一种基于双勾函数的数据加密算法研究

李宏伟[1],潘志远[1],黄继杰[2]
(1. 国家电网有限公司技术学院分公司,山东 济南 250002;
2. 北京科东电力控制系统有限责任公司,北京 100192)

摘　要:在量子计算及保密通信的背景下,传统的对称和非对称加密技术及应用需要继续深化研究。该文针对双勾曲线函数的特性进行了对称、非对称和格加密技术的研究,并探讨了其应用的场合。首先通过对其渐近线做垂直线以及线上点的 X 轴平行线,将明文数值对应为交替所做的垂直线和平行线的次数,用最后一次交点的 X 或 Y 值作为对应的密文。然后基于双勾函数的两个特征参数以及基点的选取,设计了对称加密算法和相应的非对称加密算法(DHC);并选择任意条双勾曲线函数作为格基来构成非线性的格空间,由此探讨了基于双勾曲线函数的格加密可能性。最后通过在 PC 工作站上的仿真测试,表明基于双勾函数的数据加密算法比椭圆曲线加密算法(ECC)快了好几百倍;进而通过将 DHC 算法应用到电力云培训仿真中,确保了云培训考核的安全性,表明了基于双勾函数的数据加密算法能很好地适用于快速加密的场合。

关键词:双勾函数;对称加密;非对称加密;曲线加密;格加密
中图分类号:TP391.9　　**文献标识码**:A　　**文章编号**:1673-629X(2022)06-0120-06
doi:10.3969/j.issn.1673-629X.2022.06.020

Research on a Data Encryption Algorithm Based on Double Hook Function

LI Hong-wei[1], PAN Zhi-yuan[1], HUANG Ji-jie[2]
(1. State Grid of China Technology College, Jinan 250002, China;
2. Beijing Kedong Electric Control System Co., Ltd., Beijing 100192, China)

Abstract: In the context of quantum computing and secure communication, traditional symmetric and asymmetric encryption technologies and their applications need to be further studied. We focus on the characteristics of the double-hook curve function to study symmetric, asymmetric and lattice encryption technologies, and discuss their occasion of application. Firstly, by making the vertical line of its asymptote and the X-axis parallel line of the intersection, the plaintext value is corresponding to the number of alternating vertical and parallel lines, and the X or Y value of the last intersection is used as the corresponding ciphertext. Then based on the two characteristic parameters of the double-hook function and the selection of the base point, a symmetric encryption algorithm and the corresponding asymmetric encryption algorithm (DHC) are designed, and any double-hook curve function is chosen as the lattice base to form a non-linear lattice space, thus discussing the possibility of lattice encryption based on the double-hook curve function. Finally, the simulation test on the PC workstation shows that the data encryption algorithm based on the double-hook function is hundreds of times faster than the elliptic curve encryption algorithm (ECC). Furthermore, by applying the DHC algorithm to the power cloud training simulation, the security of the cloud training assessment is ensured, which shows that the data encryption algorithm based on the double-hook function can be well suited for fast encryption occasions.

Key words: double-hook function; symmetric encryption; asymmetric encryption; curve encryption; lattice encryption

0　引　言

根据香农定理,每传送一次密文就更换密钥是绝对安全的,量子保密通信可实现这一要求[1],但量子信号的减衰除受线路运行环境的影响,还受设备精度和组网模式的影响,使得经典的对称和非对称加密方法还在继续研究和应用。文献[2-4]在研究网络安全时采用了基于主体身份鉴别和认证、数据加密传输、传输链路节点身份鉴别和认证等技术;文献[5-7]在研究

收稿日期:2021-06-21　　**修回日期**:2021-10-22
基金项目:国家电网有限公司科技项目(5222JZ17002R)
作者简介:李宏伟(1979-),男,博士,高级工程师,从事智能电网、电力系统自动化及网络安全相关研究工作。

区块链时采用了非对称加密算法 RSA、对称加密 AES 算法和单向加密算法 SHA256;文献[8-9]在研究电力变电站远动通信时采用了非对称加密和对称加密混用的算法;文献[10-14]对非对称加密中的椭圆曲线加密算法进行了研究和应用。

但随着量子计算技术的发展及其超乎想象的计算能力,使得经典的对称和非对称加密方法中的密钥和密码将有可能被轻易破解,促进了后量子密码时代的到来。其中格密码学的研究成为一大热点[15-16],且成为了美国国家标准与技术研究院(national institute of standards and technology,NIST)后量子密码时代的优选技术。

该文从非线性的双勾函数特性出发,依次研究其在对称加密、非对称加密及格加密中的算法实现及在电力云培训仿真中的应用。

1　双勾函数的特性

双勾函数形如:

$$y = ax + \frac{b}{x}, ab > 0 \tag{1}$$

双勾函数的图像是分别以 y 轴和 $y = ax$ 为渐近线的两支曲线,且图像上任意一点到两条渐近线的距离之积恰为渐近线夹角(0° ~ 180°)的正弦值与 $|b|$ 的乘积。

双勾函数是奇函数;令 $k = \sqrt{\frac{b}{a}}$,那么:增区间:$\{x \mid x \leqslant -k\}$ 和 $\{x \mid x \geqslant k\}$;减区间:$\{x \mid -k \leqslant x < 0\}$ 和 $\{x \mid 0 < x \leqslant k\}$

变化趋势:在 y 轴左边先增后减,在 y 轴右边先减后增。双勾函数的两条渐近线分别为 y 轴和 $y = ax$。

双勾函数的图形是在笛卡尔坐标系中第一和第四象限的曲线,现在基于椭圆曲线加密算法(ECC 算法)被广泛应用于互联网领域,如区块链的加密中。ECC 算法的数学原理是椭圆曲线和离散对数,使得 ECC 算法要比 RSA 算法复杂很多,这种复杂的计算虽带来了性能提升的好处,但是也同时潜藏了一些问题。首先是一套 ECC 算法标准所对应的这条曲线,可能暗藏数学机关并可以通过后门来破解,比如目前使用面很广的一套标准是美国国家安全局发布的,这套标准就被怀疑是有后门。

另外一个问题就是基于 ECC 的专利太多,而且这些专利很多都被一个公司所持有,这个公司就是黑莓,这就使得开发一套新的 ECC 方案有可能被认为触犯了某个专利。故虽然 ECC 目前发展良好,但是也面临着各种挑战,这就为基于双勾函数曲线加密的应用提供了机会。

2　基于双勾函数的加密算法

2.1　基于双勾函数的对称加密

双勾函数分为两条对称曲线,需要加密的原文分布在 X 轴上,密文是加密操作后对应的 Y 值。将加密原文定义在 $(0, +\infty)$ 上,其中分布在 $(\sqrt{\frac{b}{a}}, +\infty)$ 的原文对应 X 轴上的曲线,如图 1 所示。

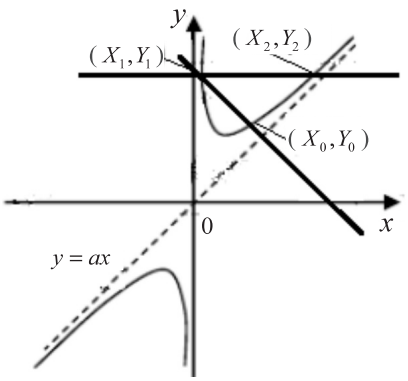

图 1　双勾函数做垂线和平行线

图 1 中垂直于渐近线的法线为:$y = -\frac{x}{a} + m$,其中 m 由法线与 x 轴的交点决定其取值。

以由双勾函数曲线上的点 (X_0, Y_0) 为一个开始的(原文,密文)对,从点 (X_0, Y_0) 做渐近线的法线,交双勾函数曲线上的点 (X_1, Y_1),再由点 (X_1, Y_1) 做平行线,交于勾函数曲线上的点 (X_2, Y_2),由下列方程:

$$\begin{cases} y = ax + \dfrac{b}{x} \\ y = -\dfrac{1}{a}x + m \end{cases} \tag{2}$$

求得 $m = Y_0 + \frac{X_0}{a}$,从而求得点 (X_1, Y_1) 值如下:

$$\begin{cases} X_1 = \dfrac{am}{2(a^2+1)} - \sqrt{\left(\dfrac{am}{2(a^2+1)}\right)^2 - \dfrac{ab}{a^2+1}} \\ Y_1 = aX_1 + \dfrac{b}{X_1} \end{cases} \tag{3}$$

再由点 (X_1, Y_1) 做平行线,交于双勾函数曲线上的点 (X_2, Y_2):

$$\begin{cases} X_2 = \dfrac{Y_1}{2a} + \sqrt{\dfrac{Y_1^2}{4a^2} - \dfrac{b}{a}} \\ Y_2 = aX_2 + \dfrac{b}{X_2} \end{cases} \tag{4}$$

再从点 (X_2, Y_2) 开始按上述方法做渐近线的法线,并与交点处做 X 轴的平行线,交于双勾曲线上,这个过程称为第二次操作。依此可进行第三次、第四次,直至第 N 次,此时 N 为偶数。可以看出第 N 次交于双勾曲线上的点由三个参数决定:重复次数 N,双勾函

数参量 a 和 b（这两个参量也可以换成渐近线与 X 轴的夹角 β，用弧度表示；和最低点（X_0，Y_0）的 X_0 值，即三元组（β，X_0，N）。

分布在 $(0,\sqrt{\frac{b}{a}})$ 的原文对应 X 轴下的曲线（见图 2）。

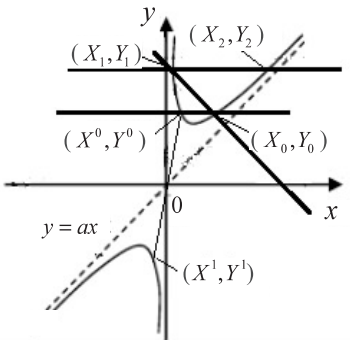

图 2 双勾函数的解密过程

以图中点（X^0，Y^0）为例，先做平行线交于点（X_0，Y_0），此为第一次操作，再按上面的步骤，从点（X_0，Y_0）作法线，交于点（X_1，Y_1），此为第二次操作，再由点（X_1，Y_1）做平行线，交于双勾函数曲线上的点（X_2，Y_2），这个过程称为第三次操作。依此可进行第四次、第五次，直至第 N 次，此时 N 为奇数。

2.2 基于双勾函数的非对称加密

上述由法线和平行线操作次数构成的集是一个阿贝尔群（P，+），因为：

封闭性：s 和 t 是整数操作次数，属于 P，那么 $s+t$ 也是整数操作次数，也属于 P。

结合性：$(s+t)+c=s+(t+c)$，为双勾曲线上同一点。

单位元：0 即为单位元（在基点 G 没操作），因为对于所有操作次数 s，$s+0=0+s=s$，为双勾曲线上同一点。

逆元：s 的逆元为 $-s$（由操作 s 次后的双勾曲线上的点，反向操作，即当 s 为奇数时，做渐近线的法线；s 为偶数时，作平行线，交于双勾函数曲线上的另一点），因为 $s+(-s)=0$，即单位元（回到基点 G）。

所以由法线和平行线操作次数构成的集 P 是阿贝尔群（P，+）。

双勾函数曲线上求解的问题描述为：已知（1）双勾函数曲线 E；（2）双勾函数曲线 E 上一点 G（基点）；（3）双勾函数曲线 E 上的一点 xG（x 为由 G 作法线和平行线的总次数）。据此求解 x，这个问题的难度保证了基于双勾函数曲线加码的安全性。

基于双勾函数数字签名法的加密算法（DHC）具体如下：

基于双勾函数的数据加密算法属于非对称密钥加密系统体系，又称公钥密钥加密体系。它需要使用不同的密钥来分别完成加密和解密操作，一个公开发布，即公开密钥，另一个由用户自己秘密保存，即私用密钥。信息发送者用公开密钥去加密，而信息接收者则用私用密钥去解密。

针对上面确定的双勾函数加密三元组（β，X_0，X_g），都采用上面基于素数的公共密钥机制来生成。这三个数中都是带小数的实数，为确保法线能尽可能不平行于 Y 轴，β 取值应在 30 至 60 之内为宜。同时，为了使第一次操作就是做法线，X_g 应取最低点 X_0 的右边值，即 X_g 大于 X_0。

在双勾函数曲线加密中，给定双勾函数曲线 E，基点 G 和点 kG（该点为从 G 点开始，做了 k 次上述操作后与双勾函数曲线 E 的交点），称（β，X_0，kG）为公钥，（β，X_0，G）值为私钥，更简单地 k 就是真正的私钥。

计算公钥和私钥利用了上述“运算”中两种操作：奇数为做渐近线的法线，记录交点的 y 值；偶数为做平行于 X 的平行线，记录交点的 x 值的负数，即记录双勾函数曲线下半部对称的点的 x 值。

采用 DHC 算法对数据进行加密和解密，首先要确定分组的大小。由于 DHC 算法计算出的取值（奇数为做渐近线的法线，取交点的 y 值；偶数为做平行于 X 的平行线，取交点的 x 值的负数，即记录双勾函数曲线下半部对称的点的 x 值）是用 4 字节表示的浮点数表示，而从缓冲区明文 M 中取出的数是整数（次数），为保证加密后的报文长度不变，每次从 M 中取 4 字节的整数 i 出来，从双勾函数曲线的点 kG 处做 i 次运算，从而得到 4 字节明文对应的密文。

使用 DHC 算法解密时，从双勾函数曲线的点 G 处循环做运算（奇数为做渐近线的法线，取交点的 y 值；偶数为做平行于 X 的平行线，取交点的 x 值的负数，即记录双勾函数曲线下半部对称的点的 x 值），直至与 4 字节密文所对应的浮点数差小于 0.000 01 为止（按照 IEEE754 的标准，单精度浮点数有效位最多小数点后 7 位），并将这次的循环次数 n 减去私钥 k 所得的整数，其 4 字节所对应的二进制就是明文中对应的 4 字节信息。

上述加解密保证了明文和密文等长，但以 4 字节作为整数的过程计算量大。为此取明文中的 2 字节作为整数（操作次数），每次从 M 中取 2 字节的整数 i 出来，从双勾函数曲线的点 kG 处做 i 次运算，从而得到 2 字节明文对应的 4 字节密文，因而密文长度是明文的 2 倍。为了更快的应用场合，也可以每次从 M 中取 1 字节的整数 i 出来，从双勾函数曲线的点 kG 处做 i 次运算，从而得到 1 字节明文对应的 4 字节密文，因而密

文长度是明文的 4 倍。

使用 DHC 算法进行数字签名时,设私钥、公钥分别为 k 、K ,即 $K=kG$,其中 G 为位于双勾函数($y=ax+b/x, ab>0$)曲线上的基点。设定哈希值用 h 表示,私钥用 k 表示,随机数用 r 表示,根据如下原理:

$hG/s+xK/s=hG/s+x(kG)/s=(h+xk)G/s=r(h+xk)G/(h+kx)=rG$ 。

(1)私钥签名的过程。

(a)选择随机数 r ,计算点 rG 。

(b)根据随机数 r ,消息 M 的哈希值 h ,私钥 k ,计算 $s=(h+kx)/r$ 。

(c)将消息 M 和签名 $\{rG, s\}$ 发给接收方。

此处的消息 M 为采用 DHC 算法对数据进行加密后的信息。

上述计算中, x 表示双勾函数曲线的基点 G 的 X 轴值, kx 是指在双勾曲线上从基点做了 k 次上文所提的操作(垂直线和平行线)的次数。

(2)公钥验证签名的过程。

(a)接收方收到消息 M 以及签名 $\{rG, s\}$ 。

(b)根据消息 M 采用与发送方相同的哈希算法求解哈希值 h 。

(c)使用发送方公钥 K 计算: $hG/s+xK/s$,将计算结果与 rG 比较,如相等即验签成功。

上述计算中, xK 指在双勾曲线上从点 K 做了 x 次上文所提的操作(垂直线和平行线)的次数。

2.3　基于双勾函数的格加密研究

利用量子干涉效应使得“量子并行计算”的若干个计算结果中,一部分的计算结果被量子干涉所强化,而另外一部分被量子干涉所抵消。这将导致观测到特定结果的概率增加,从而使得量子计算机以更高的概率输出想要得到的计算结果。基于此量子干涉效应,Peter Shor 于 1994 年提出了 Shor 算法。Shor 算法可以用量子计算机以多项式时间求解周期函数的周期,而 RSA、椭圆曲线等密码体制所基于的困难问题:大整数分解和离散对数求解,都可以转化为周期函数求解周期的问题,因而可以通过 Shor 算法求解。这使得现有的公钥密码体制很容易被量子计算机所击破。

2019 年《Nature》上发表了 Google 最新一代量子处理器 Sycamore,它包含 53 个量子比特,对量子处理器的输出进行重复性采样,并与经典计算机模拟的结果进行比较。Sycamore 完成同样的任务只需要 200 秒,而 Google 估计使用目前世界上最强大的超级计算机 Summit 需要 1 万年,以此证明该量子处理器实现了量子优越性(quantum supremacy)。IBM 提出使用二级存储可以模拟 54-bit 量子计算机,并且通过优化将经典计算机执行任务的时间从 1 万年降低到 2.55 天。针对量子计算机的这种威胁,密码学家们提出了“后量子密码”这一概念。从广义的角度上说,后量子密码学研究量子计算机出现后将对密码学产生的影响;从狭义的角度上说,后量子密码主要关注于设计可抵抗量子计算威胁的密码算法,尤其是公钥加密和数字签名算法。

格密码就是这样一类备受关注的抗量子计算攻击的公钥密码体制。2020 年 7 月 22 日,美国国家标准局 NIST 公布了其举办的后量子密码标准竞赛的第三轮入选算法,这意味着从 2016 年开始的美国后量子密码标准制定工作进入了最后的冲刺阶段,在 7 个正式入选第三轮的算法中,有 5 个都属于格密码的范畴。而与此同时,在中国密码学会举办的后量子密码算法竞赛中,格密码也在其中占据了相当大的比例。

格(lattice)是一种数学结构,定义为一组线性无关的非 0 向量(称作格基)的整系数线性组合。具体来说,给定一组格基, $x_1, x_2, \cdots, x_n$ 对任意的整数 $c_1, c_2, \cdots, c_n$, $c_1x_1, c_2x_2, \cdots, c_nx_n$ 都是属于这个格的向量,其中 n 称为格的维数。基于格的密码学近年来发展迅速,利用格上困难问题作为极微本原来构造的密码学方案层出不穷[17-20]。

$$\begin{cases} y_1 = a_1x_1 + \dfrac{b_1}{x_1} \\ y_2 = a_2x_2 + \dfrac{b_2}{x_2} \\ \cdots \\ y_n = a_nx_n + \dfrac{b_n}{x_n} \end{cases} \tag{5}$$

显然 $c_1y_1, c_2y_2, \cdots, c_ny_n$ 也是双勾函数且是非线性的,故构成了格;同时 $c_1y_1+c_2y_2+\cdots+c_ny_n$ 也是双勾函数考虑。双勾函数在正一象限的曲线,由这个格构成了一个双勾曲线空间(正半部曲线),包含了无穷多条这样的曲线,其中每条曲线由 a 和 b 两参数决定。

在用格进行加密时,需要求解数学难题来加大破解的计算量。取明文中三字节(并增加 1)构成一个正整数 a_k ,现取一未知的整数 b_k ,构成双勾曲线空间中的一条双勾曲线 y_k 。

选取 $c_{1k}, c_{2k}, \cdots, c_{nk}$,使得 $c_{1k}a_1+c_{2k}a_2+\cdots+c_{nk}a_n=a_k$ 且 $c_{1k}b_1+c_{2k}b_2+\cdots+c_{nk}b_n=b_k$,即由 $y_1, y_2, \cdots, y_n$ 构成 y_k 。当允许 $c_1, c_2, \cdots, c_n$ 为正有理数时,计算满足上式中 $c_{1k}, c_{2k}, \cdots, c_{nk}$ 的和为最小可以看成是一数学难题,存在进行加密的条件了。

另外,在这个双勾曲线空间中,求该曲线与任意两条曲线的交点。比如上式中 y_1 和 y_2 两条曲线的交点 (X_c, Y_c) ,其中:

$$X_c = \sqrt{\frac{b_2 - b_1}{a_1 - a_2}} \tag{6}$$

在用格进行加密时所构成的双勾曲线 y_k，其与上面 n 条曲线的交点为($X_{k1}, X_{k2}, \cdots, X_{kn}$)，现在就是找出整数 b_k 使($X_{k1}, X_{k2}, \cdots, X_{kn}$)存在，因为为负值开根号不成立(也即没交点，此时取值为 0，表示没交点)。对于每个整数 a_k 找出满足这条件的最小 b_k，其计算量随 n 的增大而加大，也可以看成是一数学难题，故而存在进行加密的条件了。

3 仿真实验或案例分析

在联想工作站(四颗 Inter i5－6500 Cpu，48G 内存)上进行仿真实验，同时在加解密的速度上与椭圆曲线加密算法(ECC)进行对比。在实现 ECC 时调用了 LibTommath 库(源码网址：https://blog. csdn. net/cg129054036/article/details/83862918)。

在用双勾函数加、解密(算法流程如图 3、4 所示)时，先根据选定的参数 a 、b 和基点的 x，依次做渐近线的法线和交点的 x 轴平行线，从而初始生成加密码值表。考虑到码值表的大小与取原文的字节数相关，这里取原文 1 个字节数来对应码值表前 256 个浮点数。这两算法的加密速度对比见表 1。

表 1 与椭圆曲线加密算法的速度对比

文件大小/KB	ECC 加密/s	本算法加密/s	本算法解密/s
221	340	0.03	0.202
38 197	33 000	4.647	32.558

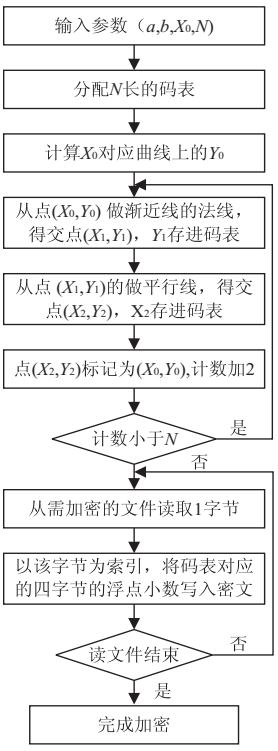

图 3 基于双勾函数的加密流程

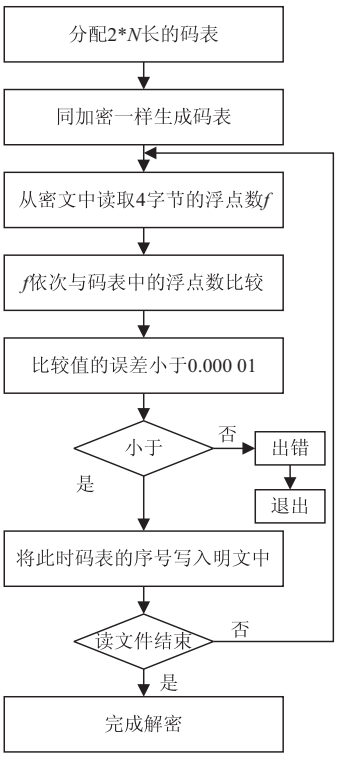

图 4 基于双勾函数的解密流程

在应用案例上，将基于双勾函数数字签名法的加密算法(DHC)应用到了电力云培训仿真中，确保了云培训考核的安全性。具体实施过程如下：

(1)教员根据每个学员的邮箱信息在密码中心为其申请证书，如图 5 所示，为学员 Bob 的邮箱“bob@b. com”申请证书。

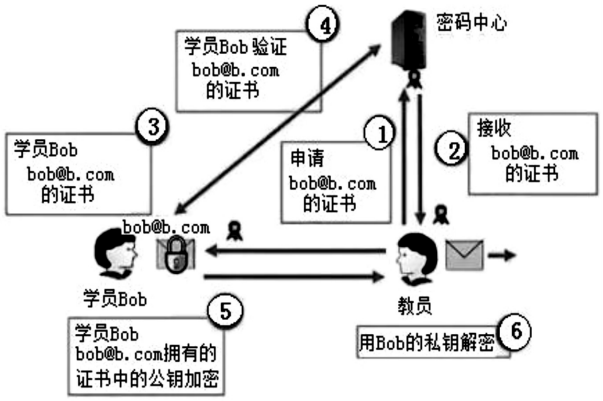

图 5 双勾函数的非对称加密应用

(2)教员收到密码中心下发的学员 Bob 的私钥。

(3)学员 Bob 从密码中心获得他的公钥。

(4)学员 Bob 对获得的公钥进行验证以确定是他的公钥。

(5)学员 Bob 采用获得的公钥加密其考试答案，并利用自已的私钥进行数字签名，一并发给教员。

(6)教员采用学员的公钥对数字签名进行验证，验证通过后，采用学员 Bob 的私钥解密报文，获得学员 Bob 的考试答案。

4　结束语

双勾曲线函数仅由两个参数决定其曲线形状,可以在其曲线上添加某种操作来进行对称和非对称的加密。该文通过对其渐近线添加垂直线操作以及线上点的 X 轴平行线操作,将明文数值对应为交替所做的垂直线和平行线的次数,用最后一次交点的 X 或 Y 值作为对应的密文。这种对称加密算法比椭圆曲线加密算法快了两个数量级,在此基础上可设计相应的非对称加密算法(DHC)来满足快速加密场合的需求。同时可选择任意条双勾曲线函数作为格基,来构成非线性的格空间,从而具有了进行格加密的可能。

参考文献:

[1] 陈智雨,郝悍勇,王　栋,等. 电力量子保密通信实用化技术研究进展与展望[J]. 电力信息与通信技术,2018,16(4):15-23.

[2] 李　健,陈　为. 基于异构条件的 NIDS 网络安全技术研究[J]. 计算机技术与发展,2017,27(9):106-109.

[3] LI X X,QIAN H F,WENG J,et al. Fully secure identity-based signcryption scheme with shorter signcryptext in the standard model[J]. Mathematical and Computer Modelling,2013,57(3 - 4):503-511.

[4] LI F G,TAKAGI T. Secure identity-based signcryption in the standard model[J]. Mathematical and Computer Modelling,2013,57(11-12):2685-2694.

[5] 伍育红,胡向东. 工业互联网网络传输安全问题研究[J]. 计算机科学,2020,47(6A):360-363.

[6] 黄克振,连一峰,冯登国,等. 基于区块链的网络安全威胁情报共享模型[J]. 计算机研究与发展,2020,57(4):836-846.

[7] 丁　伟,王国成,许爱东,等. 能源区块链的关键技术及信息安全问题研究[J]. 中国电机工程学报,2018,38(4):1026-1034.

[8] 方　芳,李广华,汪冬辉,等. 变电站内传输 IEC 62351 通信密钥的加密传输方法[J]. 中国电力,2019,52(10):26-30.

[9] 胡　洋,任振兴,滕国山,等. 一种基于 IEC 62351 的变电站远动通信混合加密算法[J]. 电力信息与通信技术,2018,16(5):24-29.

[10] 夏先智,赵　毅. 基于椭圆曲线加密算法技术优势的探讨[J]. 计算机科学,2003,30(10):181-183.

[11] 高洪波,马素萍. 椭圆曲线算法在射频识别技术加密中的优势[J]. 现代电子技术,2012,35(10):87-89.

[12] 杨艳梅,刘心军. 舰船通信网络中的数据加密技术[J]. 舰船科学技术,2019,41(6A):124-126.

[13] 陈小明. 舰船通信网络中访问数据加密方案设计[J]. 舰船科学技术,2020,42(10A):88-90.

[14] 刘　华. 网络安全加密技术在舰船数据传输中的应用[J]. 舰船科学技术,2020,42(9A):127-129.

[15] 王小云,刘明洁. 格密码学研究[J]. 密码学报,2014,1(1):13-27.

[16] 杨亚涛,赵　阳,张卷美,等. 同态密码理论与应用进展[J]. 电子与信息学报,2021,43(2):475-485.

[17] AGRAWAL S,BONEH D,BOYEN X. Efficient lattice (H) IBE in the standard model[C]//Advances in cryptology - EUROCRYPT 2010. French Riviera: Springer,2010: 553 - 572.

[18] KIM K S,JEONG I R. Collusion-resistant unidirectional proxy re-encryption scheme from lattices[J]. Journal of Communications and Networks,2016,18(1):1-7.

[19] MICCIANCIO D,VOULGARIS P. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations[J]. Siam Journal on Computing,2013,42(3):1364-1391.

[20] SINGH K,RANGAN C P,BANERJEE A K. Lattice based identity based proxy re-encryption scheme[J]. J. Internet Serv. Inf. Secur,2013,3(3/4):38-51.