基于椭圆曲线的代理盲签名方案

赵泽茂

(杭州电子科技大学通信工程学院,浙江 杭州 310018)

摘要:利用多元线性变换来说明签名协议过程中各种变量之间的转化关系,提出了一种基于椭圆曲线的代理盲签名方案.作为特例,列举了 4 种 ElGamal 型签名相应的代理盲签名方案,并对所提出方案的安全性进行了分析.分析结果表明,通过选取不同的参数组合,可以得到不同的方案,从而使得代理盲签名方案具有较大的选择空间,可广泛应用于有匿名性要求的领域.

关键词:盲签名;代理盲签名;椭圆曲线密码体制

中图分类号:TP309 **文献标识码**:A **文章编号**:1000-1980(2006)03-0329-04

盲签名的概念最早是由 Chaum① 于 1982 年提出的.所谓盲签名是指签名人不知道所签消息的具体内容,这种技术广泛应用于具有匿名性要求的领域,如电子货币系统和电子选举系统等.1996 年,Mambo 等[1] 介绍了代理签名的概念,之后提出了各种代理签名,如完全代理、部分代理、具有授权特征的代理以及部分代理等[2].将代理签名与盲签名产生代理盲签名方案,Tan② 和谭作文等[3] 提出了一种基于 Schnorr 盲签名的代理盲签名方案,该方案既具有盲签名的性质又具有代理签名的性质.Lai 和 Awasthi[4] 于 2003 年也提出了一种代理盲签名方案.

本文在分析文献[3~4]的基础上,着重对协议过程中的变量进行了更加一般性的转化和处理,利用线性变换的形式来刻画协议过程中各种变量之间的转化关系,提出了一种基于线性变换的代理盲签名方案,以此方法构造的代理盲签名方案包括文献[3~4]中的方案.笔者将这种方法平移到椭圆曲线密码体制中来,从而得到了在椭圆曲线密码体制下的代理盲签名方案,并总结了以 4 个 ElGamal 型签名方案为基础的 4 种相应的代理盲签名方案.

1 有限域上的椭圆曲线密码体制及系统参数

a. 选取定义在有限域 F_q 上的 1 条安全的椭圆曲线 E[3],使得 E 上的 F_q-有理点群的阶被 1 个大素数 n 整除,保证椭圆曲线上有理点群上的离散对数问题是难解的.

b. 选取一个基点 $G\in E$,G 的阶为 n,即有 $nG=O$,O 表示 1 个无穷远点.基点 G 公开.

c. 设 A 为系统的原始签名人,B 为 A 授权的代理签名人,A 的私钥为 $x_A\in_R Z_n^*$,$P_A=x_AG\in E$,P_A 作为 A 的公钥.B 的私钥为 $x_B\in_R Z_n^*$,$P_B=x_BG\in E$,P_B 作为 B 的公钥.公钥 P_A 和 P_B 均在系统内公开.并设 C 为信息拥有者.

d. 选取 1 种安全的 Hash 函数 $h(\cdot)$,在系统内公开.

2 基于椭圆曲线的代理盲签名方案介绍

谭作文等[3] 给出了基于椭圆曲线的代理盲签名方案,该方案包含委托过程、签名过程和验证过程,为便于符号的统一,本文对文献[3]中的符号作了相应的改动.主要结果如下:

a. 委托过程.

收稿日期:2004-09-20

作者简介:赵泽茂(1965—),男,四川蓬溪人,副教授,博士,主要从事密码学、网络信息安全研究.

① CHAUM D. Blind signature for untraceable payments. Advanced in Cryptologyt, Proc Crypto '82. Lecture Notes in Computer Science, Springer-Verlag, 1983:199-203.

② TAN Z, LIU Z, TANG C. Digital proxy blind signature schemes based on DLP and ECDLP. Beijing: Key Laboratory of Mathematics Mechanization Research, Academy of Mathematics and Systems Science, the Chinese of Academy of Sciences, 2002:212-217.

第1步:原始签名人A随机地选取1个整数 $k_A \in {}_R Z_n^*$ 且 $k_A \neq 1$,计算 $R_A = k_A G$, $r_A = x(R_A) \bmod n$, $\sigma = x_A r_A + k_A \bmod n$,将$(r_A, \sigma, R_p)$安全地传递给代理签名人B.其中 R_p 为原始签名人的授权验证公钥.

第2步:B收到(r_A, σ, R_p)后,检验 $R_p = \sigma G - r_A P_A$ 是否成立,如果成立,B接受A的委托,并计算 $s_p = \sigma + x_B \bmod n$.

b. 签名过程.

第1步:B任意地选取1个整数 $k_B \in {}_R Z_n^*$,且 $k_B \neq 1$,计算 $R_B = k_B G$,并将(R_p, r_A, R_B)传给C.

第2步:C随机地选取2个整数 $\alpha, \beta \in {}_R Z_n^*$,计算 $R_C = R_B + \beta G + (-\alpha - \beta) P_B + (-\alpha) R_P + (-\alpha r_A) P_A$, $r_C = x(R_C) \bmod n$, $e = h(r_C \| m)$, $e' = e - \alpha - \beta$, $U = (-e + b) R_C + (-e + b) r_A P_A - e P_A$,C将 e' 传递给B.

第3步:B计算 $s' = e' s_p + k_B \bmod n$,并将 s' 传给C.

第4步:C计算 $s = s' + \beta \bmod n$,则(m, s, e, U)就是最终得到的代理盲签名.

c. 验证过程.检验关系式 $e = h(x(sG - eP_B + eP_A + U) \| m)$ 是否成立,如果成立,则接受签名,否则,拒绝接受.

3 基于多元线性变换的代理盲签名方案

考虑到上述涉及的变量有 G, P_A, P_B, R_p, R_B 等,而且签名过程中的变量关系比较复杂,因此本文试图用更一般的形式进行刻画并推广,结果如下:

a. 委托过程.

第1步 委托产生阶段.A随机地选取1个整数 $k_A \in {}_R Z_n^*$ 且 $k_A \neq 1$,并计算 $R_A = k_A G$,不妨将其表示为 $R_A = (x(R_A), y(R_A))$,其中 $x(R_A), y(R_A)$ 分别表示椭圆曲线上点 R_A 的 x 坐标和 y 坐标,然后作模余运算,记 $r_A = x(R_A) \bmod n$,计算 $\sigma = k_A + r_A x_A \bmod n$,称这个方程为A的授权签名方程.又令 $R_p = \sigma G + P_B$, R_p 在系统内公开,是1个公开的变量,在签名验证时将用到,因此被称为原始签名人的授权验证公钥.

第2步 委托传递阶段.A将委托签名(σ, r_A)安全地传递给B.

第3步 委托验证阶段.B收到委托签名(σ, r_A)后,计算 $\tilde{R} = \sigma G - r_A P_A$,检验 $r_A = x(\tilde{R}) \bmod$ 是否成立,如果成立,则说明(σ, r_A)是A发送过来的,B接受A的委托,并代表A行使签名的权力.B计算 $s_p = \sigma + x_B \bmod n$, s_p 与授权验证公钥 R_p 相对应,满足关系式 $R_p = s_p G$,而且只有B才可能计算得到,因此称 s_p 为授权验证私钥(保密).否则,拒绝接受A的委托.

事实上,$\tilde{R} = \sigma G - r_A P_A = \sigma G - r_A x_A G = (\sigma - r_A x_A) G = (k_A + r_A x_A - r_A x_A) G = k_A G$,所以 $r_A = x(\tilde{R}) = x(k_A G) = x(R_A) \bmod n$ 成立.因此B接受A的委托,代表A进行签名.

b. 签名过程.

第1步:B接受A的委托后,任意地选取1个整数 $k_B \in {}_R Z_n^*$,且 $k_B \neq 1$,计算 $R_B = k_B G$,并将 R_B 传给C.

第2步:C得到 R_B 后,随机地选取4个整数 $\alpha, \beta, \gamma, \tau \in {}_R Z_n^*$,计算 $R_C = \alpha R_B + \beta R_P + \gamma P_B + \tau G$(称这个关系式为变量的多元线性变换),记 R_C 的 x 坐标为 $x(R_C)$,并计算 $r_C = x(R_C) \bmod n$.如果 $r_C = 0 \bmod n$,则需要重新选取这组参数使得 $r_C \neq 0$,然后计算 $e = h(r_C \| m)$,其中符号'‖'表示字符串和整数的二进制表示的连接,令 $e' = \alpha^{-1}(e - \beta) \bmod n$,C将 e' 传递给B.

第3步:B收到 e' 后,计算 $s' = k_B - e' s_p \bmod n$,并将 s' 传给C,B保留盲签名(e', s').

第4步:C收到 s' 后,计算 $s = \alpha s' + \tau \bmod n$, $U = \gamma P_B$,则(e, s, U)就是B代表A对消息 m 的代理盲签名.

c. 验证过程.

消息的接收者或验证者接收到消息 m 和签名(e, s, U)后,计算 $\tilde{r}_C = x(sG + eR_p + U) \bmod n$,判断 $e = h(\tilde{r}_C \| m)$是否成立,如果成立,则说明(e, s, U)就是消息 m 的有效代理盲签名,否则拒绝接收这个签名.

事实上,$sG + eR_p + U = (\alpha s' + \tau) G + eR_p + U = (\alpha k_B - \alpha e' s_p + \tau) G + eR_p + U =$

$$\alpha P_B - \alpha[\alpha^{-1}(e - \beta)] s_p G + \tau G + eR_p + U = \alpha P_B + \beta R_p + \gamma P_B + \tau G$$

因此,上述结论成立.

定理1 若将上述方案的代理签名过程中第3步的签名方程改为一般式 $ak_B = b + cs_p \bmod n$,其中参数(a, b, c)表示$(\pm s', \pm e', \pm 1)$的某一个置换,则有4种不同形式的代理盲签名方案.在这些方案中协议的整个过程都不变,产生变化的只是相应的2个变量替换式、签名方程和验证方程等,如表1所示.如果还考虑参

数前面符号的变化,那么可以得到 16 种不同的方案.

表 1　变量关系式、签名方程和验证方程

Table 1　Relational expression of variables, signature equation and verification equation

方案编号	变量关系式 1	签名方程	变量关系式 2	验证方程
一般式	$e'=e'(e,\alpha,\beta,\tau)\bmod q$	$ak_B=b+cs_p\bmod n$	$s=s(s',\alpha,\beta,e,\tau)\bmod q$	$\tilde{e}=h(x((a^{-1}b+\beta)G+(a^{-1}c+\alpha)R_p+U)\parallel m)$
N1	$e'=\alpha^{-1}(e-\beta)\bmod n$	$k_B=s'+e's_p\bmod n$	$s=\alpha s'+\tau\bmod n$	$\tilde{e}=h(x(sG+eR_p+U)\parallel m)$
N2	$e'=\alpha^{-1}(e-\tau)\bmod n$	$k_B=e'+s's_p\bmod n$	$s=\alpha s'+\beta\bmod n$	$\tilde{e}=h(x(eG+sR_p+U)\parallel m)$
N3	$e'=\alpha(e^{-1}-\tau)^{-1}\bmod n$	$e'k_B=1+s's_p\bmod n$	$s=\alpha e(e')^{-1}s'+e\beta\bmod n$	$\tilde{e}=h(x(e^{-1}G+e^{-1}sR_p+U)\parallel m)$
N4	$e'=\alpha(e^{-1}-\beta)^{-1}\bmod n$	$e'k_B=s'+s_p\bmod n$	$s=\alpha e(e')^{-1}s'+e\tau\bmod n$	$\tilde{e}=h(x(e^{-1}sG+e^{-1}R_p+U)\parallel m)$

证明　首先说明表 1 中方案 N1 的各变量关系式和签名方程选取的理由和依据. 方案 N1 的完整描述见本节的前半部分,代理签名人的签名方程为 $s'=k_B-e's_p\bmod n$,即 $k_B=s'+e's_p\bmod n$.

由于 $R_C=\alpha R_B+\beta R_P+\gamma P_B+\tau G=\alpha k_B G+\beta s_pG+\tau G+\gamma P_B$,将 k_B 代入得 $R_C=(\alpha s'+\tau)G+(\alpha e'+\beta)s_pG+\gamma P_B$,为了技术上处理的方便,不妨记 $k_C=(\alpha s'+\tau)+(\alpha e'+\beta)s_p$,则有 $R_C=k_CG+\gamma P_B$,为了便于构造签名方案中各变量的关系式,要求信息拥有者 C 的签名方程与代理签名人的签名方程在形式上保持一致,即要求 $k_C=s+es_p\bmod n$,从而有 $s=\alpha s'+\tau$,$e=\alpha e'+\beta$,即为表 1 中 N1 方案的变量关系式. 其余 3 种情况类似.

代理签名过程中签名方程的参数选取方法有很多种,本文只考虑比较简单的情形,也就是说(a,b,c)取自$(\pm s',\pm e',\pm 1)$的某一置换. 表 1 中的 4 种方案对应 4 种情形:$(1,s',e')$,$(1,e',s')$,$(e',1,s')$,$(e',s',1)$,每一种情形对应 4 种不同的符号,因此,有 16 种不同的方案.

如果(a,b,c)取$(s',1,e')$时,按照上面的处理办法,将得到如下的方程组:

$$\begin{cases}\alpha(s')^{-1}+\tau=s^{-1}\\ \alpha(s')^{-1}e'+\beta=s^{-1}e\end{cases}$$

从此方程组中不能求解得到关于 e'和 s 的关系式,故定理结论成立.

定理 2　在表1中列举的代理盲签名方案是代理强盲签名方案的概率为 $1-1/n^2$.

注　代理盲签名是由信息拥有者和代理签名人按照协议共同完成的,代理签名人不知道所签消息的内容,拥有盲签名(e',s'),信息拥有者 C 拥有代理盲签名(e,s,U),当(e,s,U)公布后,消息的接收者或验证者可以根据公共参数进行验证. 如果公布代理盲签名(e,s,U)后,代理签名人 B 可以凭借代理签名(e',s')将两者联系起来,这样,代理签名人就可以对信息拥有者进行追踪,据此,可以将代理盲签名分为代理强盲签名和代理弱盲签名.

所谓代理强盲签名是指代理签名人不能根据代理盲签名来判断该签名是由他的代理签名所产生,即签名人不能对原消息的拥有者进行追踪. 反之称为代理弱盲签名方案.

证明　以表 1 中的方案 N1 为例进行说明. 在消息拥有者 C 公布签名(e,s,U)后,B 保留了盲签名(s',e'),但不能从方程组

$$\begin{cases}s=\alpha s'+\tau\bmod n & (1)\\ e'=\alpha^{-1}(e-\beta)\bmod n & (2)\end{cases}$$

中解出求知参数 α,β,τ,因为两个方程中含有 3 个未知数.

又由于 $U=\gamma P_B$,虽然已知 U 和 P_B,但仍然不能求出 γ,因为这将面临求解椭圆曲线 E 的离散对数难题.

但值得注意的是:在上述方程组中,猜对其中一个参数的概率为 $1/n$,如果一个参数猜对的话,那么其余的 2 个参数也就可以从中解出了. 同样的道理,猜对 γ 的概率也为 $1/n$. 这样同时猜对的概率为 $1/n^2$. 当求得这 4 个参数时,B 就可以计算 $R'_C=\alpha R_B+\beta R_P+\gamma P_B+\tau G$,$r'_C=x(R'_C)\bmod n$,如果满足 $e=(r'_C\parallel m)$,则他可以判断 C 的签名就是由他的代理签名产生的. 因此定理的结论成立.

由于产生这种可能性的概率非常小,按照小概率原理,对这种情况几乎可以忽略不计,所以认为这些方案均是代理强盲签名方案.

4　方案的安全性及应用分析

在这些签名方案中,所有的验证过程均使用了原始签名人的授权验证公钥,这说明最终签名是通过原始

签名人的授权由代理签名人和信息拥有者共同完成的,同时也可以把 R_p 看成是代理盲签名的验证公钥.虽然各个方案的形式和特点不一样,但它们具有如下一些共同的性质.

a. 签名授权人签名的不可伪造性.在这些代理盲签名方案中,代理签名人 B 不能根据(σ,r_A)计算出签名授权人 A 的私钥 x_A,从而不能伪造 A 的签名,其安全性基于椭圆曲线的离散对数问题的难解性,也不能从签名方程 $\sigma = k_A + r_A x_A \bmod n$ 中获取 A 的私钥,因为签名方程中含有 2 个未知数 x_A 和 k_A,由此说明任何攻击者都难以伪造 A 的签名.

b. 代理盲签名的不可伪造性.因为代理签名密钥 $s_p = \sigma + x_B \bmod n$,其中含有 B 的私钥,所以只有 B 才能生成 s_p,尽管 $R_p = s_p G$,R_p 公开,但不能从中得到 s_p,因为这面临椭圆曲线的离散对数难题.因此除了 B 以外,其他任何人(包括 A 在内)都难以伪造一个有效的代理签名.

c. 代理盲签名的可区分性.在验证代理盲签名的有效时,要用到签名授权人公布的签名验证公钥 R_p,所以很容易将代理盲签名和原始签名区分开.

d. 代理盲签名的不可抵赖性.由于任何人都不能伪造原始签名人 A 的普通数字签名,所以 A 不能否认他的一个有效的普通数字签名.同样由性质 b 可以得到,由于除了代理签名人 B 以外,任何人都不能伪造 B 的代理签名,所以 B 也不能否认一个有效的代理盲签名.

e. 代理盲签名的可注销性.如果 A 想收回 B 的代理签名权,那么他就可以在系统内公布消息,宣布验证公钥 R_p 无效,从而 B 生成的所有代理盲签名随之失效.

f. 代理签名人和信息拥有者之间的联系性.根据上述分析,这些方案要么是代理强盲签名方案,要么是代理弱盲签名方案.如果是代理强盲签名方案,说明代理签名人 B 无法确认和信息拥有者 C 的签名联系起来,这种方案比较适合于有匿名性要求,同时又不能对签名追踪的领域,如电子货币支付系统、电子选举等领域.如果是代理弱盲签名方案,这时方案比较适合于有匿名性要求且又能对签名进行追踪的情况.

5 结 束 语

本文比较完整地给出了在椭圆曲线密码体制下如何运用线性变换来构造代理盲签名方案的方法,这种方法可以任意地选取不同的参数组合,从而使得产生代理盲签名方案具有较大的选择空间,再加上这种方案同时具备代理签名和盲签名的特点,因此可广泛应用于有匿名性要求的领域,如匿名电子选举和电子货币匿名支付系统等.

参考文献:

[1] MAMBO M. USUDA K, OKAMOTO E. Proxy signature for delegating signing operation[C]//Proc 3rd ACM Conference on Computer and Communication Security. New York: ACM Press, 1996: 48-57.

[2] 李继国. 代理签名的现状与进展[J]. 通信学报, 2003, 24(10): 115-125.

[3] 谭作文. 基于离散对数的代理盲签名[J]. 软件学报, 2003, 14(11): 1931-1935.

[4] LAI S, AWASTHI A K. Proxy blind signature scheme[J/OL]. Cryptology ePrint Archive, 2003, 10(1): 5-11[2003-07-02]. http://eprint.iacr.org/2003/072/.

Proxy blind signature scheme based on elliptic curve

ZHAO Ze-mao

(*School of Communication Engineering, Hangzhou Dianzi University, Hangzhou* 310018, *China*)

Abstract: Using the multi-linear transform formula to describe the conversion between various variables of the proxy signer and the message owner in signature protocol, a new proxy blind signature scheme based on an elliptic curve cryptosystem was proposed. As special examples, four proxy blind signature schemes based on ElGamal signature were listed, and the security of the proposed schemes was analyzed in details. By selection of different parameter sets of signature equation, different proxy blind signature schemes can be obtained, providing a wide range of parameter space to be selected. The proposed schemes can be applied to the field in which the anonymity is needed.

Key words: blind signature; proxy blind signature; elliptic curve cryptosystem