基于椭圆曲线的代理数字签名

白国强[1,2],黄 谆[1],陈弘毅[1],肖国镇[3]
(1. 清华大学微电子学研究所,北京 100084; 2. 西安交通大学数学系,陕西西安 710049;
3. 西安电子科技大学信息安全与保密研究所,陕西西安 710071)

摘 要: 现有的代理数字签名方案都是基于离散对数问题和大数因子分解问题的方案. 本文我们将代理签名的思想应用于椭圆曲线数字签名,提出了一种新的基于椭圆曲线离散对数问题的代理签名方案,并对方案的复杂性和安全性进行了分析. 在对方案的安全性分析中,我们还提出了两类椭圆曲线上的困难问题. 新方案不仅推广和丰富了代理签名的研究成果,而且也扩展了椭圆曲线密码的密码功能,为信息安全问题的解决提供了新的密码学方法.

关键词: 数字签名; 代理数字签名; 离散对数; 椭圆曲线离散对数; 椭圆曲线数字签名
中图分类号: TN918. 1 **文献标识码**: A **文章编号**: 0372-2112 (2003) 11-1659-05

Proxy Digital Signature Based on Elliptic Curves

BAI Guo-qiang[1,2], HUANG Zhun[1], CHEN Hong-yi[1], XIAO Guo-zhen[3]
(1. *Institute of microelectronics, Tsinghua University, Beijing* 100084, *China*;
2. *Department of Mathematics, Xi'an Jiaotong University, Xi'an, Shaanxi* 710049, *China*;
3. *Institute of information security, Xidian University, Xi'an, Shaanxi* 710071, *China*)

Abstract: Up to now all the known proxy digital signature schemes are based on discrete logarithmic problems or big number factorization problems. In this paper, we showed how to apply the idea of proxy digital signature scheme to elliptic curve digital signature algorithms by presenting a new proxy digital signature scheme based on elliptic curve discrete algorithmic problems. Furthermore, we also analyzed the new scheme's computation complexity and security problem. In the security analysis, we presented two hard problems over elliptic curves as well. The new scheme, which is an extension of elliptic curve cryptosystems, is beneficial for the construction of cryptographic schemes for solving some security problems.

Key words: digital signature; proxy digital signature; discrete logarithmic problems; elliptic curve discrete logarithmic problems; elliptic curve digital signature algorithm

1 引言

1996 年,M Mambao 等人在文献[1]中研究了代理数字签名问题,并提出了基于素数域的各种代理签名方案,为密码学和数字签名的研究与应用开辟了一个新领域. 利用代理签名方案,一个被称为原始签名人的用户可以将他的数字签名权委托给另外一个被称为代理签名人的用户. 对任何消息,代理签名人代表原始签名人可以生成对该消息的签名,任何知道原始签名人公钥的验证人,都可以对该消息的签名做出验证.

椭圆曲线密码[2]是一种基于椭圆曲线离散对数问题的公钥密码,1985 年由 N Koblitz 和 V Miller 分别提出,之后人们对其进行了大量研究. 作为一种公钥密码,椭圆曲线密码不仅有比较好的安全性,而且利用椭圆曲线离散对数问题可以同时构造三种基本形式的公钥体制,即公钥加密体制,密钥交换协议和数字签名方案等. 目前,椭圆曲线密码正在被应用于解决信息安全问题的实践中,而对椭圆曲线密码各种理论问题和实现技术的研究仍然是密码学和信息安全中的一个热点.

文献[2,3]讨论了与椭圆曲线有关的代理签名问题,但所述内容都不是 M Mambao 等人思想在椭圆曲线密码上的应用. 将 M Mambao 等人代理签名的思想应用于椭圆曲线密码,就能得到一种新的代理签名方案,即基于椭圆曲线的代理签名方案. 本文给出了这一方案,同时分析了这一方案的复杂性和安全性. 在分析其安全性的过程中还提出了两种椭圆曲线上的难解问题,并对其作了初步分析.

2 代理签名及椭圆曲线数字签名

2.1 代理签名

签名代表了签名人的一种权力. 在数字签名方案中,这种权力体现为签名人对自己私钥的拥有及使用. 在通常的手写签名意义下,这种权力的实现需要签名人直接在被签文件上

收稿日期:2002-12-12;修回日期:2003-07-11
基金项目:国家自然科学基金(No. 60273004);"863"课题资助(No. 2002AA140140)

签下代有自己特有书写习惯和书法特征的名字. 手写签名的这种权力不能转让. 但是,数字签名的权力可以转让. 在数字签名方案中,一个人只要拥有了签名人(下面称为原始签名人)的私钥,他就可以使用这一私钥象原始签名人一样能够完成对任何消息的签名. 在这个意义下他所具有的权力和原始签名人完全相同. M Mambao 等人在文[1]中构造了一种新的签名方案,这种新方案能够使原数字签名方案中的私钥拥有者,即原始签名人,将签名的权力委托给一个被称为代理签名人的人,同时又不暴露自己的私钥. 代理签名人利用原始签名人给他的委托信息能够完成对任何消息的签名. 对代理签名人产生的签名,任何具有原始签名人公钥的人都可以验证这种代理签名的真实性,并能同原始签名人的直接签名相区别.

一个代理签名方案至少需要三种不同类型人的参与,即原始签名人、代理签名人和代理签名的验证人. 为简单起见,本文中用 A 表示原始签名人,用 B 表示代理签名人和用 C 表示代理签名的验证人. 一个代理签名方案又至少包括四个过程,即初始化过程,数字签名权力的委托过程,代理签名的产生过程和代理签名的验证过程. 文献[4,5,6]等较详细地研究了各种基于离散对数问题和基于大数分解问题的代理签名方案.

2.2 椭圆曲线数字签名

为节省篇幅,有关椭圆曲线的基本概念请参阅文献[7]等,文中其它未经说明的符号也同文[7]. 下面设 E 是定义在有限域 F 上的一条椭圆曲线,其中 F 的特征可以是 2,也可以是其它素数. 用 $\#E$ 表示 E 中元素个数,并设 n 是 $\#E$ 的一个大素因子, $P\in E$ 是 E 中一个阶为的 n 点. 设 $Q=\omega P$,其中 ω 为一正整数, $0<\omega<n$, $Q\in E$. 则由 P 和 Q 求 ω 的问题称为椭圆曲线离散对数问题. 将 E, n 和 P 作为某一系统的公开参数,则以椭圆曲线 E 及 E 中点 P 为基点的椭圆曲线数字签名算法可叙述如下[5].

(1) 密钥对的产生. 随机选取正整数 k_A, $0<k_A<n$,做为用户 A 的私钥,然后计算 k_AP,记 $P_A=k_AP$. 则与用户 A 的私钥对应的公钥为 P_A;

(2) 签名的产生. 对任何消息 $m(0<m<n)$,用户 A 首先选取随机数 k,然后计算 kP. 记 $kP=(x,y)$,其中 $x,y\in F$. 最后,用户 A 利用自己的私钥 k_A 计算: ①$r\equiv x \bmod n$, ②$s\equiv k^{-1}(m+k_Ar) \bmod n$. 则用户 A 对消息 m 的签名是一组数 (m,r,s);

(3) 签名的验证. 对系统中的任一用户 C,当收到用户 A 的签名 (m,r,s) 后, C 首先获取 A 的公钥 P_A,然后进行下面的计算: ①$c\equiv s^{-1} \bmod n$, ②$u_1\equiv mc \bmod n$, ③$u_2\equiv rc \bmod n$, ④$u_1P+u_2P_A=(x,y)$, ⑤$r'\equiv x \bmod n$. 最后进行判断. 如果 $r'=r$,说明 m,r,s 确为 A 的签名.

对以上椭圆曲线数字签名算法的安全性,其基础是椭圆曲线离散对数问题的困难性.

3 基于椭圆曲线的代理签名方案

3.1 方案

按照组成一个代理签名方案的四个过程,我们提出基于椭圆曲线的代理签名方案如下.

(1) 初始化过程. 同第 2 节,假定 E 是定义在有限域 F 上的一条椭圆曲线, $P\in E$ 是 E 中一个阶为 n 的点,将 E, n 和 P 公开. 进一步假定 A 为原始签名人, A 的私钥为 k_A,公钥为 P_A,私钥 k_A 保密,公钥 P_A 公开. 公钥 P_A 和私钥 k_A 之间有关系 $P_A=k_AP$;

(2) 委托过程. 原始签名人 A 为了将其签名的权力委托给代理签名人 B,同时又不暴露自己的私钥 k_A, A 首先选取随机数 k_0,并计算 k_0P. 记 $Q_0=k_0P=(x_0,y_0)$,其中 $x_0,y_0\in F$. 然后 A 计算: $r_0\equiv x_0 \bmod n$ 和

$$\sigma\equiv(k_A+r_0k_0) \bmod n. \tag{1}$$

最后 A 将 σ 秘密地发送给 B,将 Q_0 可以公开地发送给 B. 以下称 (σ,Q_0) 为 A 将其签名权委托给 B 的委托信息.

代理签名人 B 收到一组委托信息 (σ,Q_0) 后,需验证以下等式是否成立:

$$\sigma P=P_A+r_0Q_0. \tag{2}$$

其中, P 是 E 的基点,为系统的公开参数, P_A 为原始签名人 A 的公钥. 对 P_A,我们假定代理签名人 B 应该有机会得到它. 对 r_0,可由 Q_0 计算得出. 若记 $Q_0=(x_0,y_0)$,则 $r_0\equiv x_0 \bmod n$. 如果等式(2)不成立,则代理签名人 B 必须拒绝接受委托信息 (σ,Q_0),认为 (σ,Q_0) 不是来自合法的原始签名人 A. 如果等式(2)成立,则说明 (σ,Q_0) 确实来自于原始签名人 A;

(3) 代理签名的产生过程. 对任何消息 $m(0<m<n)$, A 的代理签名人 B 可以按照下面的计算方法产生关于消息 m 的代理签名.

B 首先选取随机数 k, $0<k<n$,然后计算 kP. 记 $kP=(x,y)$,其中 $x,y\in F$. 接着 B 计算: ①$r\equiv x \bmod n$; ②$s\equiv k^{-1}(m+\sigma) \bmod n$. 则 (m,r,s,Q_0) 一起构成了代理签名人 B 对消息 m(代替 A 产生)的代理签名. 与普通签名比较,它多出了一个量 Q_0.

(4) 代理签名的验证过程. 任何一个验证人 C 收到代理签名 (m,r,s,Q_0) 后,利用原始签名人 A 的公钥 P_A,进行下列计算: ①$c\equiv s^{-1} \bmod n$; ②$u_1\equiv mc \bmod n$, $u_2\equiv rc \bmod n$; ③计算 $u_1P+u_2(P_A+r_0Q_0)$,设 $u_1P+u_2(P_A+r_0Q_0)=(x',y')$; ④计算 $x' \bmod n$. 如果 $x' \bmod n=r$,则代理签名 (m,r,s,Q_0) 得到验证. 验证过程的正确性可证明如下:

$$\begin{aligned} u_1P+u_2(P_A+r_0Q_0) &= mcP+rc(r_AP+r_0k_0P) \\ &= c(m+r(r_A+r_0k_0))P \\ &= s^{-1}(m+\sigma)P \\ &= kP \\ &= (x,y) \end{aligned}$$

可见,对验证人按照验证过程计算出的 x',有 $x'=x$. 因此 $x' \bmod n=x \bmod n=r$.

为保证方案的安全性,在代理签名的验证过程中,验证人 D 必须严格执行验证过程的计算步骤. 本文中,称这些步骤为代理签名的验证程序.

3.2 方案的复杂性

将以上方案和 2.2 节的椭圆曲线数字签名算法相比较,

不难看出新方案在代理签名产生过程所需要的计算量和椭圆曲线数字签名算法中签名的产生所需要的计算量完全相同.将新方案在验证过程中所需要计算量与椭圆曲线数字签名算法中验证过程所需计算量比较,新方案多出了一个椭圆曲线中的多倍点运算 $r_0 Q_0$ 和一次椭圆曲线上的点加运算 $(P_A + r_0 Q_0)$.除此之外,新方案在委托过程中还多了一个椭圆曲线中的多倍点运算 $k_0 P$ 和椭圆曲线中的运算相比,大整数模运算所需计算量可以忽略不计.

实际应用中,委托过程很少会与代理签名的产生过程及验证过程连续发生.因此,只就代理签名的产生和验证而言,可以暂时不考虑委托过程需要的计算量.这样实际应用中,新方案和正常的椭圆曲线数字签名算法比较,只在验证过程多了一个椭圆曲线多倍点运算 $r_0 Q_0$.对委托过程,也只需一次椭圆曲线多倍点运算 $r_0 P$.

3.3　方案的安全性

文[1,4]中提出了一个代理签名方案所应满足的诸多条件,例如方案的基本不可伪造性、代理签名的不可伪造性、代理签名的可区分性、代理签名的不可抵赖性、身份的可证实性、密钥的依赖性等.国内外学者都以此来衡量一个代理签名方案的安全性.仍用 A 表示原始签名人,用 B 表示代理签名人,用 C 表示代理签名的验证人,本文将这些条件归结为以下三个基本条件:

(1)代理签名人 B 不能从委托信息中获取原始签名人的私钥;

(2)代理签名人 B 也不能利用原始签名人 A 给的委托信息产生新的委托信息,从而冒充 A 发出另一委托信息给另一人 D;

(3)代理签名的伪造者 E 不能冒充 B 而产生消息 m 的代理签名,从而欺骗验证人 C.

下面分别说明本文所给出的方案满足这些条件.

(1)原始签名人 A 给予代理签名人 B 的委托信息是 (σ, Q_0),其中 $Q_0 = k_0 P$,$\sigma \equiv (k_A + r_0 k_0) \bmod n$.由 Q_0,代理签名人 B 首先能够得到 r_0.于是,假如代理签名人 B 还能从 $Q_0 = k_0 P$ 中计算出 k_0,则代理签名人 B 进一步就能够从 $\sigma \equiv (k_A + r_0 k_0) \bmod n$ 中得到原始签名人 A 的私钥 k_A.然而,从 $Q_0 = k_0 P$ 中计算 k_0 是一个典型的椭圆曲线离散对数问题.已经假定椭圆曲线离散对数问题是困难的,代理签名人 B 从 $Q_0 = k_0 P$ 中计算出 k_0 是不可能的.所以,代理签名人 B 不可能通过这种方式获得原始签名人 A 的私钥 k_A.另外,因为 k_A, $r_0 k_0$ 都是随机数,所以 σ 也是随机的.由 Shannon 的信息理论可知,在未知关于 $r_0 k_0$ 的任何信息的情况下,从等式 $\sigma \equiv (k_A + r_0 k_0) \bmod n$ 中也不能得到任何关于 k_A 的信息.所以,代理签名人 B 不能从委托信息 (σ, Q_0) 中获取原始签名人 A 的私钥 k_A.

(2)在原始签名人 A 给代理签名人 B 的信息中,假如我们计算 σ 的等式不是 $\sigma \equiv (k_A + r_0 k_0) \bmod n$,而将其变为 $\sigma \equiv (k_A + k_0) \bmod n$,相应地验证等式(2)变为

$$\sigma P = P_A + Q_0 \tag{3}$$

则 B 能够随意产生新的委托信息 (σ', Q_0'),冒充原始签名人 A 来欺骗另一被委托人 D.这里,B 产生新委托信息 (σ', Q_0') 的方法可以是:B 随意选取一个整数 k_1 后,再计算 $\sigma' = (\sigma + k_1) \bmod n$, $Q_0' = Q_0 + k_1 P$.当 D 收到信息 (σ', Q_0') 后,容易看出 D 能够验证 (σ', Q_0') 是满足等式(3)的.从而,D 认为 (σ', Q_0') 来自原始签名人 A 而非其他人.代理签名人 B 冒充原始签名人 A 成功地欺骗了另一被委托人 D.

但是在本文所提出的方案中,计算 σ 的公式是 $\sigma \equiv (k_A + r_0 k_0) \bmod n$,而不是 $\sigma \equiv (k_A + k_0) \bmod n$.下面说明,类似的欺骗行为是不会发生的.为叙述方便,下面先约定一个符号.

设 $Q = (x', y) \in E$ 为 E 中任一点,$r \equiv x \bmod n$.本文约定用 f 表示由 Q 计算 r 的函数,亦即,记 $r = f(Q)$.这里 f 事实上是一个泛函数,其定义域为集合 E,值域是小于 n 的一些非负整数.这样约定后,式(1)可写为

$$\sigma \equiv (k_A + f(Q_0) k_0) \bmod n \tag{4}$$

式(2)可写为

$$\sigma P = P_A + f(Q_0) Q_0 \tag{5}$$

代理签名人 B 为了利用原始签名人 A 所给委托信息 (σ, Q_0) 产生新的假委托信息,按照前述方法,他随意选取一个整数 k_1 后,再计算 $Q_1 = k_1 P$ 以及

$$Q' = Q_0 + Q_1 \tag{6}$$

$$\sigma' = (\sigma + f(Q_1) k_1) \bmod n \tag{7}$$

但是,容易看出这样得到的 σ 和 Q 是不符合等式(5)的.因为这时等式(5)的左边

$$\sigma' P = (\sigma + f(Q_1) k_1) P = P_A + f(Q_0) Q_0 + f(Q_1) Q_1$$

等式(5)的右边

$$P_A + f(Q') Q' = P_A + f(Q_0 + Q_1)(Q_0 + Q_1)$$

由于

$$P(Q_0 + Q_1)(Q_0 + Q_1) \neq f(Q_0) Q_0 + f(Q_1) Q_1$$

所以对委托信息 σ 和 Q',它们不满足等式(5).B 对 D 的欺骗行为不能得逞.

在式(4)中,原始签名人 A 利用随机数 k_0 将他的私钥 k_A 隐藏到 σ 中传送给 B,同时他利用 $Q_0 = k_0 P$ 将 k_0 也传给 B.假如 B 在不知道 k_A 的情况下要给另外的第三者一个包含有 k_A 信息的量 σ',那么他必须利用手中的 σ.式(7)只能看作是他利用 σ 产生 σ 的一种选择.对其它类似选择同样会导致类似(8)的一个式子出现.因此,对本文所提出的代理签名方案,代理签名人 B 不能产生新委托信息的基础是:B 不能找到一个 $Q_1 \in E$ 使等式

$$f(Q_0 + Q_1)((Q_0 + Q_1)) = f(Q_0) Q_0 + f(Q_1) Q_1$$

成立.

(3)下面说明,对任何消息 m,任何一个不知道 σ 的人 D,都不能伪造出满足 3.1 中给出的验证程序的一组代理签名 (m, r, s, Q).

容易看出,一组数据 (m, r, s, Q) 满足 3.1 中给出的验证程序等价于这组数满足以下的签名方程

$$ms^{-1} P + rs^{-1}(P_A + f(Q) Q) = kP \tag{8}$$

方程(8)中,P 是曲线的基点,为系统参数.P_A 是原始签名人的公钥,对伪造者而言,它是一个不变量.m 是被签消息.r 和

k 之间有关系 $r = f(kP)$. 因此,伪造给定消息 m 的代理签名 (m, r, s, Q) 的本质是要找到三个整数 r, s, k 以及找到 E 中一点 Q 使它们满足方程(8).

从 r 和 k 之间的关系式 $r = f(kP)$ 看出,由 k 计算 r 是容易的,但是反过来由 r 计算 k 的困难性至少相当于椭圆曲线离散对数问题的难解性. 因此在代理签名 (m, r, s, Q) 的伪造过程中,只能先选定 k,并由此先确定 r,然后才能确定 s 和 Q. 这样,可以假定在方程(8)中已知 P, P_A, m, k, r 和函数 f,剩下要找一个适当的整数 s 和 E 中一点 Q 使方程(8)左右相等.

记 $P_1 = r^{-1}kP$, $P_2 = mr^{-1}P + P_A$,则方程(8)可以改写为

$$f(Q)\,Q = sP_1 - P_2 \tag{9}$$

这样,伪造代理签名 (m, r, s, Q) 的问题转化为:已知 P_1 和 P_2,求一整数 s 和 E 中一点 Q 使方程(9)成立.

方程(9)可以看作是关于 s 和 Q 的一个不定方程. 方程(9)中,假如先指定 Q 值,那么求 s 值的问题就转化成了一个典型的椭圆曲线离散对数问题,s 的值难以求出. 假如先指定 s 值,记 $Q_1 = sP_1 - P_2$,那么问题转化为:已知 $Q_1 \in E$,求 $Q \in E$ 使

$$f(Q)\,Q = Q_1 \tag{10}$$

于是,在假定椭圆曲线离散对数问题是难解的前提下,任何人对任意消息能够伪造代理签名 (m, r, s, Q) 的问题,转化成了对问题(10)的求解.

4 两个问题

设 $Q \in E$ 为 E 中任一点,并记 $Q = (x, y)$, $r \equiv x \bmod n$. 仍用 f 表示从 Q 到 r 的函数关系,即 $f(Q) = r \equiv x \bmod n$. 则从 3.3 节的讨论可以看出,3.1 节所提出的基于椭圆曲线代理签名方案的安全性,除基于椭圆曲线离散对数问题的困难性假定外,还基于下面两种新问题的难解性.

(1) 已知 E 中一点 $Q_0 \in E$,求另外一点 $Q_1 \in E$, $Q_1 \neq O$,使

$$f(Q_0 + Q_1)(Q_0 + Q_1) = f(Q_0)\,Q_0 + f(Q_1)\,Q_1 \tag{11}$$

(2) 已知 E 中一点 $Q_1 \in E$,求另外一点 $Q \in E$,使

$$f(Q)\,Q = Q_1 \tag{12}$$

为了对式(11)、(12)的难解性做出初步分析,以下假定椭圆曲线 E 是由基点 P 生成的循环子群,即假定 $E = \langle P \rangle$. 这样,对 E 中任一非零点 Q,总有 $Q = kP$,其中 k 为小于 n 的某一正整数. 于是,函数 $r = f(Q)$ 又可写为 $r = f(kP)$. 因为 P 是一固定点,所以在 $r = f(kP)$ 中,r 实际上是 k 的函数. 以下记这一函数为 f_1,即记 $r = f_1(k)$. 对函数 f_1,易见其定义域和值域都是由非负整数组成的集合 $\{0, 1, 2, \cdots, n-1\}$. 从 $r = f(kP)$ 可以看出,由 k 计算 r 是容易的. 但是,由 r 计算 k 就成了一个典型的椭圆曲线离散对数问题. 让 k 遍历集合 $\{0, 1, 2, \cdots, n-1\}$ 中的所有元素时,可以得到相应的 r 值. 但是,从椭圆曲线的基本特性可以看出,r 与 k 之间的关系非常复杂,它们之间基本上无规律可循. 另外应注意到,在 $r = f(Q)$ 中,r 是由 $Q = (x, y)$ 中的坐标 x 确定的. 对同一个 x,通常会有两个不同的点 $Q = (x, y)$ 和 $Q = (x, -y)$ 属于 E. 因此对函数 $r = f_1(k)$,平均说来,两个不同的 k 值会对应同一个 r.

在式(11)中,记 $Q_0 = k_0 P$,记 $Q_1 = k_1 P$,则使用函数符号 f_1,式(11)可写为:

$$[f_1(k_0 + k_1)(k_0 + k_1)]\,P = [f_1(k_0)\,k_0 + f_1(k_1)\,k_1]\,P$$

这一式子等价于

$$f_1(k_0 + k_1)(k_0 + k_1) \equiv f_1(k_0)\,k_0 + f_1(k_1)\,k_1 \bmod n \tag{13}$$

因此问题(11)转化了,对给定的 k_0,求 k_1,使式(13)成立.

记 $u = f_1(k_0 + k_1)(k_0 + k_1)$, $v = f_1(k_0)\,k_0 + f_1(k_1)\,k_1$. 则 $0 < u, v < n^2$. 现在,假如我们认为在函数 $r = f_1(k)$ 中,r 的取值完全随机于 k,则可以认为对固定(或不固定)的 k_0,无论 k_1 取什么值,u 和 v 都是两个近似独立的量. 这样,求解问题(13)相当于随机取两个满足 $0 < u, v < n^2$ 的正整数 u 和 v 使 $u \equiv v \bmod n$. 显然,找到这样的 u 和 v 是困难的. 因此,问题(11)应该是相当困难的.

在式(12)中,记 $Q_1 = k_1 P$,记 $Q = kP$,继续使用上面的符号,则式(12)可等价地写为

$$f_1(k)\,k \equiv k_1 \bmod n \tag{14}$$

记 $w = f_1(k)\,k$,则 $n < w < n^2$. 这样,同样地在函数 $r = f_1(k)$ 中,假如我们假定 r 的取值完全随机于 k,则对固定的 k_1,问题(14)相当于随机取一个满足 $0 < w < n^2$ 的正整数,使 $w \equiv k_1 \bmod n$. 显然,找到这样的 w 也是非常困难的.

以上我们对问题(11)和问题(12)所做分析只是一个初步的分析. 这一分析表明,求解它们是非常困难的,它们有可能是比椭圆曲线离散对数问题更困难的一类问题. 对这两个问题,都需要做进一步的公开研究.

5 结论

椭圆曲线密码是一种重要的公钥密码,椭圆曲线数字签名算法在实际中有很多重要应用. 代理签名是密码学中的一个较新思想. 这种思想的基本内容是,在不暴露签名人(称为原始签名人)私钥的情况下,原始签名人将自己的私钥信息通过某种方式传递给一个被称为代理签名人的人以后,代理签名人利用所得到信息能够替原始签名人产生对任何消息的签名,而任何一个知道原始签名人公钥的验证人都能对该签名做出验证. 本文将这种思想应用于椭圆曲线数字签名算法,提出了一种基于椭圆曲线的代理签名方案,同时对该方案的计算复杂性和安全性进行了分析. 分析表明,这种代理签名方案和椭圆曲线数字签名算法比较,在增加较少计算的情况下就能实现代理签名的思想. 通过对该方案安全性的研究,还得到了两种椭圆曲线上的困难问题. 新方案的安全性除需要假定椭圆曲线离散对数问题是困难的外,还需要假定这两种问题也是困难的. 新方案的安全性仍有待做进一步的公开讨论.

参考文献:

[1] Mambo M, Usuda K, Okamoto E. Proxy signatures: Delegation of the power to sign messages[J]. IEICE Trans. Fundamentals, 1996, E79-A(9): 1338 - 1354.

[2] 章昭辉,陈少军. 一种基于椭圆曲线的授权签名方案[J]. 安庆师范学院学报,2002,8(1):5-6.
[3] 王泽成,苏晓萍,汪精明. 一个基于椭圆曲线的代理签名和代理盲签名[J]. 青海大学学报,2002,20(3):37-39.
[4] 祁明,L Harn. 基于离散对数的若干新型代理签名方案[J]. 电子学报,2000,28(11):114-115.
[5] 伊丽江. 代理签名体制及其应用研究[D]. 西安:西安电子科技大学研究生院,2000.
[6] 伊丽江,白国强,肖国镇. 代理多重签名——一类新的代理签名方案[J]. 电子学报,2001,29(4):569-570.
[7] Blake I, Seroussi G, Smart N. Elliptic Curves in Cryptography[M]. Cambridge, United Kingdom: Cambridge University Press, 1999.

作者简介:

白国强　男,1963 年 11 月生于陕西清涧,2000 年 12 月获西安电子科技大学密码学专业博士学位,现为清华大学微电子学研究所博士后,目前主要研究方向为椭圆曲线密码及其实现技术. Email: baigq@mail.tsinghua.edu.cn.

黄　谆　男,1978 年 5 月生于江苏南京,1995 年进入清华大学,现为清华大学博士研究生,主要研究方向为密码算法的 VLSI 实现.