

论文检测全文报告

基本信息

报告编号: 2020052636443600C6FB679711

文档名称: 物联网网关轻量级认证和加密技术研究

过滤操作: 已过滤参考文献

文档作者: 郑智聪

已过滤自引"郑智聪"的相似影响

提交方式: 上传文档检测

已过滤时间, 仅与2020及之前的文献进行对比

提交时间: 2020年05月26日

正文字符数: 13079

正文字数: 11502

检测范围: 大雅全文库

总体结论

文献相似度: 16.64%

文献原创度: 83.36%

去除参考文献相似度: 17.83%

单篇最大相似度: 1.01%

去除本人已发表论文相似度: 16.64%

单篇最大重复数: 132

重复字符数: 2176

最相似文献题名: 一种基于ECC信息植入的物联网RFID安全模型

过滤前的相似度: 17.83%

过滤前的重复字数: 2332

相似片段分布



典型相似文献

相似图书

序号	题名	作者	出处	相似度
1	范鹏飞文集 物联网专集	范鹏飞	北京: 光明日报出版社, 2017.01	0.83%
2	信息技术教程	薛联凤;章春芳	南京: 东南大学出版社, 2017.09	0.71%
3	全球经济共同性问题的性质和原因 第2卷 认识论	王宪磊	北京: 社会科学文献出版社, 2012.04	0.71%
4	大学计算机基础学习与实验指导 第3版	王移芝	北京: 高等教育出版社, 2013.08	0.71%
5	信息安全辞典	王世伟;惠志斌	上海: 上海辞书出版社, 2013.08	0.69%
6	网络空间安全学科发展	邬江兴;王清贤;邹宏	北京: 电子工业出版社, 2018.04	0.68%
7	甘蔗糖生产自动化和信息化 1	兰红星;易捷	北京: 电子工业出版社, 2013.10	0.68%
8	物联网工程核心技术丛书 ZigBee原理、实践及综合应用	葛广英;葛菁;赵云龙	北京: 清华大学出版社, 2015.08	0.68%
9	故事中国 中国当代短篇小说	郭建玲	北京: 清华大学出版社, 2018.10	0.67%
10	基于FPGA密码技术的设计与应用	杨军;余江;赵征鹏	北京: 电子工业出版社, 2012.05	0.61%
11	信息安全技术	高能;江伟玉;刘丽敏	北京: 中国人民公安大学出版社, 2018.04	0.61%
12	无线传感网络	杨博雄;倪玉华	北京: 人民邮电出版社, 2015.04	0.57%

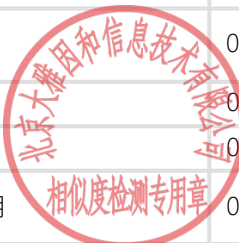
13	计算机网络原理与技术实验教程	史长琼;姜腊林;廖年冬;熊兵	西安: 西安电子科技大学出版社, 2015.01	0.57%
14	计算机网络安全与实验教程	马丽梅;王长广;马彦华;赵冬梅	北京: 清华大学出版社, 2014.10	0.57%
15	建筑设备自动化	李玉云;田国庆;李绍勇;张绍忠;张子慧;黄翔	北京: 机械工业出版社, 2016.01	0.56%
16	新编计算机文化基础	冯建华;刘以安;王家忻;魏敏;张景莉;王映;王新玲	北京: 人民邮电出版社, 2013.09	0.56%
17	物联网智能技术	张文字;李栋	北京: 中国铁道出版社, 2012.04	0.56%
18	金融与电子支付	张宽海	北京: 北京大学出版社, 2008.07	0.55%
19	现代商业银行风险管理	贾墨月;叶新年;陈永健	北京: 首都经济贸易大学出版社, 2008.03	0.55%
20	电子金融学	杨青	上海: 复旦大学出版社, 2004.06	0.55%
21	电子金融学 第2版	杨青	上海: 复旦大学出版社, 2009.02	0.55%
22	网络金融营销学	赵海军;华成;沈金波	北京: 电子工业出版社, 2013.08	0.55%
23	光纤通信原理与应用	方志豪;朱秋萍;方锐	北京: 电子工业出版社, 2019.03	0.54%
24	智慧城市发展手册	杨冰之;郑爱军	北京: 机械工业出版社, 2012.05	0.54%
25	中国物联网产业发展概况	物联网产业技术创新战略联盟	北京: 人民邮电出版社, 2016.04	0.53%
26	大学计算机基础 = UNIVERSITY COMPUTER FOUNDATION	邓海;曾日波;罗翠兰;彭志宏	北京: 人民邮电出版社, 2015.09	0.52%
27	电子商务基础与应用	田艳;李万辰	广州: 华南理工大学出版社, 2016.07	0.52%
28	可视化计算	程向前;陈建明	北京: 清华大学出版社, 2013.01	0.52%
29	全国计算机等级考试三级教程-信息安全技术 2016年版	贾春福;刘昕;刘哲理;崔宝江;王春东参	北京: 高等教育出版社, 2015.12	0.52%
30	管理信息系统	刘腾红	北京: 中国财政经济出版社, 2016.12	0.52%
31	信息安全基础	曹敏;刘艳;杨雅军;王爱菊	北京: 中国水利水电出版社, 2015.06	0.52%
32	计算机安全技术	邵丽萍	北京: 清华大学出版社, 2012.10	0.52%
33	深入Linux内核架构与底层原理	刘京洋;韩方	北京: 电子工业出版社, 2017.11	0.52%
34	网络安全设计	于九红	上海: 华东理工大学出版社, 2012.08	0.52%
35	大学信息技术	张问银;赵慧;李洪杰;吕月娥;胡静瑶;高雷;刘志强	济南: 山东人民出版社, 2016.08	0.52%
36	算法竞赛宝典 语言及算法入门	张新华	北京: 清华大学出版社, 2016.04	0.52%
37	TCPIP协议及其应用	林成浴;陈晨;钟小平;周洪霞	北京: 人民邮电出版社, 2013.07	0.52%
38	计算机网络应用技术基础	李智慧;郭凤芝	北京: 清华大学出版社, 2010.10	0.52%
39	网络系统应用	李海龙;韦素媛;叶霞;李卉	北京: 国防工业出版社, 2012.01	0.52%
40	网络工程师考试辅导 2009版	李磊	北京: 清华大学出版社, 2009.09	0.52%
41	Python编程入门与案例详解	曾刚	北京: 清华大学出版社, 2018.06	0.52%
42	全国计算机等级考试三级教程 信息安全技术 2018年版	教育部考试中心;贾春福	北京: 高等教育出版社, 2016.10	0.52%
43	全国计算机等级考试三级教程: 信息安全技术 2015年版	贾春福;刘昕;刘哲理;崔宝江;王春东参	北京: 高等教育出版社, 2014.11	0.52%
44	新体系经济管理系列教材 电子商务概论	蒲忠;杨力;黄鹂	北京: 清华大学出版社, 2013.07	0.52%
45	品悟管理	上官建新	北京: 石油工业出版社, 2013.06	0.5%
46	物联网导论	张凯;张雯婷	北京: 清华大学出版社, 2012.04	0.5%



47	网络安全基础教程	张仕斌;陈麟;方睿	北京: 人民邮电出版社, 2009.11	0.49%
48	物联网100问	国脉物联网技术研究中心	北京: 北京邮电大学出版社, 2010.09	0.48%
49	物流管理概论	曹会勇;钟强;刘志高;刘秀;闵媛媛;郭丹参	南京: 南京大学出版社, 2016.07	0.47%
50	在线分析仪器	于洋	北京: 清华大学出版社, 2015.08	0.47%

相似期刊

序号	题名	作者	出处	相似度
1	一种基于ECC信息植入的物联网RFID安全模型	金鑫;疏国会	鸡西大学学报, 2016, 第4期	1.01%
2	物联网服务发现初探:传统SOA的可行性和局限性	魏强;金芝;李戈;李力行	计算机科学与探索, 2013, 第2期	0.87%
3	基于伪随机数生成器的标量乘改进算法	李辉;刘中华;易军凯	计算机系统应用, 2015, 第1期	0.67%
4	椭圆曲线密码体制的分析和展望	商艳红;侯金凤	唐山师范学院学报, 2012, 第5期	0.64%
5	基于船联网的无线感知RFID应用技术体系及标准研究	范晓锋;郭英;何敦明	中国水运(下半月), 2018, 第8期	0.62%
6	基于WEB网络安全和统一身份认证中的数据加密技术	符浩;陈灵科;郭鑫	软件导刊, 2011, 第3期	0.61%
7	世界是联的		微电脑世界, 2010, 第6期	0.61%
8	基于RSA数字信封技术的Android数据安全机制	肖萍;李茜	信息网络安全, 2013, 第3期	0.61%
9	基于QR码的高校招聘会监测管理系统研究与设计	蒋黎妮;周燕	电脑知识与技术, 2015, 第31期	0.57%
10	物联网中的RFID技术在电子商务中的应用研究	韩景灵	农业网络信息, 2013, 第12期	0.56%
11	基于AES算法的文件加密	张文锦;周荣;高燕;汪金虎	软件导刊, 2017, 第6期	0.54%
12	物联网知识讲座(一)	张小平	物联网技术, 2011, 第3期	0.54%
13	使用RSA技术实现数字签名	吴迪;刘姝	黑龙江科技信息, 2012, 第24期	0.52%
14	网络交易风险及安全策略分析		电脑知识与技术, 2011, 第9期	0.52%
15	关于技术本质与信息科技教学的一些思考	张汶	上海课程教学研究, 2015, 第4期	0.52%
16	基于NFC的移动支付令牌研究	王越;曹竞超;杨复淮;金天	信息网络安全, 2013, 第11期	0.5%
17	物联网的“前世今生”(一)	梁睿	起重运输机械, 2018, 第8期	0.48%
18	专栏		起重运输机械, 2018, 第8期	0.48%
19	物联网	李晖	数据通信, 2010, 第2期	0.47%
20	物联网发展分析	刘丹;张丽	职业, 2012, 第15期	0.47%
21	基于JAVA的C语言上机考试系统的设计	刘申菊;田丹	黑龙江科技信息, 2016, 第17期	0.45%
22	大数据下高校档案信息系统的安全认证设计	俞豪杰;高翔	自动化技术与应用, 2019, 第11期	0.45%
23	加密算法安全强度及发展趋势分析	孙权	软件产业与工程, 2016, 第3期	0.44%
24	世界因女科学家而美	陈冰	新民周刊, 2016, 第2期	0.44%
25	生命沿着量子空间悠然前行——记优秀青年女科学家彭新华	沈春蕾	发明与创新, 2016, 第7期	0.44%
26	AES算法研究	曹晓丽;王爱强	洛阳师范学院学报, 2011, 第8期	0.43%
27	基于51核的AES算法高速硬件设计与实现	曾小波;易志中;焦歆	电子科技, 2016, 第1期	0.43%
28	一种结合优化后AES与RSA算法的二维码加密算法	刘海峰;刘洋;梁星亮	陕西科技大学学报, 2019, 第6期	0.39%



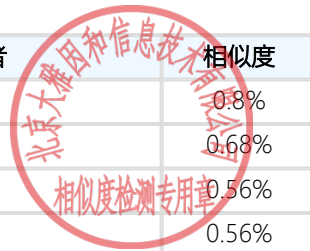
29	GF(2~n)域上的一种II型优化正规基乘法器及其FPGA实现	方冰;樊海宁;戴一奇	电子学报, 2002, 第C1期	0.37%
30	混合密码认证模型的研究	王汝传;王绍棣;孙知信;傅静	计算机学报, 2002, 第11期	0.33%
31	基于椭圆曲线的充值卡加密	孙传亮;周海港	信息技术, 2012, 第10期	0.29%
32	M估计的稳健平面标靶中心定位算法	吕亚磊;李永强;杨清科;李鹏鹏	科学技术与工程, 2019, 第3期	0.29%
33	农业物联网数字图像传输—小波变换信号滤波处理研究	易大国;曾辉;卓辉;黄彪;方逵	农业网络信息, 2015, 第11期	0.28%
34	会计电算化系统信息安全集成解决方案	刘鹏	计算机技术与发展, 2017, 第8期	0.27%
35	AES算法优化及其在ARM上的实现	张月华;张新贺;刘鸿雁	计算机应用, 2011, 第6期	0.27%
36	基于NAF的椭圆曲线集成加密方案存储空间压缩及其点压缩算法的优化	邓从政	凯里学院学报, 2015, 第3期	0.25%
37	AES算法的硬件实现分析与设计	郭建军;刘昌明;石颖;卢霞;张健	计算机安全, 2012, 第7期	0.24%
38	基于受控Hadamard门的量子神经网络模型及算法	李盼池;周红岩	计算机研究与发展, 2015, 第1期	0.23%
39	基于改进的AES算法的EPON安全方案研究	殷爱茵;王胜凯	华东交通大学学报, 2013, 第4期	0.22%
40	AES算法的实现	Fireworm	黑客防线, 2008, 第10期	0.21%
41	实验室管理中云计算技术的应用研究	王萍芳	网络安全技术与应用, 2017, 第6期	0.21%
42	福州程控数字电话交换机开局测试若干问题分析	顾重威	电信快报, 1984, 第3期	0.2%
43	抗能量分析攻击的门限窗口NAF标量乘算法	谷建光	计算机工程, 2019, 第8期	0.2%
44	基于AES加密算法的二维码防伪系统	王对;韩盛	电脑知识与技术, 2019, 第11期	0.2%
45	基于SM2与零知识的射频识别双向认证协议	李子臣;刘博雅;王培东;杨亚涛	计算机工程, 2017, 第6期	0.19%
46	远程用户基于ECDLP的快速认证密钥协商协议	王磊;李中雷;姚继明;郑宝玉	信号处理, 2017, 第9期	0.18%
47	ECDSA可公开验证广义签密	韩益亮;杨晓元	计算机学报, 2006, 第11期	0.17%
48	一种基于椭圆曲线的多方密钥交换协议	谢环;左黎明;汤鹏志	信阳师范学院学报(自然科学版), 2011, 第4期	0.16%
49	具有前向安全特性的盲签名方案	刘亚丽;刘玉龙;唐蕾	徐州师范大学学报(自然科学版), 2007, 第2期	0.15%
50	基于混沌神经网络公钥算法的RFID协议	林传超;魏腾雄;李国刚	通信技术, 2012, 第6期	0.15%

相似报纸

序号	题名	作者	出处	相似度
1	如何建立基于物联网技术的食品安全监控系统		现代物流报, 2011.12.16	0.56%
2	在量子的奥秘中寻找科学之美		中国教育报, 2016.01.09	0.44%
3	彭新华: 生命沿着量子空间悠然前行	沈春蕾	中国科学报, 2016.01.11	0.44%

相似网络文档

序号	题名	作者	相似度
1	未知标题		0.8%
2	未知标题		0.68%
3	未知标题		0.56%
4	未知标题		0.56%



5	未知标题		0.56%
6	未知标题		0.56%
7	未知标题		0.56%
8	未知标题		0.56%
9	未知标题		0.56%
10	网络金融概论		0.55%
11	信息与网络安全		0.52%
12	未知标题		0.52%
13	未知标题		0.52%
14	未知标题		0.52%
15	未知标题		0.52%
16	未知标题		0.52%
17	未知标题		0.47%
18	未知标题		0.47%
19	未知标题		0.47%
20	电子商务		0.47%
21	未知标题		0.47%
22	物联网的发展和应用分析		0.47%
23	未知标题		0.47%
24	未知标题		0.44%
25	未知标题		0.43%
26	未知标题		0.42%
27	基于椭圆曲线密码体制的移动电子商务认证和支付研究	张蓉	0.41%
28	快速安全的椭圆曲线标量乘法研究	许家芹	0.36%
29	IKE协议的研究及在cdma2000分组数据业务中的应用	杨光	0.34%
30	嵌入式GPRS数据业务安全研究	杜耀宗	0.34%
31	基于可重构硬件的公钥密码算法实现研究	文明	0.31%
32	椭圆曲线密码体制及其在无线网络安全中的应用研究	朱春	0.31%
33	中小企业异构数据库集成的研究与实现	栗华军	0.28%
34	基于EC与物流的企业信息管理系统设计与研究	山巍	0.25%
35	椭圆曲线密码系统在E-MAIL中的应用	李大亮	0.24%
36	椭圆曲线密码体制的研究与应用	张静	0.21%
37	指定多接收者签名的研究及实现	李梅	0.2%
38	基于本体的异构数据源的集成研究	谭狄溪	0.19%
39	我国民事公益诉讼制度研究	张倩	0.18%
40	对两套对外汉语口语教材练习的考察与研究	姜媛媛	0.18%
41	JAVA手机神射手游戏的设计与实现		0.18%
42	基于椭圆曲线的数字签密研究	周萍萍	0.18%
43	未知标题		0.17%
44	服务网络管理及QoS监控系统的设计与实现	张晓慧	0.17%
45	基于ECC的一次性口令身份认证方案设计与实现	陈恩	0.17%
46	椭圆曲线密码体制中标量乘法的研究	邓红兰	0.17%
47	P2P系统中访问控制技术的研究及其在CSCD中的应用	张志刚	0.16%
48	基于混沌随机数发生器的AES一次一密系统及其FPGA实现	胡涛	0.16%
49	汉语切分标注和句法分析一体化模型研究	江丰	0.15%



全文对比

学士学位论文

物联网网关轻量级认证和加密技术研究

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

指导教师 郭本振

二〇二〇年六月一日

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

学位论文原创性声明

本人所提交的学位论文《物联网网关轻量级认证和加密技术研究》，是在导师的指导下，独立进行研究工作所取得的原创性成果。除文中已经注明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中标明。

本声明的法律后果由本人承担。

论文作者（签名）： 指导教师确认（签名）：

年 月 日 年 月 日

学位论文版权使用授权书

本学位论文作者完全了解河北北方学院有权保留并向国家有关部门或机构送交学位论文的复印件和磁盘，允许论文被查阅和借阅。本人授权河北北方学院可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或其它复制手段保存、汇编学位论文。

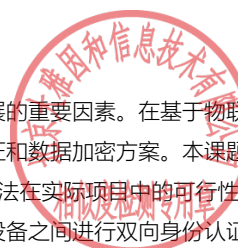
保密的学位论文在_____年解密后适用本授权书。

论文作者（签名）： 指导教师（签名）：

年 月 日 年 月 日

摘 要

随着信息技术的快速发展，物联网越来越广泛地应用在人们的生活中，而物联网的安全问题成为了阻碍其发展的重要因素。在基于物联网技术设计的温室环境监控系统中，需要实现云服务器与物联网节点设备（如传感器、控制器等）之间的双向身份认证和数据加密方案。本课题研究了基于椭圆曲线ECC的数字签名(ECDSA)和密钥协商(ECDH)算法，配合AES-128算法加密传输数据，验证了上述算法在实际项目中的可行性，能够保证物联网系统的安全。通过实际调试和实验证明该方案可在资源较低的情况下，满足云服务器与物联网网关设备之间进行双向身份认证的设



计需求，对本方案所实现的功能进行了全面的测试，系统运行稳定，操作简单。

关键词：物联网安全；双向认证；密钥协商；椭圆曲线；安全策略

ABSTRACT

With the continuous development of the Internet of Things technology, the Internet of Things is becoming more and more common in people's lives. At the same time, its security issues have become particularly important. In a greenhouse environment monitoring system designed based on the Internet of Things technology, it is necessary to implement a two-way identity authentication and data encryption scheme between the cloud server and the Internet of Things node devices (such as sensors, controllers, etc.). This topic studies the digital signature (ECDSA) and secret key negotiation (ECDH) algorithms based on elliptic curve ECC, and uses the AES-128 algorithm to encrypt the transmission data. It verifies the feasibility of the above algorithm in practical projects and can guarantee the Internet of Things system Safety. The actual debugging and experiment prove that the solution can meet the design requirements of two-way identity authentication between the cloud server and the Internet of Things gateway device under the condition of low resources. The functions implemented by the solution have been comprehensively tested, and the system is stable ,easy to use.

Key Words: IoT security; Two-way authentication; Key agreement; Elliptic curve; Security strategy

目 录

摘要.....	1
目录.....	3
第1章引言.....	1
1.1研究背景.....	1
1.2国内外研究现状.....	1
1.2.1国外研究现状.....	1
1.2.2国内研究现状.....	2
1.3主要研究内容.....	2
1.4研究意义.....	3
第2章相关理论和技术.....	4
2.1对称和非对称加密.....	4
2.1.1对称加密.....	4
2.1.2非对称加密.....	5
2.2数字签名技术.....	6
2.3椭圆曲线ECC.....	7
2.3.1概述.....	7
2.3.2ECC上的运算.....	7
2.3.3ECC上的离散数对问题.....	9
2.3.4基于椭圆曲线的DH密钥交换（ECDH）.....	9



2.4AES加密算法.....	10
第3章需求分析.....	14
3.1可行性分析.....	14
3.1.1技术可行性分析.....	14
3.1.2经济可行性分析.....	14
3.1.3操作可行性分析.....	14
3.2农业物联网安全体系及需求.....	14
第4章基于ECC、AES的轻量级认证加密算法.....	15
4.1ECC算法的性能瓶颈分析.....	15
4.2ECC算法的改进.....	16
4.3基于改进ECC-AES的混合加密方案设计.....	16
4.3.1网关认证与密钥协商.....	16
4.3.2数字签名与数据加密.....	18
4.3.3密钥更新.....	20
4.4算法安全性分析.....	20
第5章系统测试.....	22
5.1测试环境.....	22
5.2系统功能测试.....	22
5.2.1密钥协商测试.....	23
5.2.2数字签名和加密解密测试.....	24
5.2.3心跳管理测试.....	25
5.2.4密钥更新测试.....	26
5.3系统性能测试.....	27
5.3.1并发压力测试.....	27
5.3.2安全性测试.....	28
第六章结论.....	30
谢辞.....	31
参考文献.....	32
附录.....	33
引言	



本章主要叙述了物联网系统安全问题的研究背景，国内外研究现状，主要研究内容及意义。

1.1 研究背景

物联网（IoT, Internet of Things）是现代科技潮流当中最炙手可热的技术之一，被称为是继计算机和互联网之后的第三次信息技术革命[17]。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，从上往下分别为：应用层、传输层、

感知层。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。虽然他们的方案满足了降低计算复杂度的需求，但是第三方仍然需要用密码来保存用户信息，在表丢失或被窃取的情况下不能保证信息安全[18]。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来构建网络安全基础设施的实际场景，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ECC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。本课题主要研究内容有以下几点：

物联网网关与服务器之间密钥协商，双方在不暴露私钥的情况下计算出相同的加密密钥。

数据加密，通信双方认证通过后，发送的数据都是通过加密的密文。

数字签名与验签，通信双方发送数据时进行数字签名，接收数据时进行验签，确保消息没有被修改。



密钥管理，协商出的加密密钥可以人为进行更新，而不是一成不变。

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 1-1 感知层结构图

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的效率，这对于物联网安全的发展有着深远的意义。

相关理论和技术

本章介绍了课题研究用到的信息加密相关理论，详细描述了数字签名、椭圆曲线、AES加密算法的原理及相关步骤。

2.1 对称和非对称加密

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

图 2-1 数据加密解密过程

2.1.1 对称加密

对称加密使用相同的密钥对数据进行加密和解密，特点是加密解密的速度非常快，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 对称加密模型

要想保证对称加密算法保障的安全性，必须考虑如何保证密钥的安全，通信的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，所以密钥在网络中传送是不可避免的，而且很容易在密钥传送过程中被拦截并篡改。

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，分别为公钥和私钥，公钥和私钥总是成对出现，只有持有相应的私钥才能对公钥加密的数据进行解密。其中公钥可以发布到网络上，任何人都可以获得公钥，不存在密钥泄露的问题。

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[12]。

ECC算法



ECC算法是在1985年由Neal Koblitz和Victor Miller分别独立提出的[13]。

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标量乘运算，然后利用离散对数难题，将标量乘运算的结果作为公钥。本文将在2.3小节详细介绍ECC算法。

2.2 数字签名技术

在信息安全领域，数字签名是公钥加密体制的重要应用，就像在实际世界上用手写的签名和印章一样，通过在原始数据上附加一些签名数据，或是对原始数据进行编码作为数字签名。使用数字签名可以确保数据在网络中传输的过程中被伪造或修改。

数字签名技术的原理是发送方发送数据时，使用HASH函数计算信息摘要e，然后用发送的私钥对e进行加密得到签名，接收方对签名进行解密之后使用相同的HASH函数重新计算信息摘要，然后与解密出的摘要对比，如果不匹配就说明信息被篡改过。因此数字签名能够验证信息的完整性。

图 2-3 数字签名流程

常见的数字签名算法有RSA、DSA等[14]，本文研究的基于椭圆曲线的数字签名算法是在DSA的基础上，利用椭圆曲线的离散对数难题，提高了安全性和计算效率。

2.3 椭圆曲线ECC

2.3.1 概述

本文研究的椭圆曲线是指满足式2-1的方程

式 (2-1)

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 ∈ E_p 用于确定具体的椭圆曲线，且需要满足公式2-2:

式 (2-2)

图 2-4 椭圆曲线 $y^2 = x^3 - x + 1$

2.3.2 ECC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[15]。

ECC上的加法

在椭圆曲线上取两点A和B做直线AB，AB过点C与椭圆曲线相交，关于X轴做C的对称点D，则D就是A、B两点的和。

图 2-5 椭圆曲线加法

在一种特殊情况下A、B点重合时，过AB点做切线，与椭圆曲线相交于R点，关于X轴做R的对称点R'，则R'就是A、B两点的和。

图 2-6 A=B时椭圆曲线加法

另一种特殊情况下点A、B所在的直线刚好平行于Y轴时，根据椭圆曲线关于X轴对称的性质，将永远不会有与曲线的第三个交点。定义一个无穷远的特殊点，称为0点（零点），那么直线AB相交椭圆曲线与0点，记作A+B=0。

图 2-7 AB垂直于X轴时椭圆曲线加法

ECC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[11]，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，这个算法的时间复杂度是 $O(\log k)$ ，相比于直接进行倍点运算降低了很多，对于增加ECC算法的效率有十分重要的影响。

2.3.3 ECC上的离散数对问题

当给定基点G时，可以很容易的根据ECC乘法运算规则计算出 xG ，但是如果已知 xG ，要求 x 却是几乎不可能的事情，这就是椭圆曲线密码体制中所利用的“椭圆曲线上的离散对数问题”。

2.3.4 基于椭圆曲线的DH密钥交换 (ECDH)

基于椭圆曲线的DH密钥交换 (ECDH) 是利用椭圆曲线的离散数对问题，能够实现在不安全的信道里面，使通信的双方协商出一个共同的对称加密密钥，

ECDH的流程如下

A选定一条椭圆曲线E基点G。

A选择一个随机数 k 作为私钥，计算公钥 $K=kG$ 。

A将E和点K、G发送给B。

B选择一个随机整数 r ($r < n$) 。

B计算点 $R=rG$ ， $key = rK = rkG$ (key就是交换出的密钥)

B将R传给A

A收到信息后，计算 $key = kR = krG$

数学原理: $key = rK = rkG = kR = krG$

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、R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key也就是安全的。

图 2-8 ECDH密钥交换

2.4 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]。根据密钥的长度不同可以分为AES128、AES192、AES256三种，本文使用的是AES128，每一种的加密轮数如下表

表 2-1 三种AES算法加密轮数

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

AES算法的特点就是比较轻量级，有较高的计算效率，在硬件设备时实施简单，并且有的芯片有专门的AES硬件加速。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

在AES算法中，设计了两个二维矩阵，分别称为S盒和逆S盒，在进行字节代换操作时，通过查表的方式把明文字节按照矩阵进行转换，如下图所示



图 2-9 AES字节代换

行移位变换和行移位逆变换

行移位变换就是循环向左进行移位。在AES128中，状态矩阵向左移的字节数是依据行数递增的，如下图所示：

图2-10 AES行移位

列混合与列混合逆运算

列变换就是通过式2-3进行矩阵相乘，等号右边分别为行移位后的状态矩阵和一个常矩阵，得到的结果是矩阵中每一个元素都是该元素原所在列所有元素的加权和。

轮密钥加

轮密钥是将初始密钥通过轮密钥产生算法运算出来的，轮密钥加就是将状态矩阵中的数据中的每一位与轮密钥进行异或。

密钥扩展

密钥扩展是轮密钥加中提到的轮密钥产生算法。首先用一个4*4的状态矩阵来盛放初始密钥，如下图所示

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个字依次命名为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“qwerasdfzxcvtgby”，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[16]，密钥扩展过程如图 2-13 所示。

图2-12 密钥扩展过程

AES加密解密的流程图如下

图2-13 AES加密流程图 图2-14 AES解密流程图

需求分析

本章首先从技术、经济、操作三个方面分析了系统方案的可行性，然后从农业物联网的特性出发，明确了系统的设计需求和任务。

3.1 可行性分析

3.1.1 技术可行性分析

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。系统中涉及到的技术目前已经比较成熟，借助大学四年所学到的知识，以及上网查阅官方文档，请教经验丰富的老师等等方法对未知的难点进行攻克，因此在技术方面是可行的。

3.1.2 经济可行性分析

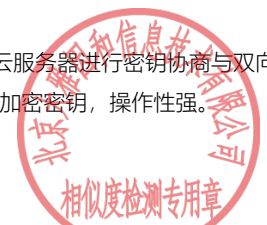
本设计的核心在于认证和加密算法。软件方面的投入主要在于研发、调研、后期维护、域名以及云服务器方面，云服务器方面可以使用腾讯云的学生服务器，内存大小够用并且费用较低。因此本设计在经济上是可行的。

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查看当前在线的网关列表，也可直接通过Web端直接刷新对应网关的加密密钥，操作性强。

3.2 农业物联网安全体系及需求

传统农业有着生产效率低下、人工成本高、产量较低、无法远程管理和自动化的问题，农业物联网的出现则很好的解决了这个问题。但是



，目前大多数的农业物联网系统都没有在物联网的安全问题方面深入考虑，存在着安全隐患，容易出现造成严重的后果。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，遭受DDOS攻击。

本文提出的轻量级的双向认证和加密方案中实现的主要功能如下：

物联网网关与服务器之间密钥协商

物联网网关上电之后，会主动向服务器发送网关认证请求，双方使用ECDH算法，协商出网关与服务器之间的数据传输密钥。

网关与服务器之间加密通信

网关与服务器之间的通信是全双工通信，网关向服务器上数据时，使用

之前协商出来的加密密钥进行AES128加密。网关收到服务器数据时，进行AES128解密。

连接管理

服务器上维护着一个网关的连接列表，可以进行批量的数据推送，网关流

分析与监控等操作。

心跳管理

网关和服务器都要监听彼此之间的通信信道，当信道在一段时间内没有数据

读写时，向对方发送心跳。服务器如果长时间没有接收到对方的心跳应答，会将对应的网关标记为下线，后续可以生成网关异常告警，自动生成工单并指派工程师维修等。而网关会标记服务器崩溃，并开启定时任务进行自动重连。

密钥刷新

用户可以在web页面上点击按钮，刷新指定网关的加密密钥。

基于ECC、AES的轻量级认证加密算法

本章首先分析了ECC算法的性能瓶颈与改进方法，在此基础上介绍了本方案实现密钥协商、数字签名、数据加密、密钥管理的细节，并对本方案的安全性进行了分析。

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算法的密钥更短。但是与AES、DES等对称加密算法比较，ECC算法的时间复杂度更高，大大限制ECC算法在资源较低的处理器中的实施。而在本文研究的农业物联网安全通信中，出于成本考虑，物联网网关、节点、传感器等计算资源都是十分有限，如果直接应用ECC算法，将对系统的主要功能和实时性造成较大影响。

根据前面对椭圆曲线算法原理的分析可知，在计算过程中耗时最长的是标量乘计算，要想提高椭圆曲线算法的运算效率，瓶颈在于标量乘运算的效率。

4.2 ECC算法的改进

传统的标量乘计算过程主要是包括点加运算和倍点运算。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[1]。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[10]。例如双基链表示法[1]、二进制算法[9]等。



以空间换时间，通过存储前面计算的结果来进行预计算。具体实现方式是存储与点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

4.3.1 网关认证与密钥协商

为了实现物联网网关和原服务器之间的双向认证和密钥协商，我们需要作出如下约定。

1.所有设备包括云认证服务器CAS，物联网网关之间共享一组公共的参数。其中包括一组EC参数 $E\{a,b,p,G,n,h\}$ ；独立的身份ID和时钟。身份标识ID用于在系统中唯一标识指定设备，其他设备需要通过ID访问指定的设备。设备时钟用于保证消息的新鲜。

2.云服务器和网关约定好了网关登录口令，用来验证密钥的正确性。

其基本流程如下。

第一步.云服务器初始化时，选取一个随机的大素数 p ，通过式（4-1）计算出ECC上的点P作为服务端的公钥，而 p 作为服务端的私钥。

式（4-1）

第二步.网关上电时，选取一个随机的大素数 r ，通过式（4-2）计算EC上的点R作为网关的公钥， r 作为网关的私钥。

式（4-2）

第三步.网关初始化公钥私钥完成后，通过TCP协议连接云服务器，经过TCP三次握手建立连接，之后网关向云服务器发起认证请求，将网关的公钥R和网关ID发送到云服务器。

第四步.云服务器接收到网关的认证请求之后，首先验证网关ID的合法性，之后用一个hash映射保存网关的ID和公钥，用做后面数字签名的验签。云服务器使用自己的私钥和网关的公钥通过公式（4-3）计算出AES加密密钥K。然后将自己的公钥P发送给网关。

式（4-3）

第五步.网关接收到云服务器的公钥之后，使用自己的私钥和云服务器的公钥，通过公式（4-4）计算AES加密密钥K。

式（4-4）

第六步.网关使用密钥K加密登录口令并发送给云服务器，验证密钥的正确性。

第七步.云服务器接收到网关登录口令之后，使用密钥K进行解密，然后与事先约定的登录口令进行对比，如果不一致就关闭连接并删除密钥K，如果一致就把与网关的会话加入连接管理，保存密钥K并向网关发送登陆成功的消息。

第八步.网关接收到登陆成功的消息之后，保存密钥K，后续使用密钥K进行AES加密解密通信。

图4-1 网关与云服务器密钥协商

4.3.2 数字签名与数据加密

由文献[11]中几种数字签名算法的分析比较可以得出结论，与RSA和DSA相比，无论是在安全性、运算速度和存储空间上，ECC算法都有着明显的优势。现代计算机运算速度快，存储空间大，可以很好地应用RSA和DSA算法，但是在本文研究的农业物联网嵌入式设备中，网关的计算资源有限，ECC算法更加轻量级的特点使之成为更理想的选择。

签名和加密的流程如下：

发送方选择一个随机数 k ， k 的范围是 $\{1, \dots, n-1\}$ ， n 为基点G的阶。

发送方计算 $P = kG$ ，G是基点。

发送方通过式（4-5）计算数字 r, x_p 是P的x轴坐标，如果 $r=0$ ，选择另一个 k 重新计算。



式 (4-5)

计算明文摘要 $z = \text{SHA1}(m)$, m 是消息的明文。

通过式 (4-6) 计算 s , 其中 dA 是发送方的私钥, k^{-1} 是 $k \bmod n$ 的乘法逆元。如果 $s=0$, 选择另一个 k 重新计算。

式 (4-6)

使用 AES128 加密算法和协商出的密钥, 对明文 (m) 进行加密, 得出密文 (w)。

将消息的签名 (r, s) 与密文 (w) 发送给接收方

解密和验签的流程如下

接收方在收到密文 (w) 和签名值 (r, s) 之后, 使用 AES128 解密算法和之前协商出的密钥对密文进行解密, 得到明文 (m)。

计算: $sG + H(m)P = (x1, y1)$, $r1 = x1 \bmod p$ 。

验证: $r1 = r \bmod p$ 。

如果等式成立, 说明验签成功, 数据没有被篡改过, 否则签名无效, 丢弃数据

图 4-2 数字签名与验签

4.3.3 密钥更新

在安全的通信系统中, 如果长期使用同一密钥, 泄漏的可能性就会提高, 通信系统的安全性就会下降。为了应对这个问题, 需要系统中增加密钥更新机制。本系统中, 可以通过 web 端登录用户管理中心, 在网关列表选择网关进行密钥更新。密钥更新的流程如下:

用户登录云服务器

用户查询在线网关列表中的网关

用户选择指定的网关, 向云服务器发送更新网关密钥的请求

云服务器验证用户和网关的合法性之后, 向网关发送密钥更新命令

网关接收到密钥更新命令之后, 重新执行密钥协商和网关登录

图 4-3 用户刷新网关密钥

4.4 算法安全性分析

1. 防窃听分析

云服务器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, 因此本方案具有防窃听能力。

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 ,

其中私钥是保存在本地, 不会在网络中传输, 并且使用 STM32 芯片的读保护模式, 使用芯片的全球唯一 id 作为网关 ID, 启动时与代码中的 ID 进行校验, 一旦不同则进行 flash 数据擦除。窃听者无法伪造加密的信息, 因此在本方案具有防假冒能力。

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, 使得本方案具有防重传的能力。



中间人攻击

中间人攻击是攻击者分别于通信双方建立连接，然后窃听或修改通信双方信息的攻击手段。在本系统中，由于存在双向认证和数字签名的机制，攻击者无法伪造出合法的认证信息，所以本放安可以防止中间人攻击。

系统测试

本章首先介绍了测试环境，从实现的功能和系统性能两个方面，设计了测试用例，对系统进行了全面的测试。

测试环境

本文在设计 and 实现物联网网关通信实验仿真过程中主要是通过PC电脑上使用Java程序模拟双向认证及安全通信的过程。整个系统分为云服务器端、Web客户端、网关客户端三个部分，其中，云服务器端和网关客户端使用Java语言为开发语言，版本为Java8，使用开源的Netty作为网络通信的框架，实现Socket服务端的网络数据监听，使用bouncycastle作为Java加密解密库的扩展，实现了本文描述的ECC算法。Web客户端使用JavaScript开发语言和开源的Vue.js前端框架。整个系统运行在PC计算机上，该计算机使用64位windows操作系统（CPU i5-7200U，2.50GHz、内存8GB、磁盘空间128GB）。

5.2 系统功能测试

整个设计方案所要实现的最终功能是能够实现物联网网关和云服务器之间密钥协商和数据加密传输，并通过Web页面进行在线网关和密钥的管理。本系统的综合测试中，首先要对密钥协商和双向认证功能进行测试，协商出密钥之后，再对数据加密解密和数字签名进行测试，最后通过Web端登录后台管理中心，进行密钥更新测试。Web端页面截图如下：

图 5-1 系统登录页

图 5-2 系统首页

5.2.1 密钥协商测试

在PC机上部署服务端，并启动网关客户端，在日志中打印网关与服务端进行密钥协商的过程。经过多次测试，在第一次进行密钥生成和密钥协商时，时间耗时在1400ms左右，后面刷新密钥时，再次生成密钥和进行密钥协商，耗时在40ms左右，速度较快，对主要逻辑影响较小。运行截图如下：

图 5-3 密钥协商过程

测试用例如下：

表 5-1 密钥协商测试用例

用例描述 操作步骤 预期结果 实际结果

网关与云服务器进行密钥协商 1在PC机部署并初始化云服务器 2启动客户端程序 3 重复运行10次 网关与云服务器协商出相同的密钥，云服务器管理网关连接列表。 符合预期

5.2.2 数字签名和加密解密测试

网关与云服务器协商出加密密钥，后续发送和接收数据都会使用AES128算法进行加密解密。同时，在通信过程中，为了保证消息不会被中间人篡改，通信双方都会保存对方的公钥，并且在发送数据时使用通过SHA算法对明文生成摘要，使用自己的私钥对摘要进行SHA1withECDSA数字签名；接收方接收到数据时，先使用对方的公钥验证数字签名，如果验签失败则直接丢弃数据，如果验签成功，说明数据没有被篡改，进行后续处理。运行截图如下：

图 5-4 数字签名和数据加密解密

测试用例如下：

表 5-2 数字签名和数据加密解密用例



用例描述 操作步骤 预期结果 实际结果

网关与云服务器通信时对消息进行加密解密和数字签名验签 1在PC机部署并初始化云服务器 2启动客户端程序 3 重复运行10次 网关向云服务器发送经过AES加密和数字签名过的数据，云服务器AES解密数据和验签。云服务器向网关发送数据。 符合预期

5.2.3 心跳管理测试

网关与云服务器双向认证通过后，会加入心跳连接的机制，通过向对方发送心跳和心跳应答，确认对方是否在线。在云服务器端维护一个计数器，当网关三次心跳都没有应答时，判断网关下线，关闭服务器与网关的TCP连接。在网关的逻辑是，云服务器宕机连接被断开时，会启动一个定时任务，每30秒进行重连。运行截图如下：

图 5-5 心跳管理

测试用例如下：

表 5-3 心跳测试用例

用例描述 操作步骤 预期结果 实际结果

网关与云服务器之间维持心跳连接 1在PC机部署并初始化云服务器 2启动客户端程序 3 重复运行10次 云服务器和网关检测socket读写空闲，空闲时向对方发送心跳，接收到心跳时发送应答 符合预期

网关心跳无应答，云服务器将其标为下线 1在PC机部署并初始化云服务器 2启动客户端程序 3阻塞客户端程序 4 重复运行10次 云服务器发送三次心跳，都没有收到应答之后，将网关标记下线，关闭通信信道 符合预期

云服务器宕机，网关执行重连 1在PC机部署并初始化云服务器 2启动客户端程序 3手动关闭服务端程序 4 重复运行10次 网关检测到TCP连接断开，判断云服务器宕机，执行定时重连 符合预期

5.2.4 密钥更新测试

用户在登录物联网网关轻量级认证加密方案用户管理中心后，点击在线网关模块，列表显示当前在线的网关，用户可点击网关后面的刷新密钥按钮，刷新指定网关的密钥。程序截图如下：

图 5-6 在线网关页面

图 5-7 密钥更新运行截图

测试用例如下：

表 5-4 密钥更新用例

用例描述 操作步骤 预期结果 实际结果

用户刷新指定网关的密钥 1用户登录物联网网关轻量级认证加密方案用户管理中心 2点击在线网关模块 3选择网关，点击密钥刷新按钮 4 重复运行10次 提示密钥刷新成功，查看后台日志，密钥已经被更新 符合预期

5.3 系统性能测试

5.3.1 并发压力测试

现实世界中物联网网关的数量是成千上万的，云服务器需要能够支持大量的物联网网关并发地进行连接和数据发送，这对于云服务器的设计十分具有挑战性。本文设计的云服务器使用NIO的IO模型，单一线程就可以支持多个客户端连接，同时使用多线程技术，异步地执行逻辑。

测试用例如下：

表 5-5 并发测试用例

用例描述 操作步骤 预期结果 实际结果



云服务器并发压力测试 1在PC机部署并初始化云服务器 2 同时启动多个网关客户端进行身份认证和登录 云服务器能够快速响应，并且不会宕机 符合预期

测试结果如下：

表 5-6 并发压力测试结果

客户端并发连接数 服务端认证总时间 实际测试情况

10 154ms 服务器快速响应，没有卡顿现象

50 240ms 服务器快速响应，没有卡顿现象

100 512ms 服务器快速响应，没有卡顿现象

200 941ms 服务器响应较慢，没有卡顿

500 3102ms 服务器响应较慢，没有卡顿

1000 21043ms 服务器响应较慢，卡顿

3000 -- 服务器出现拒绝连接的情况

测试结果：当前是在windows系统中进行测试，测试结果受CPU，内存，端口数量等限制。单机部署的情况下，合适的并发连接数在300左右，如果对性能要求较高，可以通过分布式部署、负载均衡等技术解决。

5.3.2 安全性测试

在云服务器与网关通信的过程中，进行网络抓包，截获通信过程中的数据包并进行分析，测试能否通过数据包中的信息破解出网关的密钥。

运行截图如下：

图 5-8 安全性测试抓包截图

测试用例如下：

表 5-7 安全性测试用例

用例描述 操作步骤 预期结果 实际结果

使用wireshark软件抓包，分析抓取的数据包 1部署云服务器端和网关客户端 2在通信过程中使用wireshark抓包 3分析抓取的数据包，看能否通过数据包破解密钥 从网络数据包中无法破解出密钥 符合预期

结论

本文研究了在农业物联网的环境下，基于椭圆曲线ECC和AES128的物联网网关轻量级认证与加密方案，该方案的原理主要是利用椭圆曲线的密钥协商算法（ECDH）和数字签名算法（ECDSA），使用AES128算法进行对称加密通信。系统实现的技术支持为Java语言、Netty网络通信框架、Spring Boot框架开发实现的。系统中实现了物联网网关与云服务器之间进行密钥协商、非阻塞、IO多路复用的通信模型、数字签名、心跳管理、密钥刷新等功能。可以作为一个高性能、轻量级的物联网认证与加密方案，该算法运行时占用资源较少，适合在嵌入式设备上运行，对具体的业务逻辑影响较小。

论文工作总结：

需求分析与系统设计，阅读相关文献，调查物联网认证和加密系统的基本架构，分析了将椭圆曲线算法落实到实际项目的可行性，最终通过编码实现了利用ECC和AES的轻量级认证和加密方案。

通过设计基于椭圆曲线ECC和AES128的物联网网关轻量级认证与加密方案，学到了一个软件系统从需求分析、数据结构设计、算法设计到最后编码实现等整体的流程，在这其中也遇到了很多的问题，例如如何解决TCP粘包拆包、Netty框架中如何动态加入加密解密的编解码器等，这些



都是在平时课堂上学不到的，编码能力和解决问题的能力有了明显的提高。

(3)目前基于椭圆曲线ECC和AES128的物联网网关轻量级认证与加密方案的代码已按时开发完成，但是系统仍然有优化的空间，例如可以通过添加定时任务的方式，每过一段时间就去刷新密钥，而不需要人在页面上点击；本文中为了统一技术框架和更好的可视化实验，网关客户端的逻辑是用Java语言实现的，在实际的应用中，网关客户端应该使用真正的嵌入式设备；另外可以接入移动客户端，加入节点远程控制、数据监测等功能。

谢辞

行文至此，已经到了论文的最后一步，四年的大学生涯即将结束。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。大学生活中最有价值的一件事就是在大二的时候加入信息技术研究所，在这里遇到了志同道合的老师和同学，学到了很多实际项目中的技术。

首先，感谢我的指导老师郭本振老师和科研室的王志辉老师。两位老师认真的工作态度和科学的引导给了我很大的帮助，没有两位老师的悉心指导，就没有我的这个毕业设计。两位老师在项目设计期间，给出了许多中肯的建议，在论文修改期间，针对论文中的不足之处悉心指导，在此我深表敬意。

其次，还要对大学期间每位任课老师~~和~~同学表达谢意，是你们陪我度过了人生中宝贵的四年，你们的帮助和陪伴使我不断成长和进步，让我度过了充实且快乐的大学时光。

最后感谢各位评审老师，能来参加我的毕业答辩，给我提出珍贵的建议，在此表示深深的感谢。

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.

[11] 李春平. 基于低功耗处理器的数字签名研究与实现[D].北京邮电大学,2015.

[12] 于庆文. 谈密码技术的发展趋势[J]. 网络与信息,2012,26(09):76-77.

[13] 李栋. 无线传感器网络中能量优化与安全方案研究[D].北京邮电大学,2013.

[14] 严佳韵. 基于椭圆曲线的快速数字签名算法[D].西南交通大学,2011.

[15] 刘佳. 基于ECC与嵌入式的智能家居安全协议研究与设计[D].电子科技大学,2017.



[16]田兴宇. 基于STM32的嵌入式加密链路机的设计与实现[D].黑龙江大学,2018.

[17]刘克一. 物联网概念的基本定位[J]. 数字技术与应用,2015(04):221.

[18]刘欣东,徐水帅,陈建华. 基于椭圆曲线密码的智能电网通信认证协议[J]. 计算机应用,2019,39(03):779-783.

附录

@Slf4j

```
public class ServerAuthHandler extends ChannelInboundHandlerAdapter {
```

```
@Override
```

```
public void channelActive(ChannelHandlerContext ctx) {
```

```
log.info("客户端【{}】连接，开始认证",ctx.channel().remoteAddress());
```

```
}
```

```
@Override
```

```
public void channelRead(ChannelHandlerContext ctx, Object message) {
```

```
SocketMsg msg = (SocketMsg) message;
```

```
try {
```

```
switch (msg.getType()){
```

```
case MsgType.AUTH_VALUE:
```

```
String clientPubKey = (String) msg.getContent();
```

```
String gwld = msg.getGatewayId();
```

```
if (StringUtils.isEmpty(clientPubKey) || StringUtils.isEmpty(gwld)){
```

```
log.info("网关公钥或网关ID为空，拒绝处理");
```

```
closeChannel(ctx);
```

```
return;
```

```
}
```

```
long start = System.currentTimeMillis();
```

```
log.info("2.服务端接收到密钥协商请求,客户端公钥为: {}",clientPubKey);
```

```
EcKeys ecKeys = SpringBeanFactory.getBean("EcKeys",EcKeys.class);
```

```
SocketMsg <String> publicKeyStr = new SocketMsg <String> ()
```

```
.setld(1).setType(MsgType.AUTH_BACK_VALUE).setContent(ecKeys.getPubKey());
```

```
String key = EncryptOrDecryptUtil.ecdhKey(ecKeys.getPriKey(),clientPubKey);
```

```
log.info("3. 服务端密钥协商完成，耗时： {}ms，开始验证密钥正确性,加密密钥为:{},System.currentTimeMillis()-start,key);
```



将改密钥加入密钥库

```
Gateway gw = new Gateway()

.setGwId(msg.getGatewayId())

.setGwName("第一套")

.setChannel(ctx.channel())

.setKey(key)

.setPubKey(clientPubKey);

NettySocketHolder.put(msg.getGatewayId(), gw);

ctx.writeAndFlush(publicKeyStr);

break;

case MsgType.AUTH_CHECK_VALUE:

log.info("6.服务端验证密钥正确性");

Gateway gw1 = NettySocketHolder.get(msg.getGatewayId());
```

确认密钥的正确性

```
String login = EncryptOrDecryptUtil.doAES((String) msg.getContent(),gw1.getKey(), Cipher.DECRYPT_MODE);

log.info("7. 服务端解密出登录口令:{}",login);

if (("login").equals(login)){

log.info("网关【{}】验证通过，加入连接列表",msg.getGatewayId());

gw1.setStatus("在线");

NettySocketHolder.put(msg.getGatewayId(),gw1);
```

向客户端发送认证成功消息，这里一定要先发消息再替换handler

```
ctx.writeAndFlush(new SocketMsg < String > ().setType(MsgType.LOGIN_SUCCESS_VALUE));
```

用AES加解密替换掉默认的编解码器

```
ctx.pipeline().replace(ctx.pipeline().get("decoder"),"decoder",new JsonDecoderAES());

ctx.pipeline().replace(ctx.pipeline().get("encoder"),"encoder",new JsonEncoderAES());

ctx.pipeline().addFirst("idle",new IdleStateHandler(5,0, 0, TimeUnit.SECONDS));

}else {

log.info("非法客户端，关闭连接");

closeChannel(ctx);

}
```



```
break;

default:break;

}

}catch (Exception e){

e.printStackTrace();

log.error("客户端认证出错{}",e.getMessage());

closeChannel(ctx);

}

ctx.fireChannelRead(message);

ReferenceCountUtil.release(msg);

}

private void closeChannel(ChannelHandlerContext ctx){

NettySocketHolder.remove(ctx.channel());

ctx.channel().close();

}

}
```

说明：

- 1.文献相似度=送检论文中与检测范围所有文献的相似字数/送检论文正文字符数
- 2.去除参考文献相似度=送检论文中检测范围所有文献（不包括参考文献）的相似字数/送检论文正文字符数
- 3.去除本人已发表论文相似度=送检论文中与检测范围所有文献（不包括自引）的相似字数/送检论文正文字符数
- 4.单篇最大相似度：送检论文与某一文献的相似度高于全部其他文献
- 5.正文字符数:送检论文正文部分的总字符数，包括汉字、非中文字符、标点符号、阿拉伯数字（不计入空格）
- 6.正文字数：送检论文正文部分的总字数，正文不包括摘要、关键词、目录、图片、表格、附录、参考文献等

