研究热点之一。随着双线性映射理论的研究和应用,国内外学者发现使用双线性映射可以高效地实现基于身份的密码系统[2~13]。基于身份的密码技术是以用户的公开身份为依据,产生用于加密、签名等用途的密钥,以此来简化传统的基于公钥证书的密钥管理技术[3~7]。

文中以Schnorr[4,5]提出的基于身份的签名方案为基础,引入代理委托协议,提出一种基于身份的代理签名方案。本方案满足代理签名方案的基本性质,可以应用于以"TA"为法人主体的系统环境中[4,5,13]。

1 方案理论基础

文中所用的双线性映射[4~7]是指一个循环加法群和一个循环乘法群之间的相对线性映像关系。设G_1和G_2是阶为大素数q循环加法群和循环乘法群,其生成元分别是P和g。定义双线性映射$e:G_1\times G_1\rightarrow G_2$,对于$\forall P,Q,R\in G_1$和$\forall a,b,\exists c\in Z_q^*$满足下列的基本性质:

(1)双线性:

$e(P,Q+R)=e(P,Q)e(P,R)$ $e(P+Q,R)=e(P,R)e(Q,R)$

$e(aP,bQ)=e(abP,Q)=e(P,abQ)=e(P,Q)^{ab}$

(2)非退化性:

对任何$P\in G_1$,存在$Q\in G_1$,使得$e(P,Q)=g^{c}\neq 1$ $e(P,P)=g$

收稿日期:2010-10-09;**修回日期**:2011-01-17
基金项目:国家自然科学基金(10671056);许昌学院科研基金(2011B050)
作者简介:李 沛(1982-),男,河南焦作人,助理实验师,硕士,研究方向为密码学、信息安全;王天芹,教授,博士,研究方向为数论与密码学。

(3)可计算性:

对所有的 $P,Q \in G_1$,存在有效的算法计算 $e(P,Q)$

在 G_1 和 G_2 中具有以下数学难题的定义:

1)离散对数问题(DLP):给定 $P,Q \in G_1$,找到一个正整数 $a \in \mathbb{Z}_q^*$,使得 $Q=aP$;给定 $\beta \in G_2$,找到一个正整数 $\alpha \in \mathbb{Z}_q^*$,使得 $\beta = g^\alpha$。

2)计算 Diffie-Hellman 问题(CDHP):设 $a,b \in \mathbb{Z}_q^*$,给定 $aP,bP \in G_1$,计算 $abP \in G_1$。

3)双线性 Diffie-Hellman 问题(BDHP):设 $a,b,c \in \mathbb{Z}_q^*$,给定 $aP,bP,cP \in G_1$,计算 $e(P,P)^{abc} \in G_2$

2 基于身份的代理签名方案

为了描述方便,设 A 表示原始签名人,B 表示代理签名人。

2.1 系统初始化

法人机构 TA 选择两个阶为大素数 q 的循环群 $(G_1,+)$与$(G_2,\cdot)$,以及第二节定义的双线性映射 e。选取三个密码意义上的随机语言模型[3-7]:$H_1:\{0,1\}^* \to G_1$、$H_2:\{0,1\}^* \times G_2 \to \mathbb{Z}_q^*$、$H_3:\{0,1\}^* \to \{0,1\}^m$,其中 $m \in \mathbb{Z}_q^*$。计算系统主密钥:随机选取 $s \in \mathbb{Z}_q^*$ 作为主私钥,计算 $P_{TA}=sP$ 作为主公钥,即 (s,P_{TA})。最后公开系统参数:$(G_1,G_2,e,P,q,H_1,H_2,H_3,P_{TA})$。

2.2 用户密钥生成

设 ID_A 和 ID_B 分别表示 A 和 B 的公开的、唯一可识别的身份。TA 对他们进行离线身份识别后,计算:$Q_A=H_1(ID_A)$ $Q_B=H_1(ID_B)$,Q_A和Q_B分别作为 A 和 B 的基于身份 ID 的公钥。计算:$d_A=sQ_A$,$d_B=sQ_B$,并通过安全信道分别将 d_A 和 d_B 传送给 A 和 B。双方接收到密钥之后,分别通过等式 $e(d_n,P)=e(Q_n,P_{TA})$ $(n=A \text{ or } B)$ 来验证密钥在传输过程中是否安全,如果安全则接受,否则请求 TA 重新发送。

2.3 代理密钥生成

A 为 B 建立一个授权证书 Cer(其中详细记载了 A 和 B 的身份信息,之间的授权信息和授权关系,还包含说明该授权关系的使用限制、有效日期、使用次数等内容)。代理委托协议是 A 执行 Schnorr 签名算法,对授权证书 Cer 进行签名,之后将签名和 Cer 绑定,并通过发送给 B。B 通过公开的系统参数对签名和 Cer 进行验证,已决定是否接受签名委托。具体协议如下:

1)原始签名人 A:执行 Schnorr 签名算法对授权证书进行签名,签名算法如下:随机选取 $k \in \mathbb{Z}_q^*$,

$$P_k=kP \quad r=e(P_k,P)$$

$$V=H_2(H_3(\text{Cer}),r) \quad U=Vd_A+P_k$$

A 将签名和证书绑定并 $((U,r)\|\text{Cer})$ 发送给 B,保密 k、P。

2)代理签名人 B:代理签名人收到 $((U,r)\|\text{Cer})$ 后,首先分离签名和证书,然后验证等式:$e(U,P)=e(Q_A,P_{TA})^V r$ 是否成立?若成立,则说明是合法授权,计算代理签名私钥 $S=U+d_B$;否则,认为授权是非法的并拒绝代理授权。

2.4 基于 Schnorr 方案的代理签名方案

1)B 对消息 M 进行代理签名,签名算法如下:对于随机选取两个随机数 k_1, $k_2 \in \mathbb{Z}_q^*$,定义代理签名:

$$\text{sig}=((U',r',r)\|\text{Cer})$$

其中

$$r'=e(P_1,P_2) \quad U'=V'S+k_2P_1$$

$$V'=H_2(M,r') \quad P_1=k_1P=(x_1,y_1) \quad P_2=k_2P=(x_2,y_2)$$

代理签名人保密 k_1, k_2, P_1, P_2。若 x_1 或 x_2 或 y_1 或 y_2 中有一个为 0(模 q),则重新选取 k_1, k_2。

2)验证算法:

对于代理签名 $((U',r',r)\|\text{Cer})$ 有效性验证是通过下面计算完成的:

首先计算:

$$V=H_2(H_3(\text{Cer}),r) \quad V'=H_2(M,r')$$

然后验证等式:

$$\text{ver}((U',r',r)\|\text{Cer})=\text{true} \Leftrightarrow e(U',P)=(e(Q_B,P_{TA})e(Q_A,P_{TA})^V r)^{V'r'}$$

是否成立?

3 安全性分析

本节主要讨论方案的安全性,前提是假设 DLP、CDHP 和 BDHP 是难解的。在安全性分析之前,先来证明该方案的正确性。

首先计算:

$$V_A=H_2(H_3(\text{Cer}),r) \quad V'=H_2(M,r')$$

然后计算:

$$\begin{aligned}
&(e(Q_B,P_{TA})e(Q_A,P_{TA})^V r)^{V'r'}\\
&=(e(Q_B,sP)e(Q_A,sP)^V r)^{V'r'}\\
&=(e(d_B,P)e(Vd_A,P)e(P_k,P))^{V'r'}\\
&=(e(d_B,P)e(U,P))^{V'r'}\\
&=e(S,P)^{V'r'}\\
&=e(V'S,P)e(P_1,P_2)\\
&=e(V'S+k_2P_1,P)=e(U',P)
\end{aligned}$$

等于左边,故等式成立。由本方案生成是正确的。

从方案中可以看到,TA 是用户密钥的生成机构,可以成功伪造出用户的签名,但是在以 TA 为法人主体的系统环境中,我们始终认为 TA 是诚实可信的。

因此,将可能受到的攻击分为三类:

I:来自普通用户的伪造攻击,此类攻击主要伪造代理签名。

II:来自系统中其他用户的伪造攻击,此类攻击主要伪造代理签名。

III:来自代理签名人的伪造攻击,此类攻击主要针对伪造原始签名人的签名,达到滥用签名权利的目的。

定理 1 假设 DLP、CDHP、BDHP 是难解的,在随机语言模型下,本方案具有不可伪造性。

证明:现在针对上面提出的三类攻击进行分析,首先通过生成的代理签名 $((U',r',r) \| \mathrm{Cer})$ 来看,攻击者需要伪造原始签名人的签名和代理签名人的签名。再次通过签名算法可知,生成的原始签名和代理签名的关键在于可以成功伪造出原始签名人的签名私钥和代理签名人的签名私钥,具体分析如下:

I:对于第一类攻击者,普通攻击者可以通过向 TA 发送自己的 ID,获取公钥和私钥,然后伪造出授权证书和原始签名人的签名,以此来生成"有效地"代理签名。根据授权证书的内容可知,此类攻击的成功的关键是伪造原始签名人对授权证书的签名。

首先,从原始签名人的签名 $((U,r) \| \mathrm{Cer})$ 生成等式:

$$r = e(P_k, P) \quad V = H_2(H_3(\mathrm{Cer}), r)$$

$$U = Vd_A + P_k$$

来看,第一类攻击者成功的关键是成功伪造出原始签名人的签名私钥 d_A',而 d_A' 是由 TA 生成的,因此攻击者不停地向 TA 发送 ID 序列 $(\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_n)$,以期望能获取 d_A',即请求-响应攻击。假设存在一个多项式时间敌手 Oscar 能够以一个不可忽略的概率 ε 产生一个有效的消息-签名对,则可以构造一个模拟算法 M 能够同样以一个不可忽略的概率 ε 解决 CDHP 问题和 DLP 问题。

令 q_H 为至多可向随机语言模型 H_1 提问的次数,q_H 的大小由安全参数 k 的多项式来限制。为了简化证明,假定所有的询问是不同的,要想求解 CDHP 问题,需要求解 d_A,最终可以化解到求解 TA 的密钥 s。Oscar 向随机语言模型 H_1 进行到第 $i(1 \leq i \leq q_H)$ 次询问时,模拟算法 M 给出一个响应 $Q_i = H_1(\mathrm{ID}_i)$ 并发送给 TA,TA 计算 $d_{\mathrm{ID}i} = sQ_i$,回复给 M,Oscar 输入随机数 (k_1', k_2'),模拟算法 M 以一个不可忽略的概率 ε 产生一个"有效的"签名 $((U^1,r^1) \| \mathrm{Cer})$。重复执行算法,执行 $2/\varepsilon$ 次算法后,可得到另外一个"有效的"签名 $((U^2,r^2) \| \mathrm{Cer})$。

此时根据这两个签名的有效性可知,敌手 Oscar 可以通过计算等式 $e(U^1, P) = e(U^2, P)$ 来计算出 s,从而求解了 CDHP 问题。即

$$s = ((V^1 - V^2)(j^1V^1 + i^1 - j^2V^2 - i^2)^{-1} + u) \bmod q$$

由于假定 CDHP 问题是困难的,故敌手 Oscar 成功伪造原始签名人的签名的概率可以忽略,从而就保证了授权证书的不可滥用性。同样采用此种方式,普通攻击者无法成功伪造出代理签名。

其次,假设普通攻击者采用类似于"投硬币"的游戏来产生原始签名人的密钥。

假设有一个"有效的"算法来判定攻击者选取的 $s' \in \mathbb{Z}_q^*$ 是否认系统主密钥,若是则输出 true,否则输出 false,则每次成功或失败的概率均为 $\frac{1}{2}$。由于 q 是一个大素数,即 $\log_2 q \geq 162$(q 的二进制表示的长度),则假设攻击者执行 n 次该算法后,成功获取 s,则其的概率为 $\frac{1}{2^n}$。随着算法执行次数的增加,成功的概率呈指数级减小。因此,小概率事件原理,通过这种方式伪造攻击不可行。

最后,来看看对授权证书 Cer 的伪造,由于证书中明确记载了原始签名人和代理签名人的身份信息、授权信息和使用权限、范围等信息。普通攻击者需要伪造一个授权证书 Cer' 使得 $H_3(\mathrm{Cer}') = H_3(\mathrm{Cer})$,由于 H_3 是我们定义的随机语言,故要想找到这个 Cer' 在计算上是不可行的。

通过这三种分析,得到结论:普通攻击者无法成功伪造出有效的代理签名。

II:对于第二类攻击者,这类攻击者处于系统之中,主要攻击目的就是伪造原始签名人的签名和授权证书。然后将此证书发送给代理签名人,已达到"伪装"成原始签名人的目的。根据针对第一类攻击者的分析可知,此类攻击者也需要伪造出原始签名人的身份 ID',使得 $H_1(\mathrm{ID}_A) = H_1(\mathrm{ID}')$。由于 H_1 是我们定义的随机语言,所以根据对第一类攻击者的分析过程可知,第二类攻击者在 DLP、CDHP 和 BDHP 困难性假设下无法找到这样的 ID' 和 Cer'。

III:对于第三类攻击者,攻击者的主要目的是伪造出授权证书 Cer',使得 $H_3(\mathrm{Cer}') = H_3(\mathrm{Cer})$,由于 H_3 是我们定义的随机语言,故要想找到这个 Cer' 在计算上是不可行的。此时如果攻击者转向伪造原始签名人的 ID',使得 $H_1(\mathrm{ID}_A) = H_1(\mathrm{ID}')$,则根据对第一类攻击者的分析可知,在 DLP、CDHP 和 BDHP 困难性假设下无法找到这样的 ID'。

综上所述,在 DLP、CDHP 和 BDHP 困难性假设下,本方案可以抵抗此三类攻击者的伪造攻击,因此本方案具有不可伪造性。代理签名除了应具有不可伪造性之外,还应该具有不可滥用性、密钥依赖性、可识别

(下转第 162 页)

持度下检测速度、入侵检测率进行了试验，实验表明，最小支持度越小，检测速度越慢，规则生成的时间越长，生成的规则越多，误报率可能性越大，若支持度太大，则相反，但检测率可能越低，造成漏报率较高，经多次实验，本系统将最小支持度设为 0.3，在检测速度、检测率和误报率上找到一个平衡点。

5 结束语

文中重点研究网络取证中的数据获取、分析与数据挖掘 Apriori 算法的应用，并进行了实验模拟。系统把数据挖掘、模式匹配和协议分析技术结合起来，先对获取的原始数据预处理、协议分析，再根据分析结果和挖掘生成的网络数据包关联规则记录，调用相应的犯罪特征库进行模式匹配，这样大大减少了匹配的次数，提高了检测效率。模拟实验表明，Apriori 算法的应用提高犯罪行为识别效率，发现新的犯罪行为，使取证工作处于主动状态；系统完整地重构犯罪行为，使证据更具完整性和法律效率。

参考文献：

[1] 王 玲，钱华林. 计算机取证技术及其发展趋势[J]. 软件学报，2003，14(9)：1635-1644.

[2] Ayers D. A second generation computer forensic analysis system[J]. Digital investigation，2009(6)：34-42.

[3] Wang Shiuh-Jeng，Kao Da-Yu. Internet forensics on the basis of evidence gathering with Peep attacks[J]. Computer Standards & Interfaces，2007，29：423-429.

[4] 张有东，曾庆凯，王建东. 网络协同取证计算研究[J]. 计算机学报，2010，33(3)：504-512.

[5] 国光明，洪晓光. 基于日志挖掘的计算机取证系统的分析与设计[J]. 计算机科学，2007，34(12)：299-302.

[6] Brueckner S，Guasparia D，Adelsteina F，et al. Automated computer forensics training in a virtualized environment[J]. Digital investigation，2008(5)：105-111.

[7] Sua Ming-Yang，Yub Gwo-Jong，Lin Chun-Yuen. A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach[J]. Computers & Security，2009，28：301-309.

[8] 林 英，张 雁，欧阳佳. 日志检测技术在计算机取证中的应用[J]. 计算机技术与发展，2010，20(6)：254-256.

[9] 赵 骞，崔益民，邹 涛. Bloom filter 在网络取证中的应用研究[J]. 计算机工程与应用，2010，46(14)：90-94.

[10] 杨卫平，黄烟波，段丹青，等. 基于协议分析的网络入侵动态取证系统设计[J]. 计算机技术与发展，2006，16(4)：215-217.

[11] Thonnard O，Dacier M. A framework for attack patterns' discovery in honeynet data[J]. Digital investigation，2008 (5)：128-139.

[12] 范 明. 数据挖掘：概念与技术[M]. 孟小峰，译. 北京：机械工业出版社，2003.

(上接第 157 页)

性、可区别性的特点。

4 结束语

代理签名是一种特殊的签名，它广泛地应用于电子商务、电子政务等领域。在文中，以 Schnorr 提出的基于身份的签名方案为基础，合理引入代理委托协议，提出一种基于身份代理签名方案。在双线性群中 DLP、CDHP 和 BDHP 问题难解性的假设下，本方案被证明是安全的。本方案满足代理签名方案所具有的基本特性，具有重要的实际应用价值。

参考文献：

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

[2] 杨义先，钮心忻. 应用密码学[M]. 北京：北京邮电大学出版社，2005.

[3] Shamir A. Identity-based cryptosystems and signature schemes[C]//LNCS196：Advances in Cryptology：Crypto'84. Berlin：Springer，1984：47-53.

[4] 杨 波，肖国镇. 现代密码学[M]. 第 2 版. 北京：清华大学出版社，2007：124-128，186-200.

[5] 徐茂智，游 林. 信息安全与密码学[M]. 北京：清华大学出版社，2007：178-197.

[6] Boneh D，Franklin M. Identity-based encryption from the weil pairing[C]//LNCS 2139：Advances in Cryptology，Crypto 2001. Berlin：Springer，2001：213-229.

[7] Boneh D，Lynn B，Shacham H. Short signature from the weil pairing[C]//LNCS 2248：Advances in Cryptology，Asiacrypt 2001. Berlin：Springer，2001：514-532.

[8] Paterson K. ID-based signatures from pairing on elliptic curves. [EB/OL]. 2002. http://epring. iacr. org.

[9] 蔡光兴，陈 华. 高效的基于 ID 的无可信中心签名方案[J]. 计算机应用研究，2009，26(7)：2752-2753.

[10] 周 亮，李大鹏，杨义先. 基于身份的无需可信任 PKG 的签名方案[J]. 通信学报，2008，29(6)：9-11.

[11] Stinson D R. 密码学原理与实践[M]. 第 2 版. 冯登国译. 北京：电子工业出版社，2003：233-261.

[12] 王泽成. 基于身份的代理签名和盲签名[J]. 计算机工程与应用，2003，39(23)：148-150.

[13] 李 沛，王天芹，潘美姬. 基于身份的签名方案[J]. 计算机工程与应用，2008，44(14)：103-106.