

**本科毕业论文**

题 目：物联网网关轻量级认证和加密技

技术研究

姓 名：郑智聪

学 号：201642030

院 系：信息科学与工程学院

专 业：电子信息科学与技术

年 级：2016级

指导教师：郭本振

二○二○年 六 月

物联网网关轻量级认证和加密技术研究

Lightweight authentication and encryption technology for IoT gateway

Technical research

**郑 重 声 明**

本人呈交的学位论文（设计），是在指导教师的指导下，独立进行研究工作所取得的成果，所有数据、图片资料真实可靠。除文中已经注明引用的内容外，本学位论文（设计）的研究成果不包含他人享有著作权的内容。对本论文（设计）所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确的方式标明。本学位论文（设计）的知识产权归属于河北北方学院。

本人签名： 日

**摘 要**

物联网技术飞速发展的同时，其安全问题也变得日益重要。在一种基于物联网技术设计的温室环境监控系统中，需要实现用户智能APP与物联网节点设备（如传感器、控制器等）之间的实现双向身份认证的安全策略，以保证系统的安全。因此，文章设计了一种使用EC加密算法和云服务器协助的双向认证策略。实验证明该策略可在较低的资源需求情况下，满足用户智能手机APP与物联网节点设备之间，进行双向身份认证的要求。

**关键词** 物联网安全，双向认证，密钥协商，椭圆曲线，安全策略

[第一章 引言 3](#_Toc3933)

[1.1 研究背景 3](#_Toc19594)

[1.2国内外研究现状 3](#_Toc11411)

[1.2.1 国外研究现状 3](#_Toc25533)

[1.2.2 国内研究现状 4](#_Toc7843)

[1.3 主要研究内容 4](#_Toc23091)

[1.4 研究意义 4](#_Toc31340)

[第二章 相关理论和技术 5](#_Toc6646)

[2.1 对称和非对称加密 5](#_Toc4077)

[2.1.1 对称加密 6](#_Toc28855)

[2.1.2 非对称加密 6](#_Toc1272)

[2.2 椭圆曲线相关理论 7](#_Toc26692)

[2.2.1 椭圆曲线概述 7](#_Toc21092)

[2.2.2 椭圆曲线上的运算 8](#_Toc15214)

[2.2.3 椭圆曲线上的离散数对问题 10](#_Toc8129)

[2.2.4 基于椭圆曲线的DH秘钥交换（ECDH） 10](#_Toc4961)

[2.3 AES加密算法 11](#_Toc6635)

[第三章 需求分析 13](#_Toc22652)

[3.1 可行性分析 13](#_Toc746)

[3.1.1 技术可行性分析 13](#_Toc31531)

[3.1.2 经济可行性分析 13](#_Toc28152)

[3.1.3 操作可行性分析 13](#_Toc31827)

[3.2 农业物联网特殊安全问题分析 13](#_Toc28845)

[3.2.1 终端节点安全问题分析 13](#_Toc31307)

[3.2.2 通信网络安全问题分析 13](#_Toc6818)

[3.2.3 物联网应用安全问题分析 13](#_Toc28282)

[第四章 基于ECC的双向认证和秘钥协商算法设计 14](#_Toc20232)

[4.1 算法整体设计 14](#_Toc26900)

[4.2 数字签名算法详细设计 14](#_Toc14332)

[4.2.1 客户端的设计与实现 14](#_Toc17292)

[4.2.2 服务器端设计与实现 14](#_Toc2482)

[4.2.3 数字签名的实现 14](#_Toc18349)

[4.3 数据加密解密算法详细设计 14](#_Toc15266)

[4.4 算法耗时分析 14](#_Toc30851)

[4.4.1 秘钥协商耗时分析 14](#_Toc20564)

[4.4.2 加密解密耗时分析 14](#_Toc21363)

[4.5 算法安全性分析 14](#_Toc18577)

[第五章 系统测试 14](#_Toc21302)

[5.1 测试环境 14](#_Toc1270)

[5.1.1 硬件平台 14](#_Toc2969)

[5.1.2 软件平台 14](#_Toc12604)

[5.2 性能测试 15](#_Toc11297)

[第六章 结论 15](#_Toc28343)

[谢辞 15](#_Toc26897)

[参考文献 15](#_Toc24540)

# 引言

## 1.1 研究背景

随着互联网和通信技术的快速发展，人们已经不再满足传统的人与人以及其他需要人参与交互的通信方式，物联网——一种不需要人参与，只需要机器和机器之间信息交互的通信方式应运而生。1999 年，MITAuto-ID中心的Ashton 教授最早提出了物联网这个名字，2005 年在国际电信联盟（ITU）发布的《ITU 互联网报告2005：物联网》报告中，再次提出用了“物联网”的概念[1]。在十二五规划中，物联网被列为七大战略新兴产业之一，是我国重点发展的领域，在未来物联网将会彻底改变人们的生活。

在物联网蓬勃发展的同时，层出不穷的针对物联网的攻击事件，人们越来越关注物联网系统的安全问题。2015年黑客针对乌克兰的电力系统发起恶意攻击，导致70多万居民家庭停电数小时；2016年的Mirai事件中，攻击者利用网络摄像头等大量的物联网设备向域名服务器发起DDoS攻击，导致大量用户无法使用网络。据Gartner调查，全球近20%的单位和部门，近年来遭受过物联网攻击。

一般的物联网体系主要由三层组成，自下而上分别为：感知层、传输层、

应用层。物联网一般的工作模式是：感知层负责感知周围的信息，并通过传输层连接上应用中心，应用中心负责数据的汇集、分析等。其中传输层和应用层可以在现有的，成熟的架构基础上运作实施，这两层的安全保护都有成熟的认证体系，

而对于感知层，因为硬件资源受限、传感器节点分布较广泛等特点，现有的安全技术无法很好地实施，迫切需要一种轻量级的认证和加密体系。

## 1.2国内外研究现状

### 1.2.1 国外研究现状

近年来，随着物联网中的安全问题日益暴露，世界各地越来越多的官方组织、学术机构加入到物联网安全的研究当中，旨在构建一系列的安全规范和协议。

Nicanfar 等[2]在 2015 年提出了一个基于椭圆曲线加密的认证协议。尽管他们的方案大大降低了计算复杂度， 但是由于可信任的第三方需要密码表来保存用户信息而易受 到表丢失或被窃取的攻击。之后，Li等[3]提出一个新的密码 协议但同样也被证明易受到窃听，并且由于缺少密钥协商而易受到模仿攻击。2019年Q.Jiangetal.[4]在分析Das协议的基础上，提出了一种新的在云服务器协助下，实现可穿戴设备认证和密钥协商的安全协议。该协议使用了ECC算法进一步增强了数据的安全性，降低了协议对设备计算资源消耗。2019年Wangetal[5] 提出了一种使用ECC算法和云服务器辅助的物联网网关与用户智能手机进行双向身份认证和密钥协商的协议。

### 1.2.2 国内研究现状

近年来，物联网在我国的发展已经进入多行业落地阶段，同时也开始进入物联网安全建设阶段，相关科研单位及安全厂商都在积极探索物联网安全规范与技术[6] 。

2017年，汪洋在《物联网轻量级认证和加密技术研究》中，提出了一种新的 RFID 双向认证协议，在认证信息中加入随机数和时间戳，利用椭圆曲线密码算法（Elliptic curve cryptography, ECC）对认证过程中的敏感信息进行加密，保证认证信息的机密性[1]。2018年，史冰清在《高安全性的物联网网关设计与实现》中设计实现了能够在物联网网关上使用的混沌-AES加密算法，该算法密匙混沌化、密钥空间更大、实现了“一块一密”，并且没有增加密钥管理的负担[7].同年，王斌在《工业物联网信息安全防护技术研究》中，针对物联网不同的层次结构，针对性地设计了应用于不同层次结构的安全防护策略[8]

## 1.3 主要研究内容

本文针对当前物联网系统感知层设备多数使用对称密钥协议，构建网络安全基础设施。考虑到密钥维护工作繁多，运维人员经常接触通信密钥，容易引起密钥泄漏和内部特权人员攻击的情况。以及感知层设备计算、存储和通信资源有限，攻击者容易发起资源耗尽型的DDos攻击的情况。使用EC加密算法设计了一种系统云认证服务器（Cloud Authentication Server CAS）与物联网网关设备之间的双向认证、密钥协商的解决方案。

## 1.4 研究意义

对万事万物的感知能力是物联网技术的精髓，因此，感知层构成了物联网体系中举足轻重的一部分。感知层通过传感器等设备，借助于蓝牙、无线网络等传输信息到物联网中心系统，其结构图如下：

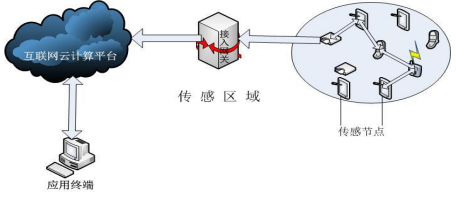


图 1.2 感知层结构图(这个图后面自己画)

在一般的物联网系统中，通常使用AES,DES等对称加密算法，但是对称加密算法又存在着秘钥泄露的风险，一旦攻击者通过非法手段获取了秘钥，后果不堪设想。而嵌入式设备又有着受限的资源，严苛的工作环境等特点，使用RSA等非对称加密算法的话，大大影响传感器的工作效率。因此，迫切的需要一种适用于嵌入式设备的轻量级认证和加密协议，在保障安全性的基础上，尽量降低带宽、内存等资源的占用，提高秘钥协商和加密解密的效率，这对于物联网安全的发展有着深远的意义。

# 第二章 相关理论和技术

## 2.1 对称和非对称加密

随着网络信息技术的发展，网络信息的安全问题成为了阻碍其发展的最大因素。人们的信息在网络中传输，很容易被不法分子拦截并篡改，轻则造成人们隐私数据的泄露，重则造成人民个人财产的损失。

而对网络信息进行加密则是保证机密信息和数据泄露的主要手段，以下为密码学中的一些基本概念。

1. 加密：将数据按照一定的规则进行变换的过程
2. 解密：将加密后的数据，按照规则转换成原数据的过程
3. 明文：加密之前的数据，能够被轻易读取
4. 密文：加密之后的数据，隐藏原文本的信息
5. 秘钥：控制加密和解密过程的参数

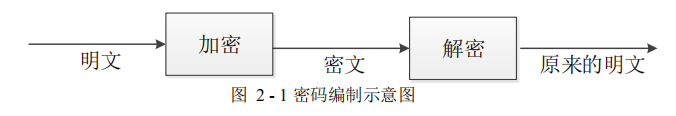


图 2-1应该在这里搞一个图

### 2.1.1 对称加密

对称加密指的是，加密和解密使用的秘钥是相同的。其特点是加密解密的速度较快，实施起来较为简单的同时也能有较好的安全性。对称加密的过程如下图所示：

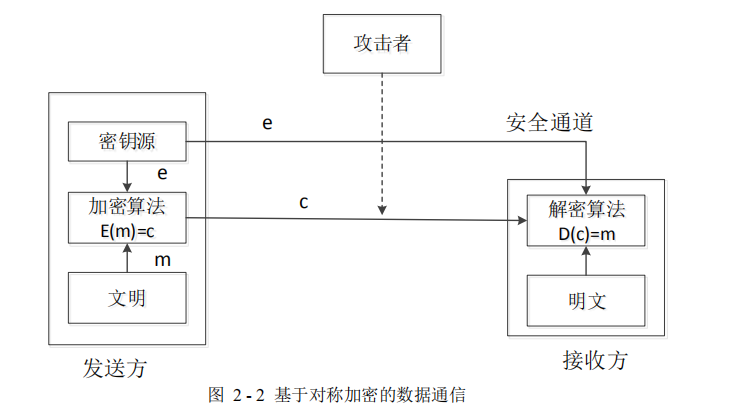


图 2-2 这个图到时候也得自己画

常用的对称加密算法按照加密解密的对象进行划分，还可分为分组密码算法和流密码算法两种。分组密码的加密方式是先将待加密的数据进行编码，然后将编码的数字划分成等长的分组，再对每一个分组进行秘钥加密。流密码的加密方式是对流数据的每一位或每字节进行加密处理。

由于对称加密的双方使用相同的秘钥，保障算法的安全性的前提是保障秘钥的安全性，双方都不能将秘钥泄露出去，否则会面临密码被破解的危险。而在物联网的环境中，网关节点等距离服务器都比较远，不可避免地具有在网络中传输秘钥的情况，在秘钥传输的过程中很容易被窃取。

### 2.1.2 非对称加密

非对称加密算法最早产生于上世纪七十年代[9]，与对称加密不同的是，非对称加密需要两个密钥来进行加密和解密，分别为公开密钥（public key，简称公钥）和私有密钥（private key，简称私钥），公钥加密的信息需要私钥才能解密，私钥加密的信息需要公钥才能解密。公钥可以在网络上进行传输，任何人都可以获得公钥，不存在秘钥泄露的问题。常用的非对称加密算法有RSA,ECC两种。 1. RSA算法

RSA密码体制是由 Rivest、Shamir 和 Adleman 在 1977 年联合提出的[1]。RSA 算法的原理是基于一个数论事实：将两个大素数相乘很容易，但是想要对其乘积进行因式分解却极其困难，因此可以将乘积公开作为公钥。

1. ECC算法

ECC算法是在1985年由Neal Koblitz和Victor Miller分别独立提出的。

相比于RSA算法，ECC可以做到在同等的安全强度下，具有更小的秘钥长度。ECC算法的原理是定义椭圆曲线上的运算，然后利用基于有限域上椭圆曲线点群离散对数分解难题，将倍点运算的结果作为公钥。本文将在2.2小节详细介绍ECC算法。

## 2.2 椭圆曲线相关理论

### 2.2.1 椭圆曲线概述

本文研究的椭圆曲线是指满足式2-1的方程

/var/folders/d3/w9bxxqbs4x16w4c5tgjc67y80000gn/T/com.kingsoft.wpsoffice.mac/wpsoffice.ZdT320wpsoffice 式 2-1公式2-1中p是一个较大的素数，且p值越大安全性越高，计算量也就越大。a，b∈ Ep用于确定具体的椭圆曲线，且需要满足公式2-2:

wpsoffice 式2-2

满足上述要求的椭圆曲线Ep(a,b)中，取点G，和整数k 则 K = kG，K也是椭圆曲线Ep(a,b)的点。在椭圆曲线中，给定G，k，容易求出 K; 但如果已知K和G，很难求出k。在椭圆曲线加密算法中，G称为基点( base point) ，k称为私钥( private key)，K称为公钥( public key)。确定了椭圆曲线和公钥、私钥之后，就可以用这些参数对数据进行加密

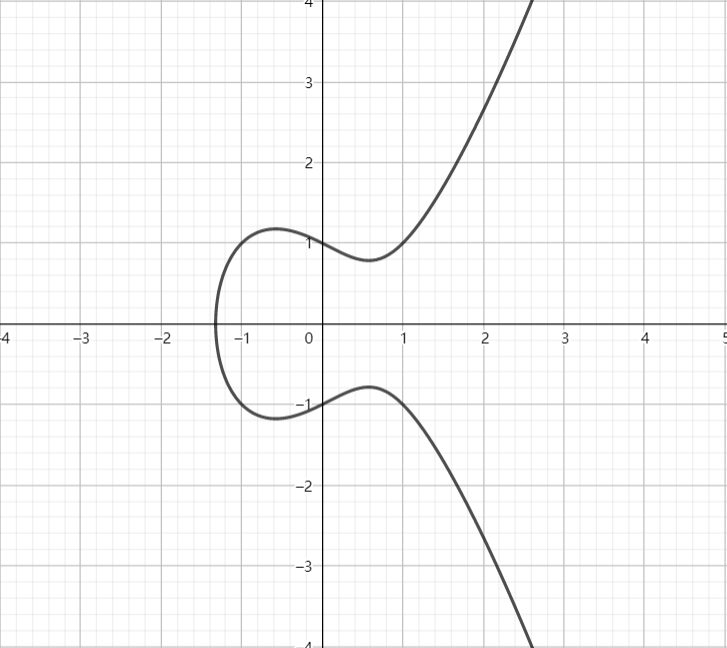


图2-3 椭圆曲线y^2 =x^3-x+1

### 2.2.2 椭圆曲线上的运算

椭圆曲线上的运算，其实指的就是椭圆曲线上点的加法和乘法

1. 椭圆曲线上的加法

设椭圆曲线上有两点，A和B点，那么作过这两点的直线与该曲线相交于第三点（C点），然后关于X轴对称得到D点，则D为这两个点的和，记作D=A+BD=A+BD=A+B。很明显，D点也在该曲线上。所以椭圆曲线上两点之和也是曲线上的点。

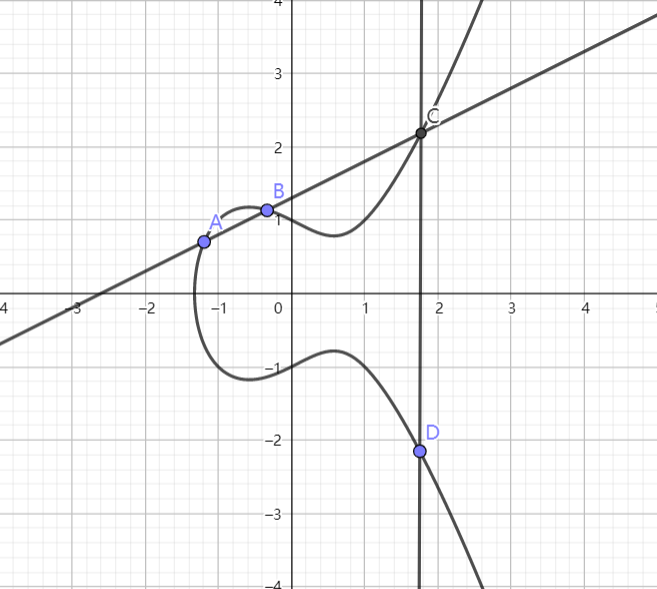


图2-4 椭圆曲线加法

若A=B,则为过A点的切线交于椭圆曲线为R'。如下图所示。

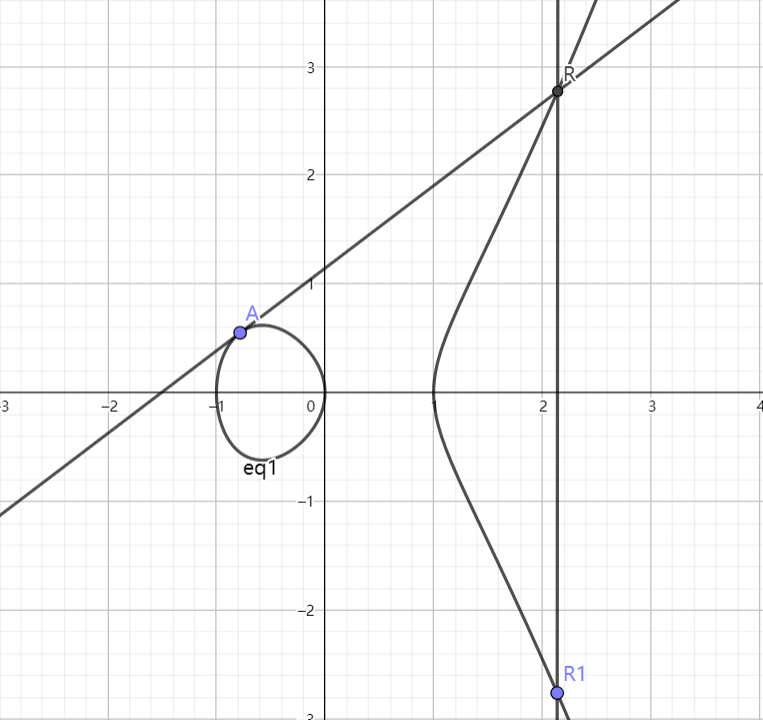
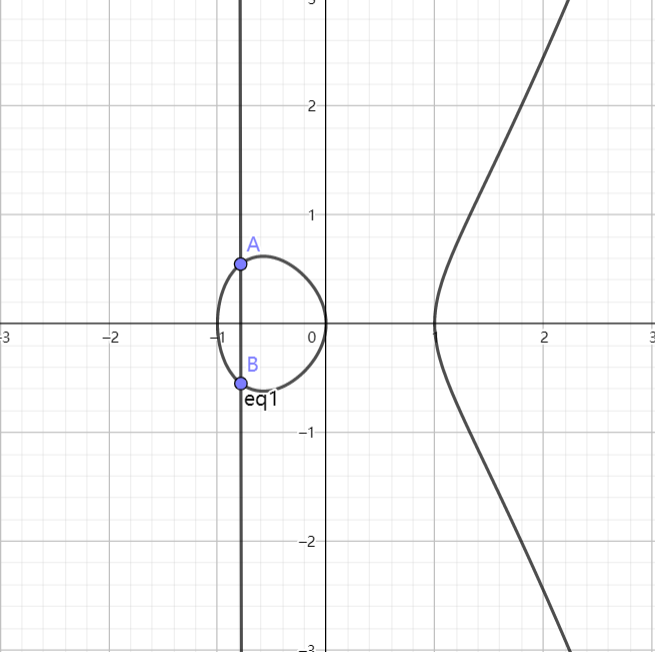


图2-5 A=B时椭圆曲线的加法

如果点A、B所在的直线刚好平行于Y轴时，根据椭圆曲线的性质，将永远不会有与曲线的第三个交点，我们定义坐标系中距离X轴无穷远点为椭圆曲线上的一个特殊点，称为0点（零点）。

 图2-6 AB垂直于X轴时

因为椭圆曲线关于X轴对称，所以对于曲线上任意一点A，总存在另一点B使得过A、B的直线垂直于X轴，也就是该直线与曲线交于0点，所以A+B=0。因为0点是距离X轴无穷远的点，所以过A点与0点的直线是垂直于X轴的，它与曲线相交于另一点B点，那么B点关于X轴对称的点就是A点，即A点为A点和0点之和。

由椭圆曲线加法的定义可以得出，椭圆曲线的加法满足交换律（A+B=B+A）和结合律（(A+B)+C = A+(B+C)）。

1. 椭圆曲线上的乘法

给定椭圆曲线上的一个点P，计算kP的过程也可以看成连续k个P相加的过程，此过程又称为倍点运算。由于椭圆曲线上的加法满足结合律，那么

P+P+P+P = 2P+2P

这样一来，假设要计算16P，则可以先计算出来2P，然后计算4P，如此类推，可以把16次的加法运算减少到4次，从时间复杂度的角度来看，这个算法是一个O(logk)的算法，这个方法被称为快速幂算法。可以大大减小倍点运算的时间复杂度，对于增加ECC算法的效率有十分重要的影响。

### 2.2.3 椭圆曲线上的离散数对问题

由椭圆曲线上的运算法则可以得出，当给定点P时，“已知数x求点xG的运算”不难，因为有加法的性质，运算起来可以比较快。但反过来，“已知点xG求x的问题”则非常困难，因为只能遍历每一个x做运算。这就是椭圆曲线密码中所利用的“椭圆曲线上的离散对数问题”。

### 2.2.4 基于椭圆曲线的DH秘钥交换（ECDH）

ECDH全称是椭圆曲线迪菲-赫尔曼秘钥交换（Elliptic Curve Diffie–Hellman key Exchange），主要是用来在一个不安全的通道中建立起安全的共有加密资料，一般来说交换的都是私钥，这个密钥一般作为“对称加密”的密钥而被双方在后续数据传输中使用。ECDH的流程如下

1. A选定一条椭圆曲线E，并取椭圆曲线上一点作为基点G。
2. A选择一个私有密钥k（k<n），并生成公开密钥K=kG。
3. A将E和点K、G传给B
4. B收到信息后，产生一个随机整数r（r<n,n为G的阶数） 假设r=6 要加密的信息为3,因为M也要在E29(4,20) 所以M=(3,28)
5. B计算点C1=M+rK和C2=rG。
6. B将C1、C2传给A
7. A收到信息后，计算C1-kC2，结果就应该是点M C1-kC2

数学原理:C1-kC2=M+rK-krG=M+rkG-krG-M

至此：A和B就协商出来相同的秘钥，后面就可以使用这个秘钥进行对称加密通信。攻击者只能获取中间在信道中传输的E和点K、G、C1、C2等，由于椭圆曲线的数学难题，无法计算出A和B的秘钥k、r，那么协商出来的秘钥也就是安全的。

图2-7 在这画一个流程图或者时序图

## 2.3 AES加密算法

AES算法最初是由比利时密码学专家Joan Daeman和Vincent Rijmen设计和提出，又叫做Rijmen算法[10]。最开始被用来替代DES算法，AES为分组密码，分组的长度为128位，根据秘钥的长度不同可以分为AES128、AES192、AES256三种，推荐加密的轮数也不同，本文使用的是AES128，每一种的加密轮数如下表

|  |  |  |  |
| --- | --- | --- | --- |
| AES | 密钥长度 | 分组长度 | 加密轮数 |
| AES128 | 4 | 4 | 10 |
| AES192 | 6 | 4 | 12 |
| AES256 | 8 | 4 | 14 |

表2-1

AES对软硬件的要求都相对较低，计算效率较高，容易在硬件设备上实施。AES采用轮加密的方式，加解密的关键步骤如下：

1. 字节代换与字节逆代换

AES定义了一个S盒和一个逆S盒，字节代换与字节逆代换就是一个简单的查表操作，例如加密是就是把明文字节按照S盒进行映射，如下图所示

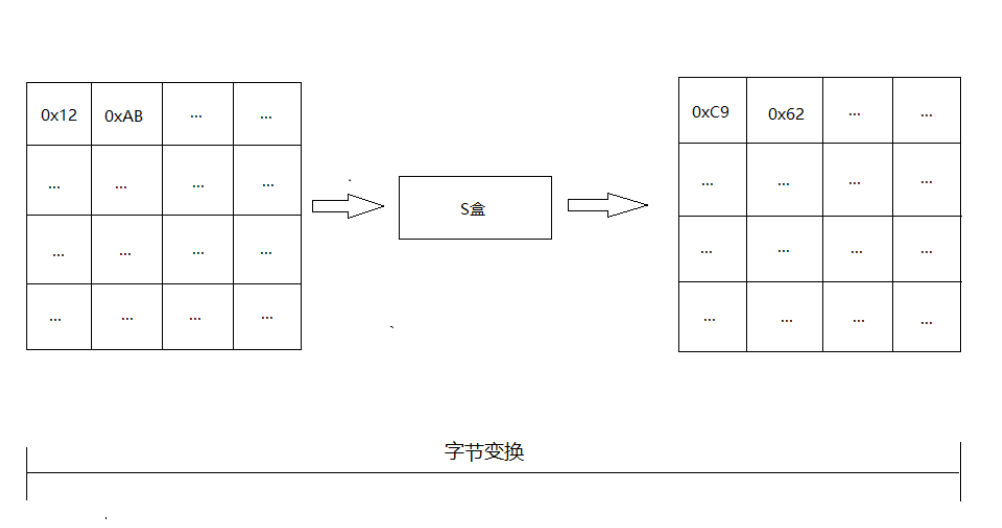


图2-8 AES字节代换

1. 行移位变换和行移位逆变换

行移位是左循环移位操作。在AES128中，状态矩阵的第1行左移0字节，第2行左移1字节，第3行左移2字节，第4行左移3字节，如下图所示：

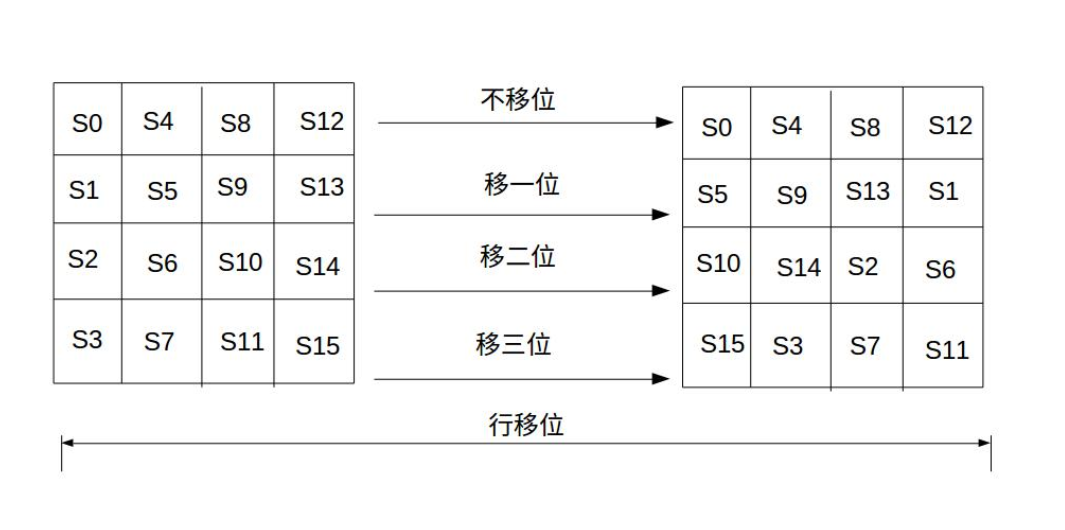


图2-9 AES行移位

行移位的逆变换就是行移位执行相反的操作。在AES128中，状态矩阵的第1行右移0字节，第2行右移1字节，第3行右移2字节，第4行右移3字节

1. 列混合与列混合逆运算

列变换就是对状态矩阵中的列进行混合变换。列混合变换是通过矩阵相乘实

现的，经行移位后的状态矩阵与固定的矩阵相乘，得到混淆后的状态矩阵。其中，矩阵元素的乘法和加法都是定义在基于GF(2^8)上的二元运算,并不是通常意义上的乘法和加法。逆变换矩阵同正变换矩阵的乘积恰好为单位矩阵。

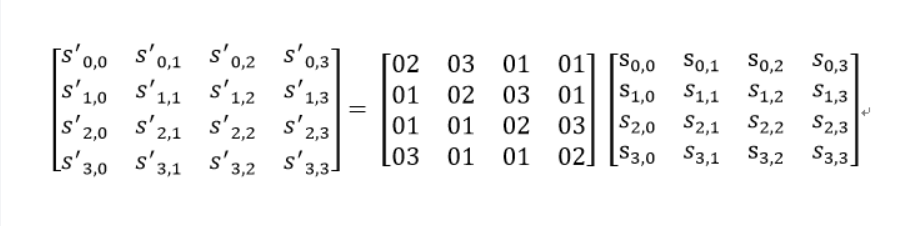


图2-10 列混合中的相乘

1. 轮秘钥加

轮密钥加是将轮密钥同状态矩阵中的数据进行逐位异或操作，轮密钥是通过初始密钥和轮密钥产生算法共同产生的。因为异或的逆操作是其自身，轮密钥加的逆运算同正向的轮密钥加运算完全一致。

# 第三章 需求分析

## 3.1 可行性分析

### 3.1.1 技术可行性分析

### 3.1.2 经济可行性分析

### 3.1.3 操作可行性分析

## 3.2 农业物联网特殊安全问题分析

### 3.2.1 终端节点安全问题分析

### 3.2.2 通信网络安全问题分析

### 3.2.3 物联网应用安全问题分析

# 第四章 基于ECC的双向认证和秘钥协商算法设计

## 4.1 算法整体设计

## 4.2 数字签名算法详细设计

### 4.2.1 客户端的设计与实现

### 4.2.2 服务器端设计与实现

### 4.2.3 数字签名的实现

## 4.3 数据加密解密算法详细设计

## 4.4 算法耗时分析

### 4.4.1 秘钥协商耗时分析

### 4.4.2 加密解密耗时分析

## 4.5 算法安全性分析

# 第五章 系统测试

## 5.1 测试环境

### 5.1.1 硬件平台

### 5.1.2 软件平台

## 5.2 性能测试

# 第六章 结论

# 谢辞

学生时代的生活是弥足珍贵的，因为时光是一张有去无返的单程票，关于北方学院有我带不走的记忆，更有带不走的收获。

# 参考文献

[1] 汪洋. 物联网轻量级认证和加密技术研究[D].南京邮电大学,2017.

[2] Nicanfar H, Leung V C M. Multilayer Consensus ECC-Based Password Authenticated Key-Exchange (MCEPAK) Protocol for Smart Grid System[J]. IEEE Transactions on Smart Grid, 2013, 4(1):253-264

[3] Li D, Aung Z, Williams J R, et al. Efficient and fault-diagnosable authentication architecture for AMI in smart grid[J]. Security & Communication Networks, 2015, 8(4):598-616.

[4] Q. Jiang, Y. Qian, J. Ma, X. Ma, Q. Cheng, and F. Wei, “User centric three-factor authentication protocol for cloud-assisted wearable devices,” Int J Commun Syst, vol. 32, no. 6, p. e3900, Apr. 2019.

[5] ZHIHUI WANG, JIANLI ZHAO, BENZHEN GUO, JINGJINGYANG, XIAO ZHANG. Mutual Authentication Protocol for IoT-based Environment Monitoring System[j]Journal of Environmental Protection and Ecology 2019,6(2)

[6] 袁琦. 我国物联网安全发展现状和建议[J]. 现代电信科技, 2014(10):36-39.

[7] 史冰清. 高安全性的物联网网关设计与实现[D].电子科技大学,2018.

[8] 王斌. 工业物联网信息安全防护技术研究[D].电子科技大学,2018.

[9] 黎俊男. 基于AES与ECC的游戏数据混合加密研究与实现[D].华南理工大学,2018.

[10]龙辉. 基于ECC-AES混合加密的智能配电网安全通信方案设计[D].湘潭大学,2016.