基于双线性对的代理签名

蔡庆华,陈文莉
(安庆师范学院 计算机与信息学院,安徽 安庆 246011)

摘 要:双线性映射作为一种构建密码体制的新工具,在密码学领域中引起了普遍的关注,并在数字签名中得到应用。在代理签名方案中,代理签名人可以代表原始签名人生成签名;在代理多签名方案中,一个代理签名人可以同时代表多个原始签名人在文件上签名。利用椭圆曲线上的Weil配对的双线性性质构造了一个代理数字签名方案和一个代理多签名方案,并对它们的正确性和安全性做了分析。在代理多签名方案中,代理签名的长度均独立于原始签名人的个数,其验证也与一般的代理签名类似。

关键词:代理签名;代理多签名方案;双线性映射;Weil配对
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2006)09-0230-03

A Proxy Signature Based on Bilinear Pairing

CAI Qing-hua, CHEN Wen-li
(School of Computer Science and Information, Anqing Teachers' College, Anqing 246011, China)

Abstract: The bilinear pairings are useful tools in cryptography. And they have wide applications in digital signature. Proxy signature schemes allow a proxy signer to generate a proxy signature on behalf of an original signer. And proxy multi-signature schemes allow a proxy signer can generate a proxy signature on behalf of two or more original signers. A proxy signature scheme and a proxy multi-signature scheme are proposed by using the bilinear property of Weil pairing defined on elliptic curves, and their security and correctness are also analysed. The sizes of the proxy signatures in proxy multi-signature scheme is independent of the number of original signers. The verification is similar to that of ordinary proxy signatures.

Key words: proxy signature; proxy multi-signature scheme; bilinear map; Weil pairing

0 引 言

在现实商品交易、签订合同过程中,当某人(这里称为签名授权人)因公务或身体健康原因不能行使签名权时,一般可委托其秘书用其私章或公章代其签名。在电子商务活动中,如CA证书的签发、电子支票或电子货币的分发等同样要委派其他人替自己行使签名权,这就是文中要研究的代理签名[1]。

bilinear pairings是代数曲线的Weil pairing和Tate pairing,是构造基于身份的加密方案的重要工具。

假设G_1是一个由P产生的循环加法群,它的阶是q,G_2是一个阶为q的循环乘法群,则bilinear pairings是映射$e:G_1\times G_1\rightarrow G_2$。假定离散对数问题(DLP)在两个群上都是困难的,则bilinear pairings有以下性质[2]。

(1)双线性:对任意的P,Q,RG,有$e(P,Q+R)=e(P,Q)e(P,R)$;$e(P+Q,R)=e(P,R)e(Q,R)$;对任何$a\in Zq^*$,aP表示P自加a次,因而对任意的$a,b\in Zq^*$,有$e(aP,bQ)=e(P,Q)^{ab}$。

(2)非退化性:存在$P,Q\in G$,使得$e(P,Q)$不等于1。

(3)可计算性:对于$P,Q\in G$,存在一个高效的算法计算$e(P,Q)$。

设G是一个由P生成的阶为素数l的加法循环群($G=<P>$),假定在G上乘法和逆在单位时间内可计算出,且$a,b,c\in Zq^*$。

那么有以下4个数学问题:

a. DLP(离散对数问题):给定两个成员P和Q,很难找到一个存在的整数n使得$P=nQ$。

b. CDHP(计算上的Diffie-Hellman问题):给出(P,aP,bP),计算abP是困难的,不存在多项式时间算法。

c. DDHP(决定性的Diffie-Hellman问题):给出(P,aP,bP,cP),能够判断在Zq^*上$c=ab$是否成立。

d. GDHP:在素数阶循环群G上,DDHP在多项式时间内能够被解决,但没有任何可能的算法可以解决CDHP。

在素数阶循环群G上,DDHP在多项式时间内能被解决,但没有任何可能的算法可以解决CDHP,称G为GDH群。这样的群在有限域上的椭圆曲线上能够获得。下面的签名方案就是基于此类GDH群。

收稿日期:2006-01-06
基金项目:安徽省教育厅自然科学研究项目(2005KJ365zc)
作者简介:蔡庆华(1974-),男,安徽太湖人,讲师,硕士,研究方向为计算机网络与信息安全。

1 基于双线性对的数字签名

1.1 基本方案

以下为数字签名的基本方案[3]。

1)系统初始化。

设 G_1,G_2 分别是阶为 q 的加法群和乘法群,其中 q 是素数,在 G_1,G_2 中离散对数问题都是难解的。设 e 是由椭圆曲线上的 Weil 配对派生得到的一 $G_1 * G_1$ 到 G_2 的双线性映射,$H:\{0,1\}^* \rightarrow G_1$,是一公开的单向加密 Hash 函数。

2)密钥生成。

用户 A 随机选取一个整数 x 作为密钥,$x \in Zq^*$,计算公开点 $Y = xP$ 并将其作为公钥。

3)签名生成。

对于消息 m,签名者计算:$S = xH(m)$,S 即为消息 m 的签名。

4)签名验证。

消息接收方接收到明文签名文对(m,S)后,验证下式是否成立:

$e(S,P) = e(H(m),Y)$,若成立,则签名正确,否则签名不正确。

1.2 方案分析

正确性分析:$e(S,P) = e(xH(m),P) = e(H(m), xP) = e(H(m),Y)$

安全性分析:若假设 CDHP 是困难的,该体制已在随机预言模式下被证明对抗任意选择明文攻击是安全的。

2 基于双线性对的代理签名方案

设 G_1 为有限域 Fq 上的椭圆曲线有理点群的一个加法子群,P 是 G_1 的生成元;G_2 取这个有限域上的一个乘法子群,双线性映射 e 是由椭圆曲线上 Weil 配对派生得到,H_1,H_2 是单向 Hash 函数,其中 $H_1:\{0,1\}^* \rightarrow Zq^*$,$H_2:\{0,1\}^* \rightarrow G_1$,原始签名人和代理签名人私钥分别为 x_a 和 x_b,其公钥分别为 $Y_a = x_aP$ 和 $Y_b = x_bP$。

2.1 代理密钥生成

第一步:原始签名人 A 确定证书 m_w,在 m_w 中确定代理的诸多事宜,并计算 $S = x_aH_2(m_w)$,然后将 m_w 和 S 传给代理签名人 B。

第二步:代理签名人验证证书 m_w 的合法性,即检验下列方程是否成立:

$e(P,S) = e(Y_a, H_2(m_w))$

当且仅当上面等式成立时接受 S,代理签名人计算出 $X = S + x_bH_2(m_w)$,并将其作为自己的代理密钥。

2.2 代理签名生成

对某个消息 m,代理签名人用代理密钥 X 生成数字签名的过程如下:

代理签名人选择 $k \in Zq^*$ 后计算:$r = e(P,P)^k$,$v = H_1(m||r)$,$U = vX + kP$,则对消息 m 的代理签名为(U,v,m_w)

2.3 代理签名验证

签名接收人可用下列等式验证:$v = H_1(m||e(U,P)e(H_2(m_w), Y_a + Y_b)^{-v})$,如果成立,接收人就可接收签名,否则拒绝此签名。

3 方案分析

3.1 正确性分析

如果原始签名人 A 和代理签名人 B 都遵循协议,则验证者总接收此签名,事实上有:

$$e(U,P)e(H_2(m_w), Y_a + Y_b)^{-v} =$$
$$e(vX + kP,P)e(H_2(m_w), Y_a + Y_b)^{-v} =$$
$$e(v(S + x_bH_2(m_w)) + kP,P)e(H_2(m_w), Y_a + Y_b)^{-v} =$$
$$e(v(S + x_bH_2(m_w)),P)e(kP,P)e(H_2(m_w), Y_a + Y_b)^{-v} =$$
$$e((S + x_bH_2(m_w)),P)^v e(kP,P)e(H_2(m_w), Y_a + Y_b)^{-v} =$$
$$e(kP,P)e(H_2(m_w),(x_a + x_b)P)^v e(H_2(m_w), Y_a + Y_b)^{-v} =$$
$$e(kP,P)e(H_2(m_w), Y_a + Y_b)^v e(H_2(m_w), Y_a + Y_b)^{-v}) = e(kP,P) = r$$

因此有 $v = H_1(m||r) = H_1(m||e(U,P)e(H_2(m_w), Y_a + Y_b)^{-v})$,此代理签名将被接受。

3.2 安全性分析

下面从代理签名所应满足的特性:可区分性、可验证性、不可伪造性、强可识别性、强不可否认性和抗滥用性等对文中方案进行分析。

(1)可区分性:这一点很显然,因为有效的代理签名中包含有授权证书 m_w,而且证书 m_w、原始签名人和代理签名人的公钥都要在代理签名的验证过程中出现。

(2)可验证性:对消息 m 完整有效的代理签名为(m,Sm,U,m_w),从原始签名人发送的(δ,s)及其验证过程,验证人可以确信代理签名人拥有原始签名人对授权证书 m_w 的签名,一般来说证书 m_w 包含了代理签名人的身份信息和代理权限等,因此符合可验证性。

(3)不可伪造性:若第三方想冒充代理签名人和原始代理人对消息 m 伪造代理签名,但他没有原始签名人对授权证书 m_w 的签名 S,则不可能伪造;另一方面,原始签名人也不能伪造代理签名,因为代理签名人用原始签名人所不知的代理私钥和安全 GDH 签名产生代理签名。

(4)强可识别性:完整有效的代理签名有原始签名人授权证书 m_w,于是任何人都能从授权证书 m_w 上确定相应代理签名人的身份。

(5)强不可否认性:同强可识别性一样,完整有效的代理签名有原始签名人授权证书 m_w,在验证过程中都要用 m_w,而代理签名人不可能更改证书 m_w。所以代理签名人一旦产生了代理签名,他将不能否认所产生的代理签名。在验证过程中验证者必须用到代理签名人的公钥,因而他

们也不能否认自己产生的签名。

(6)抗滥用性:在我们的代理签名方案中用到了证书 m_w,用证书 m_w 规定了代理的权限。因此该方案具有抗滥用性。

4 基于双线性对的代理多签名方案

代理多签名体制,它允许一组原始签名人授权给一个代理签名人来代表他们。伊丽江等人[4]于 2000 年首先提出了代理多签名体制的概念和两个代理多签名体制,此后又有几个代理多签名体制[5,6]被提出。文中基于上述方案提出一新的代理多签名方案。

假设 $A_1, A_2, \cdots, A_n$ 表示原始签名人的组,对任意 $i \in \{1,2,\cdots,n\}$,A_i 的秘密密钥为 x_i,A_i 对应的公开密钥为 $Y_i = x_iP$,$A_1, A_2, \cdots, A_n$ 想把他们的签名权力委托给某个代理签名人 B。B 的公开秘密密钥对(x_b, Y_b)满足 $Y_b = x_bP$。原始签名人的组产生委任状 m_w,在委任状 m_w 中有关于委托关系的详细描述。

(1)代理密钥生成。每个原始签名人 $A_i(i \in \{1,2,\cdots,n\})$ 计算 $s_i = x_iH_2(m_w)$,然后 A_i 把 m_w 和 s_i 发送给代理签名人 B。B 收到后检验是否有 $e(S_i,P) = e(H_2(m_w),Y_i)$,如果这个等式成立则 B 计算 $X = s_1 + s_2 + \cdots + s_n + x_bH_2(m_w)$ 作为代理秘密密钥,而代理公开密钥为 $Y_1 + Y_2 + \cdots + Y_n + Y_b$。其中 B 的代理秘密密钥 X 只有 B 自己知道,其他人包括原始签名人 $A_i(i = 1,2,\cdots,n)$ 也无法知道。

(2)代理签名生成。对消息 M 代理签名人 B 利用基于双线性对签名机制(把 X 作为签名密钥)来获得代理签名 $S = XH_2(M)$。

代理签名验证收到消息 M 和代理签名 $S = XH_2(M)$ 后验证者利用原始签名人 $A_i(i = 1,2,\cdots,n)$ 和代理签名人 B 的公钥可以验证代理签名。他接受此代理签名当且仅当:

$$e(S,P) = e(H_2(M),H_2(m_w))(Y_1 + Y_2 + \cdots + Y_n + Y_b))$$

其方案正确性可由下述等式保证:

$$e(S,P) = e(xH_2(M),P) = e(H_2(M),XP) =$$
$$e(H_2(M),(s_1 + s_2 + \cdots + s_n + x_bH_2(m_w))P) =$$
$$e(H_2(M),(x_1 + x_2 + \cdots + x_n + x_b)H_2(m_w)P) =$$
$$e(H_2(M),H_2(m_w))(Y_1 + Y_2 + \cdots + Y_n + Y_b))$$

5 小 结

双线性配对被用来构造密码体制,包括加密体制和签名体制。文中利用双线性配对提出了一个新的代理签名体制、一个新的多代理签名体制。新体制最重要的一点是,代理签名的长度均独立于原始签名人或代理签名人的个数。

参考文献:

[1] Mambo M, Usuda K, Okamoto E. Proxy Signature for Delegating Signing[A]. In Proc 3rd ACM Conference on Computer and Communications Security[C]. New York: ACM Press, 1996.

[2] 马春波,何大可. 基于双线性映射的卡梅隆门限签名方案[J]. 计算机研究与发展, 2005,42(8):1427-1430.

[3] Bonch D, Lynn B, Shacham H. Short signatures from the Weil pairing[A]. In: Advances in Cryptology - Asiacrypt' 2001[C]. Lecture Notes in Computer Science 2248. Heidelberg: Springer,2002.514-532.

[4] Yi Lijiang,Bai Guoqiang,Xiao Guozhen. Proxy multi-signature scheme :A new type of proxy signature scheme[J]. Electronic Letters,2000,36(6):527-528.

[5] Hwang S J,Chen C C. A new proxy multi-signature scheme [A]. In: Proceedings of International Workshop on Cryptology and Network Security[C]. Taiwan: Springer - Verlag, 2001.26-28.

[6] Sun H. On proxy multi-signature schemes[A]. In: Proceedings of International Computer Symposium[C]. Taiwan: Springer-Verlag,2000.65-72.

(上接第 229 页)

5 总 结

网络端点接入控制的概念提出了怎样控制单个网络端点的安全级别,较好地解决了让用户更方便、更安全地接入网络的问题。相信在其被广泛应用之后,整个网络环境安全水平都会有大幅度的提高。

参考文献:

[1] 中国互联网络信息中心. 中国互联网络发展状况统计报告(2005/1)[EB/OL]. http://www.cnnic.net.cn/download/2005/2005011801.pdf,2005.

[2] 国家计算机网络应急技术处理协调中心. CNCERT/CC2005 年上半年网络安全工作报告[EB/OL]. http://www.cert.org.cn/upload/2005CNCERTCCAnnualReport.pdf,2005.

[3] Roberts P F. Startups Rush to Fill Network Access Control Void[EB/OL]. http://www.eweek.com/article2/0,1895,1860588,00.asp,2005-09-19.

[4] 思科网络准入控制计划首度"接触"中国厂商[EB/OL]. http://news.xinhuanet.com/it/2005-01/10/content_2439189.htm, 2005-01-10.

[5] Rasmussen M. Demand for Endpoint Security Growing, Forrester Research[EB/OL]. http://www.csoonline.com/analyst/report2170.html,2004,01-30.

[6] 李 军. 渐成热门的网络端点安全技术[J]. 计算机安全, 2005(1):14-16.