椭圆双曲线密码系统

张鑫彦 闫德勤
(辽宁师范大学计算机与信息技术学院 大连 116029)

摘 要 近年来,椭圆曲线理论在密码学中的作用越来越大。在许多的应用中椭圆曲线密码系统已经取代了传统的RSA公钥系统,因此一些针对椭圆曲线密码系统的攻击也越来越多。为了提高椭圆曲线密码的安全性而且保持其原有的优点,提出了椭圆双曲线密码系统。此系统有极好的随机性,在理论上提高了原椭圆曲线密码的安全性,而且还可以提供灵活的操作方法,这样就可以使目前已有的攻击技术无法追踪其破解线索,从而更好地提高信息的安全性。

关键词 椭圆双曲线,EHDSA,ECDSA

Elliptic Hyperbola Cryptography System

ZHANG Xin-yan YAN De-qin
(School of Computer and Information Technology, Liaoning Normal University, Dalian 116029, China)

Abstract In recent years, the elliptic curve cryptography system (ECCS) plays more and more important role in the cryptography. Instead of traditional public key cryptography system that it is RSA, it is the ECCS in a lot of application areas. Therefore, there are more and more attacks on the ECCS. In this paper, we advanced the technology that improves the ECCS's safeness and keeps its good property. The technology is called "Elliptic Hyperbola Cryptography System (EHCS)". The EHCS has the same calculation complexity as ECCS, but it has excellently randomness. So EHCS can improve cryptographic safeness in theory. The EHCS has more flexible operation mode than ECCS. Therefore, the EHCS can improve information technology's safeness.

Keywords Elliptic hyperbola, EHDSA, ECDSA

自从20世纪80年代在密码学中用到了椭圆曲线以来,在同样的安全性下椭圆曲线以其密钥短、硬件实现代价小、速度快等优点正在被需多学者所关注。现在已经有很多的学者开始破译以椭圆曲线理论为基础的加密算法而且有了很大的成绩,见文献[15,16]。这说明椭圆曲线加密理论正面临着威胁,如果不即时进行改进,很有可能在不久的将来会给信息安全带来很大的隐患。所以,本文在椭圆曲线理论的基础上,对椭圆曲线理论进行了改进,使原来的单曲线理论变成了椭圆双曲线理论,这样不但保证了椭圆曲线原有的良好属性比如计算简单、运算速度快等等,而且产生结果的随机性更大了,从而提高了以椭圆曲线理论为基础的密码算法的安全性。

1 椭圆曲线基本理论[1,2]

定义1 设K是域,K上的椭圆曲线E的方程为:

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$$

式中,系数$a_1,a_2,a_3,a_4,a_6\in K$满足:对任意坐标在代数闭包$\overline{K}$中的满足方程E的点(x_1,y_1),偏导数$2y_1+a_1x_1+a_3$和$3x_1^2+2a_2x_1+a_4-a_1y_1$不同时为0。

设$P=(x_1,y_1)$,$Q(x_2,y_2)$是椭圆曲线E上的两个不同点,则$R=P+Q$,其中$R=(x_3,y_3)$定义如下:首先,通过P和Q画一条直线,那么这条线会和椭圆曲线交于第三点,R为这第三点的对称点,如图1所示。

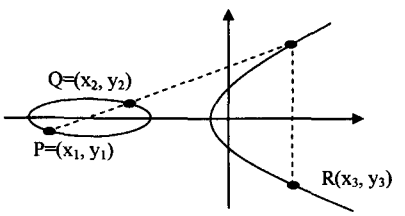

图1

设$P=(x_1,y_1)$是椭圆曲线E上的一个不同点,则$R=P+P$,其中$R=(x_3,y_3)$定义如下:首先,通过P画一条切线,那么这条线会和椭圆双曲线交于另外一点,R为这点的对称点,如图2所示。

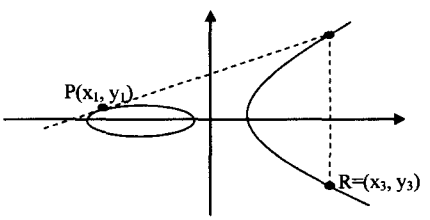

图2

到稿日期:2009-09-14 返修日期:2010-01-20 本文受国家自然科学基金(60372071),中国科学院自动化研究所复杂系统与智能科学重点实验室开放课题基金(20070101),辽宁省教育厅高等学校科学研究基金(2008344),大连市科技局科技计划项目(2007A10GX117)资助。

张鑫彦(1982—),男,硕士生,主要研究方向为密码学,E-mail:zxy30555@163.com;闫德勤(1962—),男,博士,教授,主要研究方向为密码学。

以上用图的形式描述了椭圆双曲线的加法运算，下面则给出椭圆曲线运算的一般代数表达式。

设 $P(x_1,y_1)$ 和 $Q(x_2,y_2)$ 则可得：

$$R=P+Q=(\lambda^2+a_1\lambda-a_2-x_1-x_2,\lambda(x_1-x_3)-y_1-a_1x_3-a_3)$$

其中

$$\lambda=\begin{cases}\dfrac{y_1-y_2}{x_1-x_2}, & \text{当 } P\neq Q\\ \dfrac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}, & \text{当 } P=Q\end{cases}$$

2 椭圆双曲线理论方法的研究

2.1 椭圆双曲线概念的提出

根据定义 1 可以推出以下定义。

定义 2 设 K^{-1} 是域，K^{-1} 上的反椭圆曲线 E^{-1} 的方程为：

$$y^2-a_1xy+a_3y=-x^3+a_2x^2-a_4x+a_6$$

式中，系数 $a_1,a_2,a_3,a_4,a_6\in K^{-1}$ 满足：对任意坐标在代数闭包 $\overline{K^{-1}}$ 中的满足方程 E^{-1} 的点 (x_1,y_1)，偏导数 $2y_1-a_1x_1+a_3$ 和 $-3x_1^2+2a_2x_1-a_4+a_1y_1$ 不同时为 0。

将定义 1 与定义 2 进行结合，就可以得出椭圆双曲线的概念。

定义 3（椭圆双曲线） 设 $DK\in K\cup K^{-1}$ 是域，DK 上的椭圆双曲线 DE 的方程为：

$$\begin{cases}y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6, & x\text{ 轴正方向的曲线}\\ y^2-a_1xy+a_3y=-x^3+a_2x^2-a_4x+a_6, & x\text{ 轴负方向的曲线}\end{cases}$$

式中，系数 $a_1,a_2,a_3,a_4,a_6\in K$ 满足：对任意坐标在代数闭包 $\overline{DK}$ 中的满足方程 DE 的点 (x_1,y_1)，x 轴正方向的曲线偏导数 $2y_1+a_1x_1+a_3$ 和 $3x_1^2+2a_2x_1+a_4-a_1y_1$ 不同时为 0，以及 x 轴负方向的曲线偏导数 $2y_1-a_1x_1+a_3$ 和 $-3x_1^2+2a_2x_1-a_4+a_1y_1$ 也不同时为 0。以下用曲线 $+\infty$ 和曲线 $-\infty$ 表示 x 轴正方向的曲线和 x 轴负方向的曲线。

2.2 椭圆双曲线的运算法则确定

设 $P=(x_1,y_1)$，$Q(x_2,y_2)$ 是椭圆双曲线 DE 上的两个不同点，则 $R=P+Q$，$R'=\overline{P+Q}$（我们将 $\overline{P+Q}$ 称点 P 和点 Q 的反加运算），其中 $R=(x_3,y_3)$，$R'=(x_4,y_4)$ 定义如下：首先，通过 P 和 Q 画一条直线，那么这条线会和椭圆双曲线交于两点，R 和 R' 为这两点的对称点，其中在 x 轴正半轴方向的点为 R，x 轴负半轴方向的点为 R'，如图 3 所示。

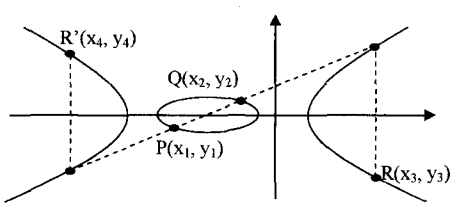

图 3

设 $P=(x_1,y_1)$ 是椭圆双曲线 DE 上的一个不同点，则 $R=P+P$，$R'=\overline{P+P}$，其中 $R=(x_3,y_3)$，$R'=(x_4,y_4)$ 定义如下：首先，通过 P 画一条切线，那么这条线会和椭圆双曲线交于两点，R 和 R' 为这两点的对称点，其中在 x 轴正半轴方向的点为 R，x 轴负半轴方向的点为 R'，如图 4 所示。

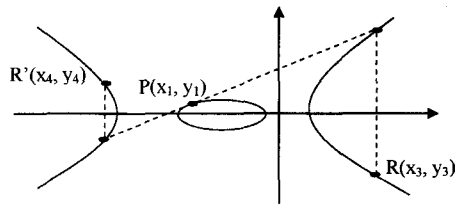

图 4

以上用图的形式描述了椭圆双曲线加法和反加法运算，下面则给出椭圆双曲线的运算的一般代数表达式以及表达式解的过程。

设 $P=(x_1,y_1)$，$Q(x_2,y_2)$ 是椭圆双曲线 DE 上的两个不同点，且 $x_1\neq x_2$，则计算 $R=P+Q$ 和 $R'=\overline{P+Q}$ 的坐标 (x_3,y_3) 和 (x_4,y_4)。先求 P 和 Q 的直线 PQ 的斜率为：

$$\lambda=\frac{y_1-y_2}{x_1-x_2}$$

因此可得直线 PQ 的方程为：

$$y=\lambda x+\frac{x_1y_2-x_2y_1}{x_1-x_2}$$

设 $\mu=\dfrac{x_1y_2-x_2y_1}{x_1-x_2}$，由此直线 PQ 的方程可以转化为 $y=\lambda x+\mu$。将此方程代入椭圆双曲线的方程 DE 中可得：

$$\begin{cases}(\lambda x+\mu)^2+a_1x(\lambda x+\mu)+a_3(\lambda x+\mu)=x^3+a_2x^2+a_4x+a_6, & \text{曲线}+\infty\\ (\lambda x+\mu)^2-a_1x(\lambda x+\mu)+a_3(\lambda x+\mu)=-x^3+a_2x^2-a_4x+a_6, & \text{曲线}-\infty\end{cases}$$

$$\Rightarrow$$

$$\begin{cases}(\lambda x+\mu)^2+(a_1x+a_3)(\lambda x+\mu)=x^3+a_2x^2+a_4x+a_6, & \text{曲线}+\infty\\ (\lambda x+\mu)^2-(a_1x-a_3)(\lambda x+\mu)=-x^3+a_2x^2-a_4x+a_6, & \text{曲线}-\infty\end{cases}\tag{1}$$

令方程(1)等于零即：

$$\begin{cases}x^3+(a_2-\lambda^2-a_1\lambda)x^2+(a_4-2\lambda\mu-a_3\lambda-a_1\mu)x+a_6-\mu^2-a_3\mu=0, & \text{曲线}+\infty\\ x^3-(a_2-\lambda^2+a_1\lambda)x^2+(a_4+2\lambda\mu+a_3\lambda-a_1\mu)x-a_6+\mu^2+a_3\mu=0, & \text{曲线}-\infty\end{cases}$$

又因为 P,Q,R,R' 是方程(1)的 4 个根所以有：

$$\begin{cases}x^3+(a_2-\lambda^2-a_1\lambda)x^2+(a_4-2\lambda\mu-a_3\lambda-a_1\mu)x+a_6-\mu^2-a_3\mu=(x-x_1)(x-x_2)(x-x_3), & \text{曲线}+\infty\\ x^3+(\lambda^2-a_2-a_1\lambda)x^2+(a_4+2\lambda\mu+a_3\lambda-a_1\mu)x-a_6+\mu^2+a_3\mu=(x-x_1)(x-x_2)(x-x_4), & \text{曲线}-\infty\end{cases}$$

从而得到：

$$\begin{cases}\lambda^2+a_1\lambda-a_2=x_1+x_2+x_3, & \text{曲线}+\infty\\ a_2-\lambda^2+a_1\lambda=x_1+x_2+x_4, & \text{曲线}-\infty\end{cases}$$

$$\Rightarrow$$

$$\begin{cases}x_3=\lambda^2+a_1\lambda-a_2-x_1-x_2, & \text{曲线}+\infty\\ x_4=a_2-\lambda^2+a_1\lambda-x_1-x_2, & \text{曲线}-\infty\end{cases}$$

因为 x_1,x_2 都是 DK 中的元素，所以 x_3,x_4 也是 DK 中的元素，而且直线 PQ 与椭圆双曲线的交点 y 坐标为：

$$\begin{cases}y'_3=\lambda x_3+\mu, & \text{曲线}+\infty\\ y'_4=\lambda x_4+\mu, & \text{曲线}-\infty\end{cases}$$

为了求出 R 与 R'，需要在曲线上找到另外两个交点和这个两个交点关于 x 轴对称，所以可以得到：

$$\begin{cases} y_3 = -\lambda x_3 - \mu - a_1 x_3 - a_3, & \text{曲线}+\infty \\ y_4 = -\lambda x_4 - \mu + a_1 x_4 - a_3, & \text{曲线}-\infty \end{cases}$$

最终可以得到椭圆双曲线上的运算表达式(如果 $P(x_1, y_1)$和 $Q(x_2, y_2)$是已知的):

$-P=(x_1, -y_1 - a_1 x_1 - a_3)$

引用曲线正半轴方程系数

$\overline{-P}=(x_1, -y_1 + a_1 x_1 - a_3)$

引用曲线正半轴方程系数

$R=P+Q=(\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1 - a_1 x_3 - a_3)$

引用曲线正半轴方程系数

$R'=\overline{P+Q}=(a_2 - \lambda^2 + a_1\lambda - x_1 - x_2, \lambda(x_1 - x_4) - y_1 + a_1 x_4 - a_3)$

引用曲线负半轴方程系数

其中

$$\lambda=\begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2}, & \text{当 } P \neq Q \\ \dfrac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}, & \text{当 } P = Q \end{cases}$$

引用曲线正半轴系数。

下面来看一个例子:

例　对于有限域 F_p,其中 $p=2003$,下列方程定义了一条椭圆双曲线 DE:

$$\begin{cases} y^2 + 2xy + 8y = x^3 + 5x^2 + 1136x + 531, & \text{曲线}+\infty \\ y^2 - 2xy + 8y = -x^3 + 5x^2 - 1136x + 531, & \text{曲线}-\infty \end{cases}$$

已知 $P=(1118,269)$,$Q=(892,529)$是 DE 上的两个点,求 $-P, P+Q, P+P, \overline{-P}, \overline{P+Q}, \overline{P+P}$。

解:已知可以将方程转化为如下形式:

$$\begin{cases} y^2 + 2xy + 8y = x^3 + 5x^2 + 1136x + 531, & \text{曲线}+\infty \\ y^2 + 2001xy + 8y = -x^3 + 5x^2 + 867x + 531, & \text{曲线}-\infty \end{cases}$$

由上述方程可得:

$-P=(1118,1493)$

$P+Q=(1681,1706)$

$P+P=(1465,677)$

$\overline{-P}=(1118,1959)$

$\overline{P+Q}=(308,1738)$

$\overline{P+P}=(75,921)$

3　基于椭圆双曲线理论方法的密码学算法

3.1　椭圆双曲线的离散对数问题

一般的离散对数问题是给定有限域 F 和 $y, g, p \in F$,求 $x \in F$ 使得 $y \equiv g^x \bmod p$ 成立。椭圆双曲离散对数问题是指对于椭圆双曲线 E 上 3 点 P, Q, Q',寻找两个整数 d, d',使得 $Q=dP$ 和 $Q'=\overline{d'P}$ 同时成立。也可以从密码学角度来描述椭圆双曲线离散对数问题,设 $P \in DEp(a,b)$,且 P 的除数为素数 n,则 $DEp(a,b)$中由点 P 生成的子集 $\langle p\rangle = \{0, P, 2P, \cdots, (n-1)P\} \cup \{\overline{P}, \overline{2P}, \cdots, \overline{(n-1)P}\}$,在 $[1, n-1]$中随机选取两个整数 d, d',计算 $Q=dP, Q'=d'P$,则 $(d,Q), (d',Q')$就可以作为集体密钥对或可以任选其一作为一对密钥对,这是椭圆双曲线的一个特点即具有灵活的操作性,在使用中可以在得到的结果中进行一个简单的运算就可以让破解者找不到破解线索,从而提高了安全性。因此椭圆双曲线的离散对数基本可以描述为由 $DEp(a,b), P, n, Q$ 和 Q' 来确定 d, d' 的问题。

3.2　椭圆双曲线 Diffie－Hellman 密码体制

像椭圆曲线一样,椭圆双曲线也可以实现双钥密码体制即在此密码体制中每个用户都有一对选定的密钥,一个公开另一个保密,其他用户可以用某一用户的公开密钥来加密信息发给他,而只有该用户自己可以利用他自己的私钥对密文进行解密。

(1)密钥产生。定义椭圆双曲线 $DEp(a,b)$,在 $DEp(a,b)$中选取基点为 $G(x,y)$,$G(x,y)$的阶数为 n(n 是一个大素数),在$[1, n-1]$之间选取两个整数 d, d',则计算 $Q=dG$ 和 $Q'=\overline{d'G}$,得到密钥对(d,Q)、(d',Q'),其中 Q, Q' 为公钥,d, d'为私钥。之后对(d,Q)、(d',Q')进行检查:1)检查要保证 $Q \neq 0, Q' \neq 0$;2)检查 Q, Q' 的坐标是否是有限域 $GF(p)$上的元素;3)检查 Q, Q' 是否为 $DEp(a,b)$上的点;4)检查是否有整数 m 使得 $mQ=0, mQ'=0$。经上述步骤后,椭圆曲线密码系统就得到有效的密钥对(d,Q),(d',Q')。

(2)数据加、解密过程。设用户 B 和用户 A 发送消息 m,过程如下:用户 A 通过上一步骤的说明获得有效的密钥对(d,Q),(d',Q'),用户 A 可从中选择任何一个密钥对,也可以对这两个密钥进行简单运算并得出更安全的密钥对,这样攻击者就无法追踪了。比如我们这里设用户 A 选择的密钥对为(dA, QA),则用户 A 将 dA 作为私钥保管好,并产生公开的密钥 QA(其中 $QA=dA*G$);第二步是用户 A 将 $DEp(a,b)$和点 QA, G 传给用户 B;第三步是用户 B 接到信息后,将它所要发送的明文 m 编码到 $DEp(a,b)$上的一点 M,并在$[1, n-1]$之间随机选取一整数 r,计算:$C1=M+rQA, C2=rG$;第四步用户 B 将$(C1, C2)$发给用户 A;第五步用户 A 用他的私钥 dA 解密,方法如下:$C1 - kC2 = M + rQA - k(rG) = M + rQA - rQA = M$,最后再对 M 解码就可以得到明文 m。

3.3　椭圆双曲线数字签名算法

大家对于椭圆曲线数字签名算法 ECDSA(Elliptic Curve Digital Signature Algorithm)[3,6,7]一定不陌生,此算法是 DSA 数字签名算法在椭圆曲线上的模拟,于 1992 年由 Scott Vanstone 提出。一个数字签名实际上是一个由签名者的私钥和被签名的消息决定的一串数字,该数字必须可以在不知道签名的私钥的情况下进行验证。一个签名算法应该是在选择明文攻击下具有存在性和不可伪造的性质,也就是说签名算法应该能够保证,一个攻击者或者敌手无论得到多少他所选定的消息的签名,仍然不能构造任何一个其他消息的有效签名。下面就把这种数字签名算法引入到椭圆双曲线中,即椭圆双曲线数字签名算法 EHDSA(Elliptic Hyperbola Digital Signature Algorithm)。

假设一个签名者需要签名一个消息 m,他首先需要选取一个有限域 F_q,一组定义在 F_q 上的椭圆双曲线 DE,以及 DE 上的一个阶为 n 的有理点 G,这些都是需要公开的参数。另外,签名者还需要在区间$[0, n-1]$中随机选取两个整数 d, d',则计算 $Q=dG, Q'=d'G$ 中的任何一个作为公钥对外公布,也可以对其进行 3.2 节中(2)的运算。这里还设 dA 和 $QA=dAG$ 为密钥对,签名者要签名消息 m 时,可以按如下步骤进行:

1)选择随机或伪随机整数 k 属于$[1, n-1]$;

2)计算 $kG=(x_1, y_1)$和 $r=x_1 \bmod n$ 并且 $r=0$,否则转

到步骤1)；

3)计算 $k^{-1} \bmod n$；

4)计算 $e=MD5(m)$；

5)计算 $s=k^{-1}(e+dAr) \bmod n$，且 $s\neq 0$，否则重新选择 k 进行计算；

6)输出消息 m 的签名(r,s)。

为了验证上述消息 m 的签名(r,s)，验证者必须预先获得一份签名者公布的参数，一旦得到了这些参数，对签名的验证过程如下：

1)确认 r,s 是区间$[1,n-1]$中的整数；

2)计算 $e=MD5(m)$；

3)计算 $w=s^{-1} \bmod n$；

4)计算 $u_1=ew \bmod n$ 和 $u_2=rw \bmod n$；

5)计算 $X=u_1G+u_2QA$，如果 X 为零点则拒绝签名，否则计算 $v=x_1 \bmod n$，其中 $X=(x_1,y_1)$；

6)如果 $v=r$ 则验证成功。

以上的数字签名算法只是举了一个例子，读者还可以根据情况来改变算法，使其更安全。

结束语 本文基于对椭圆曲线理论方法的研究，提出了一种新的椭圆双曲线密码的加/解密方法，该方法的一个重要优点在于它在计算的过程中不增加计算的难度便可提高密码的安全性。我们可以从坐标图上看出椭圆双曲线密码比原椭圆曲线密码多了一条曲线，点的选择范围要大很多，而且在代数表达式中可以看到椭圆双曲线密码的随机性要大得多等等，这些都是密码体制的良好特性，从而为信息增加了更大的安全系数。另外，椭圆双曲线计算出的数据比原椭圆曲线计算出的数据多，这样就给我们提供了灵活的操作方法，从而使攻击方法找不到追踪的线索。鉴于椭圆曲线密码对信息安全的重要作用，本文所提出的椭圆双曲线密码方法对该领域的研究具有推动作用。

参 考 文 献

[1] Cohen H, Frey G. Handbook of Elliptic and Hyperelliptic Curve Cryptography[Z]. Discrete Mathematics and its application. Chapman & Hall/CRC, 2006

[2] Sliverman J H. The Arithmetic of Elliptic Curves[M]. Springer Verlag, 1996

[3] Miller V. Uses of elliptic curve in cryptography[C]//CRYPTO'85, Lecture Notes in Computer Science, LNCS218. Springer-Verlag, 1986: 417-426

[4] Birch B J, Kuyk W. Modular Functions of One Variable IV[C]// Lecture Notes in Mathematics 476. New York-Berlin-Heidelberg: Springer-Verlag, 1975

[5] Ross R. K_2 of elliptic curves with sufficient torsion over Q[J]. Comp Math, 1992, 81: 211-221

[6] Koblitz N, Menezes, Vanstone S. The state of elliptic curve cryptography[J]. Designs, Codes and Cryptography, 2000, 19: 173-193

[7] IEEE P1363a. included ECDSA, ECNR, ECNR2, ECPV, ECDH and ECMQV. Draft Version D9[Z]. 2001

[8] Silverman J H. Advanced Topics in the Arithmetic of Elliptic Curves[M]. New York-Berlin-Heidelberg-Tokyo: Springer-Verlag, 1994

[9] Cremona J. Algorithms for Modular Elliptic Curves[M]. Cambridge: Cambridge University Press, 1997

[10] Knapp A W. Elliptic Curves[M]. Princeton: Princeton University Press, 1992

[11] Lang S. Elliptic Functions, GTM(112)[M]. New York-Berlin-Heidelberg: Springer-Verlag, 1987

[12] Ramakrishnan D. Regulators, Algebraic Cycles, and Values of L-functions[M]. Contemporary Mathematics, 83, Providence, RI: Amer Math Soc, 1989: 183-310

[13] Silverman J H. The arithmetic of elliptic curves[M]. New York-Berlin-Heidelberg-Tokyo: Springer-Verlag, 1986

[14] Silverman J H. Computing heights on elliptic curves [J]. Math Comp, 1988, 51: 339-358

[15] Akishita T, Takagi T. Zero-Value Register Attack on Elliptic Curve Cryptosystem[J]. IEICE, 2005, E88-A(1)

[16] Eicher J, Opoku Y. Using the Quantum Computer to Break Elliptic Curve Cryptosystems[Z]. CiteSeer, 1997

[17] 于飞. 对于有限域上椭圆曲线的一些算术问题的研究[D]. 合肥：中国科学技术大学, 2008

[18] 王海艳. 最优扩域上的椭圆曲线加密系统研究[D]. 太原：太原理工大学, 2007

[19] Kapoor V, Kapoor V. Ramesh Singh, Elliptic Curve Cryptography[J]. ACM Ubiquity, 2008, 20(9): 20-26

[20] Uhsadel L, Poschmann A, Paar C. An Efficient General Purpose Elliptic Curve Cryptography Module for Ubiquitous Sensor Networks[J]. Software Performance Enhancement for Encryption and Decryption(SPEED 2007), 2007

[21] Barbosa M, Moss A, Page D. Compiler Assisted Elliptic Curve Cryptography[C]//OTM Conferences, 2007(2): 1785-1802

(上接第71页)

[22] Li J, Li N. OACerts: Oblivious attribute certificates[C]// Proc. of the 3rd Conference on Applied Cryptography and Network Security (ACNS). Lecture Notes in Computer Science, volume 3531. Springer, 2005: 301-317

[23] Li J, Li N. Policy-hiding access control in open environment[C]// Proc. of the 24nd ACM Symposium on Principles of Distributed Computing (PODC). New York: ACM Press, 2005: 29-38

[24] Stallings W. Cryptography and Network Security: Principles and Practice(second ed)[M]. Prentice Hall, 1999

[25] Yu T. Automated trust establishment in open systems [D]. Illinois: University of Illinois, 2003

[26] Rescorla E. SSL and TLS: Designing and Building Secure Systems[M]. Addison-Wesley, 2001

[27] Witteman M. Advances in Smartcard Security [J]. Information Security, Bullentin, 2002

[28] Ryutov T, Neuman C, Kim D, et al. Integrated Access Control and Intrusion Detection for Web Servers [J]. IEEE Transactions on Parallel and Distributed Systems, 2003, 14(9): 841-850

[29] Winslett M, Yu T, Seamons K E, et al. Negotiating trust on the web [J]. IEEE Internet Computing, 2002, 6(6): 30-37

[30] Bertino E, Ferrari E, Squicciarini A C. Trust-X: A peer to peer framework for trust negotiations[C]// Proc. of the IEEE Trans. on Knowledge and Data Engineering. Washington: IEEE Computer Society Press, 2004: 132-138