



标准版(适用于初检)----论文检测综合报告

温馨提示：定稿请使用VIP至尊版检测，至尊版检测更全面，结果更权威
论文狗查重学术不端检测系统（网址：<https://www.lunwengo.net>）

物联网网关轻量级认证和加密技术研究


报告编号:F689CEBAFB744E189914BC3D39E55D32	检测时间:2020-04-01 18:22:53	检测字数:12689
作者:郑智聪		

相似度:49.87% 引用率:13.17% 复写率:36.7% 自写率:50.13%

检测范围

中国期刊库
博士论文库
网友专利库
网页库
工作总结

中国图书库
会议论文库
网友标准库
网友共享库
思想汇报



硕士论文库
报纸库
百科库
自建库
项目申报书

一、全文标红

0
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
本人提交的学位论文（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

1.1 研究背景3

1.2国内外研究现状3

1.2.1 国外研究现状3

1.2.2 国内研究现状4

1.3 主要研究内容4

1.4 研究意义4

第二章 相关理论和技术5

2.1 对称和非对称加密5

2.1.1 对称加密6

2.1.2 非对称加密6

2.2 椭圆曲线相关理论7

2.2.1 椭圆曲线概述7

2.2.2 椭圆曲线上的运算8

2.2.3 椭圆曲线上的离散数对问题9

2.2.4 基于椭圆曲线的DH密钥交换（ECDH）10

2.3 AES加密算法11

第三章 需求分析15

3.1 可行性分析15

3.1.1 技术可行性分析15

3.1.2 经济可行性分析15

3.1.3 操作可行性分析16

3.2 农业物联网安全体系及需求16

第四章 基于ECC、AES的轻量级认证加密算法17

4.1 ECC算法的性能瓶颈分析17

4.2 改进的ECC算法17

4.2.1 窗口NAF算法17

4.2.2 服务器端设计与实现17

4.2.3 数字签名的实现17

4.3 数据加密解密算法详细设计17

4.4 算法耗时分析17

4.4.1 密钥协商耗时分析17

4.4.2 加密解密耗时分析17

4.5 算法安全性分析17

第五章 系统测试17

5.1 测试环境17

5.1.1 硬件平台17

5.1.2 软件平台17

5.2 性能测试18

第六章 结论18

谢辞18

参考文献18

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，MIT Auto-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，出现了很多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，从下往上分别为：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，该算法密钥混沌化、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：

1

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密钥泄露的风险，一旦攻击者通过非法手段获取了密钥，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，提高密钥协商和加密解密效率，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。

加密：将数据按照一定的规则进行变换的过程

解密：将加密后的数据，按照规则转换成原数据的过程

明文：加密之前的数据，能够被轻易读取

密文：加密之后的数据，隐藏原文本的信息

密钥：控制加密和解密过程的参数

2

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，使用一致的密钥来进行加密和解密。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：

3

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密钥加密。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密钥，保障算法的安全性的前提是保障密钥的安全性，双方都不能将密钥泄露出去，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密钥的情况，在密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，不存在密钥泄露的问题。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。

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，具有更小的密钥长度。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

4

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。 $a, b \in \mathbb{F}_p$ 用于确定具体的椭圆曲线，且需要满足公式 2-2:

5

式 2-2

满足上述要求的椭圆曲线 $E_p(a, b)$ 中，取点 G ，和整数 k 则 $K = kG$ ， K 也是椭圆曲线 $E_p(a, b)$ 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

6

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

椭圆曲线上的加法

设椭圆曲线上有 A 和 B 两点，作过这两点的直线与椭圆曲线相交于 C 点，然后关于 X 轴对称得到 D 点，则 D 为 A, B 两个点的和，记作 $D = A + B$ 。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。

7

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。

8

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 O 点（零点）。

9

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 ($(A+B)+C=A+(B+C)$)。

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 $O(\log k)$ 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密钥交换 (ECDH)

ECDH全称是椭圆曲线迪菲-赫尔曼密钥交换 (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

A选定一条椭圆曲线E，并取椭圆曲线上一点作为基点G。

A选择一个私有密钥k ($k \in \mathbb{Z}_n$)，并生成公开密钥 $K=kG$ 。

A将E和点K、G传给B。

B收到信息后，产生一个随机整数r ($r \in \mathbb{Z}_n$, n为G的阶数)。

B计算点 $C_1=M+rK$ 和 $C_2=rG$ 。

B将 C_1 、 C_2 传给A。

A收到信息后，计算 C_1-kC_2 ，结果就应该是点M C_1-kC_2 。

数学原理： $C_1-kC_2=M+rK-krG=M+rkG-krG-M$ 。

至此：A和B就协商出来相同的密钥，后面就可以使用这个密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、 C_1 、 C_2 等，由于椭圆曲线的数学难题，无法计算出A和B的密钥k、r，那么协商出来的密钥也就是安全的。

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，根据密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	128	128	10
AES192	192	128	12
AES256	256	128	14

表2-1 三种AES算法加密轮数

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：

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，例如加密就是把明文字节按照S盒进行映射，如下图所示

10

图2-8 AES字节代换

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：

11

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

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。

12
图2-10 列混合中的相乘
轮密钥加

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。

密钥扩展
密钥扩展是从 初始密钥得到轮密钥的过程。首先将初始密钥放到一个4*4的状态矩阵中，如下图所示

13
图2-11 初始密钥状态矩阵
矩阵的每一列的4个字节组成一个字，4个字一次命名为W[0]、W[1]、W[2]、W[3]，构成一个以字为单位的数组W，例如，初始密钥为“qwertasdfzxcvtgby”，则矩阵中的K0=q，K1=w，K2=e，K3=r，W[0]=qwer，接着对 W 数组扩充 40 个新列，即得到一个共 44 列的密钥扩展数组，密钥扩展过程如图 2-12 所示。

14
图2-12 密钥扩展过程
若i不是4的倍数，那么W[i]=W[i-4]W[i-1]，若i是4的倍数，那么W[i]=W[i-4]T(W[i-1])，其中，T是一个由字循环、字节代换和轮常量异或所组成的函数。

字循环：将1个字中的4个字节循环左移1个字节。即将输入字[b0,b1,b2,b3]变换成[b1,b2,b3,b0]。
字节代换：对字循环的结果使用S盒进行字节代换。
轮常量异或：将前两步的结果同轮常量Rcon[j]进行异或，其中j表示轮数。轮常量Rcon[j]是一个字，Rcon[j]=(RC[i], '00','00','00','00')，RC[i]的值如表 2-2所示。

	i	1	2	3	4	5	6	7	8	9	10
RC[i]		01	02	03	08	10	20	40	80	1B	36

表2-2 轮常量异或中的RC[i]
AES加密解密的流程图如下

15
图2-13 AES加密流程图图2-14 AES解密流程图

第三章 需求分析

3.1 可行性分析

本章主要介绍了该系统设计的需求和可行性分析，系统可行性分析的目的是：了解客户需求，市场未来发展趋势，确定项目是否值得开发；对项目功能、限制条件进行分析，在已有的硬件资源和技术条件下，确定项目是否能够实现。

3.1.1 技术可行性分析

技术上的可行性分析主要分析能否应用现有的技术完成对系统的设计。本设计利用开源的Netty框架实现网络通信，通过设计合理的数据结构来完成认证加密流程，使用ECC进行密钥协商、数字签名，使用AES进行加密解密。系统中应用到的技术已非常成熟，设计中遇到的难题可方便的查找相关资料，因此在技术上的分析是可行的。

3.1.2 经济可行性分析

本设计的核心在于运行于嵌入式设备上的认证和加密算法。其中软件部分的投入主要是软件开发和人力消耗，软件开发所使用的工具均为现有的免费工具，人力消耗可通过利用课余时间开发解决。硬件部分的投入如下表：

主要设备列表				数量	单价/元	合计/元
STM32F				1	7	7
电路板				1	30	30
外围器件				1	10	10
屏蔽双绞线				2	4	8
总计						55

从上表可以看出，单单从硬件成本计算的话，只有55元。因此本设计在经济上是可行的。

3.1.3 操作可行性分析

从操作上来讲，农业物联网的网关可以随机部署在农场的各个地方，随机性比较大，网关上电后，可自行与云服务器进行密钥协商与双向认证，后续的数据都是加密传输。用户可在PC查看当前以及历史的大棚温湿度数据，也可直接通过Web端直接控制大棚内的设备，例如电灯、风机等。简单方便，操作性强。

3.2 农业物联网安全体系及需求

农业物联网系统为农业生产提供高效、自动化和远程的管理服务，减少人工开销、增加产量、降低风险、提高监管水平。但是，多数系统没有深入考虑安全问题，存在安全隐患，一旦出现问题，后果不堪设想，例如：

- 传感器参数篡改，例如氨气浓度参数被篡改，导致错过报警时机
- 设备非法启动、停止，例如风机无故启动、湿帘无故关闭
- 传感器冒充，收到非法的监测数据

此外，考虑到成本、农业物联网系统的节点，设备一般采用计算能力有限、存储容量较小的芯片（比如，STM32），造成节点和设备难以或无法使用复杂的安全方案。因此，本文结合农业物联网设备处理能力有限的特性，提出一种轻量级的双向认证和加密方法。

第四章 基于ECC、AES的轻量级认证加密算法

4.1 ECC算法的性能瓶颈分析

与RSA等其他非对称加密方式相比较，在相同安全性的要求下，ECC算法使用更短的密钥就可以达到RSA相同的效果。但是与传统的AES、DES等对称加密体制比较，ECC算法的时间复杂度要高得多，这也是限制ECC算法发展的重要原因。而在本文研究的农业物联网安全通信中，其大部分设备都是计算资源有限的嵌入式设备，并且指令传输的实时性要求较高，如果直接应用传统的ECC算法来实现农业物联网中的双向认证和数据加密等，将对通信实时性造成较大影响。

根据前文对椭圆曲线算法的原理分析可知，在椭圆曲线中，最耗时的计算就是标量乘计算，即kG的计算，标量乘计算的效率决定了实现椭圆曲线密码体制的效率。

4.2 改进的ECC算法

传统的标量乘计算过程主要是包括点加运算和倍点运算，点加运算就是对不同点的相加运算，倍点运算就是对相同点的相加运算。阅读文献可知，现有的改进ECC标量乘运算方法有两类：

将整数k基于某种形式展开来表示，通过控制展开式中非零元素的个数，从而使得点加和倍点运算次数大幅降低。这种方法主要是对标量k的表示进行变换，将其变换到不同的表示域上进行运算，通过这种方法降低标量乘中的点加和倍点运算的次数，进而有效地减少标量乘的运算量，提高其运算效率。例如双基链表示法[1]、二进制算法[9]等。

以空间换时间，增加算法的空间复杂度来降低时间复杂度，通过牺牲一点的存储空间进行预计算，存储与点G相关的计算结果，在后续的计算中通过查表的方式实现快速地计算kG，以降低点加和倍加运算的次数，提交运算效率。例如滑动窗口法及结合NAF方法的w-NAF窗口法[1]。

4.3 基于改进ECC-AES的混合加密方案设计

对称加密算法具有速度快、强度高、便于实现等特点，尤其适合加密大块数据，但密钥分配与管理比较困难，而非对称加密算法具有密钥分发与管理简单、速度慢等特点，一般用于加密少量数据、如传输密钥、数字签名等。我们将对称加密算法(AES)和非对称加密算法(ECC)混合使用，得到的混合加密体制，即基于AES与ECC的混合密码体制，既可有效地提高效率，又使网络传输更安全

考虑到密钥生成、密钥协商，用户认证，鉴权等操作，需要消耗较多的计算资源和存储资源，我们提出将网关需要进行的上述操作，交由系统云认证服务器完成，以降低网络资源消耗需求的方案。图2描述了用户智能终端在系统云认证服务器辅助下，与指定物联网网关之间，进行双向身份认证和密钥协商的策略。其基本流程如下。

第一步.用户通过浏览器web客户端登录系统云服务器，服务器验证用户身份的合法性。

第二步.用户浏览器客户端p，通过公式（3）计算出，EC上的点P(x,y)。然后，生成请求接入GWID指定网关的请求信息Requestu-g={Appid,GWID,P}，将Requestu-g发送给系统认证服务器。

<table><tr><td>（3）</td></tr></table>

第三步.云服务器接收到Requestu-g后，验证用户访问GWID指定网关的权限。如满足，则选择一个数r，通过公式（4）计算出EC点R。使用公式（5）计算出EC节点形式的会话密钥K。

<table><tr><td>（4）</td></tr><tr><td>(5)</td></tr></table>

第四步.云服务器使用服务器与网关会话密钥，加密{Appid,GWID,TimeStamp,K}，作为用户智能终端指定GWID的临时身份认证证书Au。将点R和证书，返回给用户智能终端App；加密{Appid,GWID,TimeStamp,K, random number}作为证书A'，发送给GWID指定网关。

第五步.网关收到上述证书A'后，解码证书，提出信息，使用公式（6）计算出与用户终端APP通信的对称会话密钥k，等待用户接入请求。

<table><tr><td>（6）</td></tr></table>

第六步.用户端接收到云服务器返回的点R和证书A后，使用公式（7），计算出EC节点形式的会话密钥K。在通过公式（6），计算出会话密钥k。

<table><tr><td>（7）</td></tr></table>

第七步.用户端，使用计算出的密钥k和AES128算法，加密证书A，发送给GWID指定网关。

第八步.网关收到用户端P的接入请求后，使用密钥k和AES128算法，解密运算得到证书A，与服务器接收到的证书A'中的信息进行比较。一致则身份验证成功。双方使用密钥k进行后续通信工作。

流程图如下

4.4 算法分析

4.4.1 安全性分析

1. 防窃听分析

通信过程中，服务器与网关之间以及服务器与客户端之间的通信信道，是安全的加密信道。因此，窃听者无法窃听获取，信息的真实内容。客户端与网关之间建立通信信道时，监听者可以获取公钥Kc-g，但无法得到双方的私钥k，即使获取密文C，也无法获取真实信息，因此协议具有防窃听能力。

防假冒分析。

系统中通信信息使用存有椭圆曲线 $E_p(a,b)$ 、选定的基点G和私钥t，并且M中的双方的身份ID，窃听正无法伪造加密的信息，因此在本系统中，具有防假冒能力。

防重传分析。

重传攻击是窃听者在非法获取到网络中的通讯信息后，通过重发先前信息以非法获取信任的攻击手段。本系统消息中添加了时间戳、有效期和顺序号等信息，使得协议具有防有防重传的能力。

伪装攻击

攻击者如果想要伪装成合法用户与网关进行通信，必须要伪造出合法的认证信息。通过上述的分析知道，只有服务器指定用户具有服务器认证证书，因此协议可以防止伪装攻击。

中间人攻击

根据攻击者没有办法伪装成其他用户进行通信，并且攻击者无法伪造出合法的认证信息，所以这个协议可以抵挡住中间人攻击。

4.4.2 效率分析

4.4.3 能耗分析

通过算法能耗的理论分析，算法的能耗与算法时间的复杂度的变化之间存在密切的关系，时间复杂度越高，能耗越高。为此，本文针对ECC、改进ECC、RSA 三种加密算法的能耗展开了分析，其能耗分析结果从高到低排列依次是 RSA 算法、ECC 算法、改进 ECC 算法，可见改进 ECC 算法的能耗最低，计算结果最优。

第五章 实验与结论

5.1 实验环境及开发平台

5.1.1 实验环境

5.1.2 开发平台

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.

二、相似详情

序号	标题	文献来源	作者	发表时间
1	基于物联网的温室环境监控系统设计与实现.doc. 淘豆网	本地库		
2	物联网多设备通信中的加密模块设计与实现.pdf	互联网		
3	DH密钥交换 和 ECDH 原理(转) - Fish_Ou - 博客园	互联网		
4	物联网智能吧-百度贴吧--需要充满活力的你 --物联网是新一代...	文献期刊		
5	中移杭研 “全链路”业务安全智能防护系统- 浙江— C114(通信网)	互联网		

6	乌克兰停电事件回顾与分析1 - 道客巴巴	会议		
7	物联网通信协议的安全研究综述-计算机科学.PDF 文档全文预览	互联网		
8	物联网 安全事件频发,人大代表建议完善监管体系保护用户隐私_攻击	会议		
9	...技术架构上看,物联网 可分为 三层:感知层、 传输层 和应用层B的评论	会议		
10	认识物联网平台架构_嵌入式_云上笛暮-CSDN博客	文献期刊		
11	硬核,《信息安全技术物联网感知层网关安全技术要求》标准解读_处理	互联网		
12	...结构图每一个传感器就像是一台微型智能计算机它具有基本的感知...	本地库		
13	一文详解AES最常见的3种方案_AES-128、AES-192和AES-256-...	互联网		
14	计算机 信息 管理技术 在网络 安全中的应用 - 土木工程网	互联网		
15	探究大 数据 时代下计算机 网络信息 安全问题	互联网		
16	...HN P0stcard 下表显示了字符串中一个字符的 加密过程 ...	会议		
17	加密 和 解密 (1):常用 数据加密 和 解密 方法汇总_网络_weixi...CSDN博客	互联网		
18	1.区块链技术和应用.doc_淘豆网	互联网		
19	分组密码_我不是大牛-CSDN博客	文献期刊		
20	加密算法-流密码加密_人工智能_前行的博客-CSDN博客	会议		
21	加解密篇- 非对称加密算法(RSA、DSA、ECC、DH)_网络_u...	互联网		
22	RSA RSA算法基于一个 十分简单的 数论事实:将两个大素数相乘 十分容...	图书		
23	RSA算法 与 ECC算法 _sinat_36747994的博客-CSDN博客	互联网		
24	基于DSP+FPGA的数字电视条件接收系统设计- 道客巴巴	学位论文		
25	椭圆曲线 内点的运算_python,其他_baidu_41913345的博客-CSDN博客	互联网		
26	江苏省2012届一模数学试卷卷南京盐城无锡苏州常州镇江扬州doc下载...	学位论文		
27	椭圆曲线加密浅析_Python_知盛数据集团西安研发中心技术博客-...	会议		
28	公钥私钥以及比特币地址的产生过程_区块链_象牙塔下的渣渣-...	会议		
29	最简单的详解椭圆曲线算法,secp256k1 是如何生成公钥和私钥的_...	文献期刊		
30	【证明:任何直线与 椭圆曲线 $y^2=x^3-x$ 至多有 三个交点】作业帮	会议		
31	OpenSSL密码库算法笔记——第5.4.11章椭圆曲线的多倍点运算——...	会议		
32	移动端网络安全-密钥交换的前世今生(2)_网络_zhoujabod的博客-...	互联网		
33	椭圆曲线密码学ECC - pupilheart - 博客园	互联网		
34	椭圆曲线算法(ECC)学习(一)	互联网		
35	椭圆曲线上的点加运算和点乘运算E为定义在域K上的椭圆曲线。由...	图书		
36	第一章引言第一章引言课题研究背景随着无线局域网WLAN 标准和...	会议		
37	椭圆曲线密码学ECC - pupilheart - 博客园	互联网		
38	椭圆曲线 加密算法 - 假的鱼的博客 - CSDN博客	互联网		
39	[转]SM2算法第二十二篇:DH与ECDH密钥协商原理- Crysaty - 博客园	互联网		
40	加密算法有几种?基于什么原理?-问答-阿里云开发者社区-阿里云	会议		
41	加密算法有几种?基于什么原理?-问答-阿里云开发者社区-阿里云	图书		
42	ECC椭圆曲线加解密原理详解(配图)_网络_Mark的博客-CSDN博客	互联网		
43	椭圆曲线--给自己看_Java_qq_38184895的博客-CSDN博客	图书		
44	HTTPS具体过程,7次握手,以及如何防止中间人攻击的- 简书	互联网		
45	【前端Js】高级 加解密密 标准 AES加密 (javascript代码实...CSDN博客	互联网		
46	AES 加密算法的原理详解_网络_FKNIGHT 的博客-CSDN博客	互联网		
47	AES加密算法及其实现_苏叶-CSDN博客	互联网		
48	...图密码学课程设计18 字节替换字节代换是非线性变换独立地对状态...	图书		
49	AES加密 - 假如蜗牛有梦想 - 博客园	互联网		
50	AES简介及源码实现(C)_运维_IOT2017的博客-CSDN博客	互联网		
51	AB矩阵的逆为什么要把B矩阵的逆写在前面_360问答	互联网		
52	AES加密算法的详细介绍【面试+工作】 - 云+社区- 腾讯云	会议		
53	【实习笔记】AES 加密算法原理简单解析- Alchemyhx - 简书	互联网		
54	AES算法测试用例程序Java实现(密钥长度128比特)_Java_空旷在...	本地库		
55	AES加密 - 假如蜗牛有梦想 - 博客园	互联网		

56	C++实践(三):C++实现加密算法AES_C/C++_goodluckwl的专栏-...	互联网		
57	AES算法测试用例程序Java实现(密钥长度128比特)_Java_空旷在...	本地库		
58	有限域GF(2^8)上字节运算.pptx.ppt	文献期刊		
59	AES算法测试用例程序Java实现(密钥长度128比特)_Java_空旷在...	学位论文		
60	Java实现AES加密算法_Java_mathor的博客-CSDN博客	互联网		
61	浅谈软件项目管理的过程.docx_淘豆网	文献期刊		
62	系统需求分析及可行性分析- 豆丁网	互联网		
63	面向嵌入式系统的基于混沌的快速图像加密算法- 道客巴巴	互联网		
64	基于AES和ECC混合加密系统的算法研究- 豆丁网	互联网		
65	AES加密原理和AOE工程实践- 普惠出行产品技术- 博客园	学位论文		
66	浅议快速安全的椭圆曲线标量乘法研究.pdf	互联网		
67	GF(2~m)上ECC标量乘法的快速实现研究--《解放军信息工程大学...	互联网		
68	机器学习中常常提到的正则化到底是什么意思?- 知乎	本地库		
69	空间换时间,把递归的时间复杂度降低到O(2n)- 草根程序猿 - 博客园	互联网		
70	加密算法有几种?基于什么原理?-问答-阿里云开发者社区-阿里云	图书		
71	android数据加密- 简书	文献期刊		
72	...加密与安全:非对称加密算法ECC和RSA以及对称加密算法AES...	图书		
73	当前网站的安全证书不受信任怎么解决?_360问答	图书		
74	《网络信息安全》期末复习总结- 道客巴巴	互联网		
75	电子支付方式的安全性及如何预防网络诈骗- 道客巴巴	学位论文		
76	...伪装、会话劫持等攻击方式实现了显式密钥认证。协议具有的...	会议		
77	算法能耗复杂度的定义与推导- 计算机学报.pdf	互联网		

三、免责声明

- 报告编号系送检论文检测报告在本系统中的唯一编号。
- 本报告为中国学术不端论文检测系统算法自动生成，仅对您所选择比对资源范围内检验结果负责。

