基于椭圆曲线的智慧课堂云平台加密传输算法①

张良杰
（福州工商学院工学院　福建福州 350715）

摘　要 针对目前 HTTPS 应用的一些缺陷，例如 SSL 证书收费问题、SSL 证书有效期问题等，导致的 HTTPS 应用不太灵活的情形，设计了一种适配非 HTTPS 和 Socket 自定义通信环境下的基于椭圆曲线的加密传输算法，在实际的智慧课堂云平台应用中，性能良好、简单高效，易于实现又不失安全性，具有一定的应用前景和推广价值。

关键词 椭圆曲线；智慧课堂；云平台；加密传输

Encrypted Transmission Algorithm of Smart Classroom Cloud Platform Based on Elliptic Curve

Zhang Liangjie
(School of Technology，Fuzhou Technology and Business University，Fuzhou，Fujian，350715，China)

Abstract In view of some shortcomings of current HTTPS applications, such as SSL certificate charging issues, SSL certificate validity issues, etc., the HTTPS application is not very flexible. An elliptic curve-based encrypted transmission algorithm adapted to non-HTTPS and Socket custom communication environments is designed. In the actual application of the smart classroom cloud platform, the algorithm has good performance, simple and efficient, easy to implement without losing security, and has a certain application prospect and promotion value.

Keywords Elliptic Curve；Smart Classroom；Cloud Platform；Encrypted Transmission

①本文系 2019 年福建省中青年教师（高校教育信息化专项）科研课题“基于深度学习的智慧课堂云平台的构建”（项目编号：JAT191923）的研究成果之一。

1 引言

自从20世纪90年代开始，互联网大规模发展，直到现在的4G、5G等移动通信的普及，网络给人们的生活带来了翻天覆地的变化。各种应用，甚至是移动应用，层出不穷，人们享受着高速带宽带来的便捷网络的同时，数据的安全问题就越来越突出。根据Thales eSecurity的调查报告，2016年26%的受访者表示遭遇了数据泄露，2017年的占比上升至36%，而到2018年这一比例明显上升至67%[1]。带宽的增加也给网络窃取数据带来了便利，如何在网络传输中保障数据的安全在当今是一个值得研究的热门课题。

HTTP协议无疑是当今网络传输最通用的标准协议，但HTTP不安全，所传输的数据都是明文，因此就有了HTTPS的流行。但是HTTPS也有相应的缺陷，SSL证书通常是需要费用的，证书的有效期通常都是一两年，而且SSL证书通常需要绑定域名，应用起来不灵活，HTTPS通常占用资源较多，对缓存的支持也不友好。

本文从实际应用出发，以智慧课堂云平台为实际应用场景，提出一种基于椭圆曲线的加密传输算法，简单高效，又不失安全性。

2 椭圆曲线

椭圆曲线是指由Weierstrass方程所确定的平面曲线。其三次非奇异方程的一般形式如公式（1）。

$$y^2=x^3+ax+b,\ 4a^3+27b^2\neq 0 \qquad (1)$$

若取a=−2.8，b=1，则曲线如图1所示。

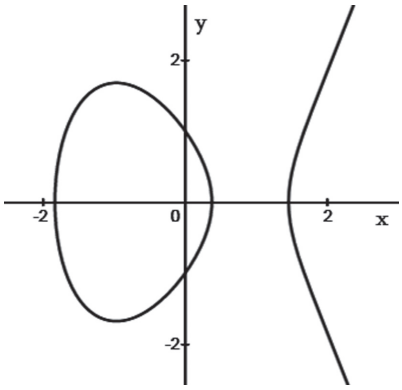

图 1　a=−2.8，b=1 曲线

椭圆曲线的几何特点是：

（1）曲线关于X轴对称；

（2）一条直线与椭圆曲线最多有三个交点。

椭圆曲线的加法M+N=Q定义到几何学上为：连接M点和N点的线段延长与椭圆曲线相交第三点为−Q，把−Q做X轴对称获得点Q即为相加后的结果点，而−Q为Q的逆元，如图2所示。

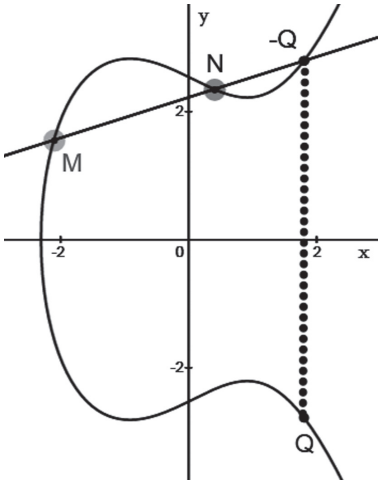

图 2　椭圆曲线的加法运算

加法运算是椭圆曲线的基本运算，可用加法去拓展其他运算，例如椭圆曲线的标量乘法实际上就是点的不断自加，定义无穷远点0为单位元，则2M=M+M，即按M点做曲线的切线，相交椭圆曲线的第三点（无穷远点也算一个点）即为2M的逆元。

3 本加密传输算法

本算法在智慧课堂云平台的实际应用中，以图像加密为例，主要应用场景为人脸识别照片的加密传输以及在课前、课后阶段学生的笔记、作业等照片的加密传输。在实际的应用场景中，从摄像头获得原始图像后便依照平台规定的某一算法生成密钥（种子为时间戳和用户ID）开始对图像加密，加密结束即代表端侧处理完成，接着需要依照规范调用云平台接口传输加密数据。

在图像传输上，由于端侧不做任何的图像持久化存储（包括原始图像），为了保障云平台能够解密接收到图像，以及在传输过程中为了使数据防篡改，对加密后的图像应用MD5散列获取16位字符串校验码，实际只需加密传输时间戳（13位）+用户ID（7位）+校验码（16位）共36位字符串数据即可。

HTTPS无疑是网络安全传输事实上的标准，文献[2]描述了Android平台下正确安全使用HTTPS协议保障传输安全的方式。然而即便部署了HTTPS协议，在未使用安全参数和未能正确配置情况下也会暴露安全问题[3]。为了适配在非HTTPS以及Socket自定义通信环境下的安全性，平台在数据传输上采用了椭圆曲线加密算法。近年来，椭圆曲线加密算法得到了非常广泛的应用，早在2010年就已经成为了国产商用密码的标准[4]，椭圆曲线加密算法的优势是在非对称加密领域里，在保证同样安全性情况下，它比RSA拥有更小的密钥尺寸，更容易应用到手机等资源受限的终端上[5-6]。赵辉[7]等设计并实现了一个跨平台的椭圆曲线加密系统，新算法运算速度较快。陈辉焱[8]等构造了一种基于椭圆曲线的高效前向安全数字签名方案，有力地保证了新签名方案的正确性和安全性。赵洁[9]等提出了一种基于椭圆曲线加密和cookie信息的物联网终端安全认证协议，用于解决物联网中终端设备接入网络服务器的安全性问题。程文彬[10]等设计了基于椭圆曲线密码体制的密钥管理机制来达到保障密钥安全的目的。陈亚茹[11]等从椭圆曲线数字签名的安全性和计算的高效性出发，提出了一种椭圆曲线数字签名的改进方案。可见，椭圆曲线在各领域应用广泛。

为了把椭圆曲线应用到加密上，需要由原来的实数域上的定义转换成有限域上的定义，加密用到的便是椭圆曲线上离散化的点，对公式（1）进行离散处理，如公式（2）所示定义在大素数p下的有限域F_p椭圆曲线方程。

$$y^2 = x^3 + ax + b \pmod{p},\ 4a^3 + 27b^2 \neq 0 \pmod{p} \quad (2)$$

其中a、b的约束条件为小于p的非负整数。椭圆曲线的加密依据是离散对数问题，即已知G和k，求kG很容易，但已知G和kG，求k却非常困难。

本系统应用了密码标准化组织（SECG）推荐的secp256k1椭圆曲线，密钥长度为256位，密钥空间充足。由于其构造在独特的Koblitz曲线上，占用更少的带宽和存储资源，也成了区块链中的关键加密技术。其参数为：

p=FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F

a=00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

b=00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000007

G=(79BE667E F9DCBBAC 55A06295 CE870B07
029BFCDB 2DCE28D9 59F2815B 16F81798,
483ADA77 26A3C465 5DA4FBFC 0E1108A8
FD17B448 A6855419 9C47D08F FB10D4B8)

n=FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE
BAAEDCE6 AF48A03B BFD25E8C D0364141

因明文数据的字符定义域是数字和小写字母的36个字符，设计了如表1所示的点与字符的编码表，其中G为椭圆曲线的基点，G^k为基点的k次幂。

表 1　有限域椭圆曲线上的点与字符对应编码表

G^1	G^2	G^3	G^4	G^5	G^6
c	3	o	b	1	d
G^7	G^8	G^9	G^{10}	G^{11}	G^{12}
9	m	l	2	k	4
G^{13}	G^{14}	G^{15}	G^{16}	G^{17}	G^{18}
6	5	y	8	t	j
G^{19}	G^{20}	G^{21}	G^{22}	G^{23}	G^{24}
7	a	u	z	x	e
G^{25}	G^{26}	G^{27}	G^{28}	G^{29}	G^{30}
r	q	i	v	f	w
G^{31}	G^{32}	G^{33}	G^{34}	G^{35}	G^{36}
0	p	s	n	g	h

具体加密传输算法如下：

（1）端侧获取云平台的secp256k1椭圆曲线的公钥K（云平台的私钥为k），该公钥也可在端侧首次登录时获取并保存本地；

（2）端侧随机生成自己的私钥r，并计算$C_0=rG$加密点坐标；

（3）遍历明文36位字符串数据分别生成$C_1=M_1+rK$、$C_2=M_2+rK$，…，$C_{36}=M_{36}+rK$加密点坐标，其中M_1，M_2，…，M_{36}为每个字符按表1的编码点；

（4）把C_0，C_1，…，C_{36}的37个加密点拼凑成一个点集字符串；

（5）在点集字符串末尾拼接16个零作为占位符，应用MD5散列获取16位字符串校验码替换占位符；

（6）应用gzip算法对包含校验码的字符串进行压缩处理，并用Base64编码成可见字符串；

（7）联合加密后的数据（例如图像）一起传输到云平台；

（8）云平台接收后进行解压、校验、解密处理，过程就不在赘述。

解密原理采用的是ElGamal算法[12]，以第一个字符为例：

$$C_1-kC_0=M_1+r(kG)-k(rG)=M_1 \quad (3)$$

即可通过编码表获取M_1点所对应的字符，其余字符解密类似。

4　本算法实际应用情况

本算法在智慧课堂云平台上得到了实际应用，主要应用场景为人脸识别照片的加密传输以及在课前、课后阶段学生的笔记、作业等照片的加密传输，实际应用的流程如图3所示，以作业提交为例，实际端侧情况如图4和图5所示，实际应用的网络传输如图6所示。

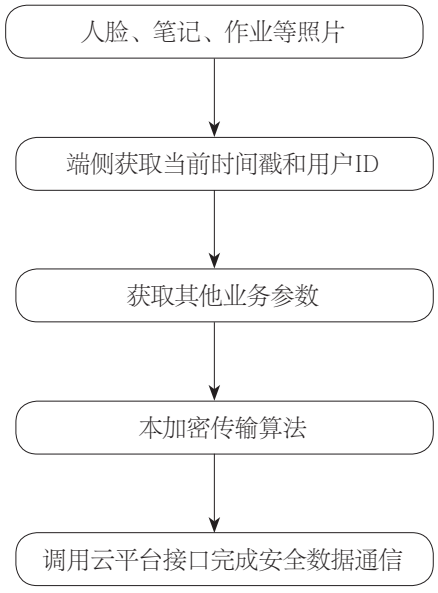

图 3　实际应用流程图

图 4　端侧作业任务界面

图 5　端侧作业提交界面

图 6　实际应用的网络传输

5　结语

本文从实际应用出发，以智慧课堂云平台为实际应用场景，提出一种基于secp256k1椭圆曲线的加密传输算法，在实际的系统应用中加密传输效果良好，简单高效，易于实现又不失安全性。未来的进一步研究和算法的迭代，会进一步关注性能上的改进，并扩展加密传输算法在智慧课堂云平台其他场景上的应用，逐步剥离构造通用场景下的加密传输算法。

参考文献

[1] 腾讯网络安全与犯罪研究基地. 2018网络安全大事件盘点[EB/OL]. [2019-01-18] https://www.sohu.com/a/289835406_786964 html.

[2] WEI X T, WOLF M. A Survey on HTTPS Imple-Mentation by Android Apps: Issues and Countermeasures [J].Applied Computing and Informatics, 2017, 13(2): 101—117.

[3] HUANG J K, ZHANG Z X, LI W J, et al. Assessment of the Impacts of TLS Vulnerabilities in the HTTPS Ecosystem

of China ［J］. Procedia Computer Science，2019（147）：512—518.

［4］姚键. 国产商用密码算法研究及性能分析［J］. 计算机应用与软件，2019，36（6）：327—333.

［5］NATANAEL D，FAISAL，SURYANI D. Text Encryption in Android Chat Applications Using Elliptical Curve Cryptography（ECC）［J］. Procedia Computer Science，2018（135）：283—291.

［6］KHAN A A，KUMAR V，AHMAD M. An Elliptic Curve Cryptography Based Mutual Authentication Scheme for Smart Grid Communications Using Biometric Approach［J］. Future Genetation Computer Systems. 2018（81）:557—565.

［7］赵辉，史蕊. 一种基于椭圆曲线加密系统的设计与实现［J］. 河南大学学报（自然科学版），2011，41（1）：81—84.

［8］陈辉焱，袁勇，万宗杰，等. 一种基于椭圆曲线的前向安全数字签名［J］.电信科学，2015，31（10）：106—109.

［9］赵洁，张华荣. 椭圆曲线加密结合cookie信息的物联网终端安全认证协议［J］.电信科学，2016，32（6）：136—142.

［10］程文彬，刘佳. 基于ECC的智能家居密钥管理机制的实现［J］.电信科学，2017，33（6）：121—128.

［11］陈亚茹，丛培强，陈庄. 一种椭圆曲线数字签名的改进方案［J］. 信息安全研究，2019，5（3）：217—222.

［12］KAMALAKANNAR V，TAMILSELVAN S. Security Enhancement of Text Message Based on Matrix Approach Using Elliptical Curve Cryptosystem［J］. Procedia Materials Science，2015（10）:489—496.