

单位代码: 10293 密 级:

南京邮电大学

硕 士 学 位 论 文



论文题目: 物联网轻量级认证和加密技术研究

学 号	<u>1014041101</u>
姓 名	<u>汪洋</u>
导 师	<u>陈春玲</u>
学 科 专 业	<u>计算机软件与理论</u>
研 究 方 向	<u>分布计算与互联网技术</u>
申 请 学 位 类 别	<u>工学硕士</u>
论 文 提 交 日 期	<u>2017 年 2 月</u>

Research of Lightweight Authentication and Encryption Technology in Internet of Things

Thesis Submitted to Nanjing University of Posts and
Telecommunications for the Degree of
Master of Engineering



By

Yang Wang

Supervisor: Prof. Chunling Chen

February 2017

南京邮电大学学位论文原创性声明

本人声明所呈交的学位论文是我个人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得南京邮电大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

本人学位论文及涉及相关资料若有不实，愿意承担一切相关的法律责任。

研究生学号：_____ 研究生签名：_____ 日期：_____

南京邮电大学学位论文使用授权声明

本人授权南京邮电大学可以保留并向国家有关部门或机构送交论文的复印件和电子文档；允许论文被查阅和借阅；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、缩印或扫描等复制手段保存、汇编本学位论文。本文电子文档的内容和纸质论文的内容相一致。论文的公布（包括刊登）授权南京邮电大学研究生院办理。

涉密学位论文在解密后适用本授权书。

研究生签名：_____ 导师签名：_____ 日期：_____

摘要

无线射频识别 (Radio Frequency Identification, RFID) 技术是物联网感知层中的关键性技术, 以其抗污染、穿透识别性强、无屏障阅读、传输速度快等优势被广泛应用于各种领域, 但 RFID 系统环境也面临着窃听、跟踪、仿冒等诸多安全威胁。由于其自身系统环境资源有限, 对带宽、能量等有诸多限制, 现有的安全协议无法适应严苛环境, 因此, 研究适用于 RFID 环境中的轻量级认证和加密技术对物联网以及 RFID 技术的推广应用有着重要意义。

在深入探究了 RFID 系统的基本构成以及所面临的安全威胁后, 基于传统的一次性口令认证 (One Time Password, OTP), 提出了一种新的 RFID 双向认证协议。在认证信息中引入任意数和时间戳, 并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。在对 RFID 环境中的轻量化加密算法的研究中, 研究分析了现有的轻量级密码算法的安全效率。重点关注算法的轻量化水平, 分析对比各种密码算法的底层运算效率。通过分析发现, 椭圆加密算法具有高效的安全性、运行速度快、占用容量小以及低带宽等优势, 但其轻量级水平仍然较低。在深入探究了椭圆密码算法运行过程后发现, 标量乘运算是加解密过程中的关键环节, 其运算效率直接决定着整体密码算法的运行效率。因此以传统双基标量乘算法为基础, 并结合广义双基链思想, 提出了一种基于新双基的标量乘扩展算法。其中利用点群运算中的半点运算替代倍点运算, 同时扩展了基数的系数集合, 进一步降低了运算冗余度。将改进后的 ECC 算法与 RFID 双向认证协议相结合, 在进行模拟实现之前, 利用 BAN 逻辑对提出的 RFID 认证协议进行形式化逻辑证明。而后在 JDK 环境下通过模拟实现来验证结合了改进 ECC 算法的 RFID 双向认证协议的有效性和实用性。

协议的可行性和安全性分析表明, 该基于 ECC 和 OTP 认证的 RFID 双向认证协议满足 RFID 系统环境基本的安全性能要求, 可抵抗跟踪、重放、假冒等多种攻击, 同时实现了标签端与数据库端的双向认证, 提高了 RFID 环境的安全性。而对改进的 ECC 算法的运算复杂度分析可知, 新双基链算法有效提高了椭圆曲线密码算法的运算效率, 其运算效率比改进前的双基链标量乘算法高了近 30%。协议经 BAN 形式化逻辑证明, 达到了预先设置的证明要求, 从而在逻辑上验证了认证协议的正确性。模拟实验结果进一步说明, RFID 双向认证协议可行有效。

关键词: 物联网感知层, 射频识别, 轻量级认证, 一次性认证, 椭圆密码算法, 标量乘

Abstract

RFID is the key technology in the sensing layer of the Internet of Things. It is widely used in various fields because of its anti-pollution, strong recognition, no barrier reading and fast transmission speed. But the RFID system environment also faces eavesdropping, tracking and counterfeiting and many other security threats. Because of its limited resources, there are many restrictions on bandwidth, energy. Existing security protocols cannot adapt to the harsh environment. Therefore, it is of great significance for the development of the Internet of things and the popularization of RFID technology to study the application of lightweight authentication and encryption technology in RFID environment.

After deeply studying the composition and the security threats of RFID system, a new RFID authentication protocol based on the traditional OTP authentication is proposed. Any number and time stamps are introduced in the authentication information, and the sensitive information in the authentication process is encrypted by the ECC algorithm to ensure the confidentiality of the authentication information. In the research of lightweight encryption algorithm in RFID environment, this paper analyzes the security efficiency of the existing lightweight encryption algorithm and the underlying computing efficiency of various cryptographic algorithms. Through the analysis, It is found that the elliptic encryption algorithm has the advantages of high security, fast processing speed, small storage space and low bandwidth requirement, but its lightweight level is still low. After depth study of the elliptic curve cryptography algorithm running process, it is found that the scalar multiplication is the key operation in the process of encryption and decryption. The operation efficiency determines the overall efficiency of the algorithm code. Therefore, based on the traditional double - base scalar multiplication algorithm, and combined with the idea of generalized double-base chain, a new scalar multiplication algorithm based on new double-base is proposed. In this way, the half-point operation of point group is used to replace the double-point operations. And at the same time, expanding the coefficient set of base, which further reduces the computational redundancy. Combining the improved ECC algorithm with the RFID bidirectional authentication protocol, the BAN logic is used to prove the formal logic of the proposed RFID authentication protocol before the simulation is carried out. And then in the JDK environment, verifying the effectiveness and practicability of the RFID two-way authentication protocol based on improved ECC algorithm by simulation.

Depend on the feasibility and security analysis of the protocol, the RFID two-way authentication protocol based on ECC and OTP meets the basic security performance requirements of the RFID environment. That can resist various attacks such as tracking, replay and counterfeiting. At the same time, it realizes the tow-way authentication between the tag and the database, and improves the security of the RFID environment. According to the computational complexity analysis of the improved ECC algorithm, the new double base chain algorithm can effectively improve the efficiency of the elliptic curve cryptography algorithm, which is about 30% higher than that of the original double base chain scalar multiplication algorithm. The formal logic of BAN proves that the protocol meets the requirement of preset. Thus, the correctness of the authentication protocol is verified logically. The simulation results further demonstrate that the RFID tow-way authentication protocol is feasible and effective.

Key words: Internet of Things sensing layer, Radio Frequency Identification, Lightweight authentication, One-time certification, Elliptic cryptography, scalar multiplication

目录

第一章 绪论	1
1.1 研究背景和意义	1
1.1.1 研究背景	1
1.1.2 研究意义	2
1.2 国内外研究现状	3
1.2.1 RFID 环境中轻量级认证技术	3
1.2.2 RFID 环境中轻量级密码算法	6
1.3 研究内容和目标	7
1.3.1 研究内容	7
1.3.2 研究目标	7
1.4 论文的结构组织	8
第二章 RFID 系统与椭圆曲线密码学基础	9
2.1 RFID 系统	9
2.1.1 RFID 系统组成	9
2.1.2 RFID 系统主要工作原理	10
2.2 RFID 系统的安全分析	11
2.2.1 RFID 系统的安全漏洞	11
2.2.2 RFID 系统的安全威胁	11
2.2.3 RFID 系统的安全方案	13
2.3 椭圆曲线密码学相关理论概述	13
2.3.1 群和有限域基础	13
2.3.2 椭圆曲线理论基础	14
2.3.3 椭圆曲线密码体制	16
2.4 本章小结	17
第三章 基于 ECC 和 OTP 认证的 RFID 双向认证协议	18
3.1 OTP 认证机制	18
3.1.1 OTP 认证技术基本原理	18
3.1.2 S/Key 一次性口令认证协议	19
3.1.3 S/Key 认证协议安全性分析	20
3.2 RFID 双向认证协议	21
3.2.1 注册阶段	21
3.2.2 认证阶段	22
3.3 协议性能分析	23
3.3.1 可行性分析	23
3.3.2 安全性分析	24
3.3.3 效能性分析	26
3.4 本章小结	27
第四章 现有密码算法轻量化分析与 ECC 轻量化改进	28
4.1 现有的加密算法轻量化分析	28
4.1.1 对称密码算法	28
4.1.2 非对称密码算法	29
4.1.3 现有的算法性能评估与比较	30
4.2 基于传统双基的椭圆曲线标量乘算法	32
4.2.1 双基链表示	33

4.2.2 基于传统双基链的标量乘算法.....	34
4.2.3 传统双基链标量乘运算量分析.....	36
4.3 基于新双基的椭圆曲线标量乘算法.....	36
4.3.1 广义双基链与半点运算.....	37
4.3.2 扩展的新双基链表示方法及标量乘算法.....	38
4.3.3 改进后 ECC 算法与其他算法性能比较.....	44
4.4 本章小结.....	46
第五章 RFID 双向认证协议正确性证明与实现.....	47
5.1 认证协议正确性证明.....	47
5.1.1 BAN 逻辑.....	47
5.1.2 协议正确性证明.....	49
5.2 协议的仿真系统设计.....	52
5.2.1 协议仿真环境与初始参数设置.....	52
5.2.2 认证系统总体设计.....	52
5.2.3 认证系统的模块设计.....	53
5.3 认证系统测试.....	56
5.3.1 注册模块测试.....	56
5.3.2 数据处理模块测试.....	57
5.3.3 认证模块测试.....	59
5.4 本章小结.....	60
第六章 总结与展望.....	61
6.1 总结.....	61
6.2 展望.....	62
参考文献.....	63
附录 1 攻读硕士学位期间撰写的论文.....	65
附录 2 攻读硕士学位期间参加的科研项目.....	66
致谢.....	67

第一章 绪论

1.1 研究背景和意义

1.1.1 研究背景

随着工业 4.0 概念的提出以及我国“互联网+”行业计划的不断深入，物联网(Internet of Things)作为“互联网+”的重要支撑和载体，其中的射频识别技术、无线传感器网络等物联网技术的研究和发展显得越来越重要。1999 年 MIT Auto-ID 中心的 Ashton 教授在研究射频识别(Radio Frequency Identification, RFID)时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，引用了“物联网”的概念，并对其进行了详细阐述。报告中指出，无所不在的“物联网”通信时代即将来临，这是 IT 技术时代的一次革命，届时，世界上的万事万物都可以通过互联网连接在一起，进行信息交互，体现了物联网时代无处不在的信息感知。这将使得与互联网息息相关的射频识别、传感器网络、嵌入式等技术得到更加广泛而深入的应用。物联网本质上是在现代互联网技术基础上的衍生与发展，是现有网络信息技术的综合式应用与提升。它是一种虚拟网络与现实世界实时交互的新型系统，是通过各种交互式传感采集设备，如传感器、RFID 技术、红外线感应器、全球定位系统等，根据已有的协议规定，将世界上的任何物品通过互联网连接起来，从而实时的进行信息交互和通信控制，以实现连入网络的所有事物的智能化识别、控制、定位、监控和管理的新型网络系统^[1]。物联网借助互联网作为其技术支撑，特点是深度全面的数据信息感知、结合无线网络与互联网技术的可靠信息传输、智能化的海量信息处理。相对应于物联网的三个特点，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^[2]，如图 1.1 所示。其中感知层利用传感器、RFID 设备等实时获取物体信息，并通过蓝牙、红外线、无线传感网络等短距离传输方式传输信息；相对于感知层的短距离传输而言，传输层即通过各种电信网络、无线网络等适合长距离传输的网络将获取的信息及时、安全、准确的传送到数据中心；应用层运用云计算、模糊识别以及数据挖掘等智能技术，对所得的数据进行处理分析，为进一步的智能化应用提供数据基础和指导。由以上可以看出，传输层和应用层可以在我们现有的成熟的技术架构基础上运作实施，如传输层中用于数据传输的计算机网络和无线通信网络，应用层中采用的云计算和大数据技术等，对这两层中的安全保护都可以利用现有的比较成熟的安全协议体系。而感知层中涉及更多的资源受限的软硬件环境，

由于它们结构较为简单，现有的成熟的安全协议无法很好地适应该环境，轻量级认证和加密等安全协议应运而生。

本文即是基于江苏省信息安全应急中心的物联网轻量级认证和加密技术研究课题展开，主要针对的是一种典型的感知层环境——RFID 系统环境展开相关的轻量级认证和加密技术研究。

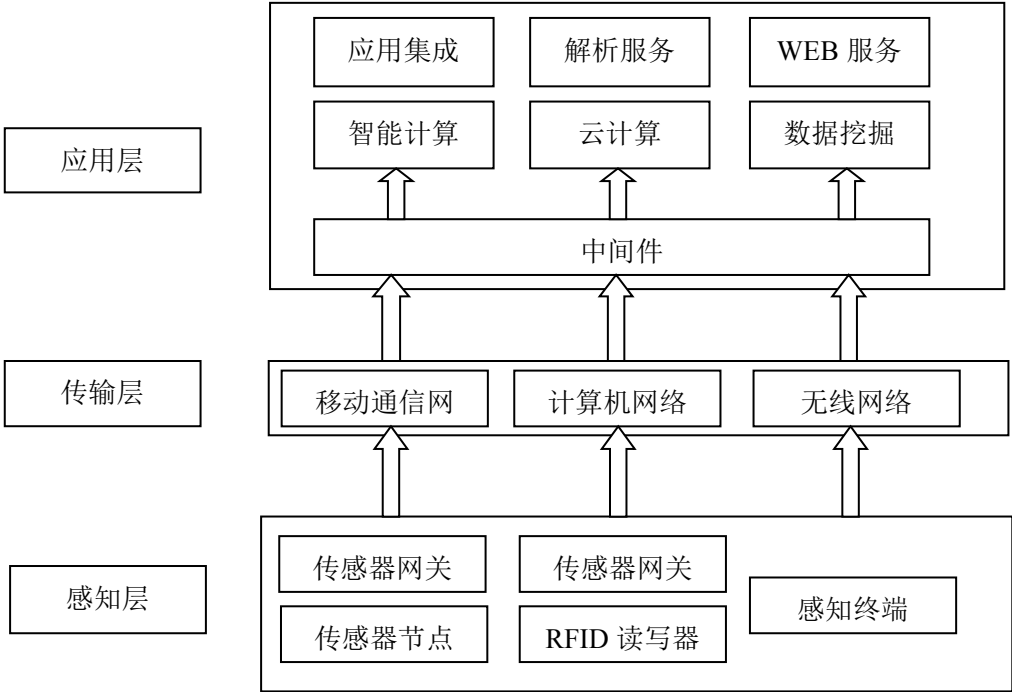


图 1.1 物联网层次架构图

1.1.2 研究意义

物联网技术的精髓在于事物的信息感知，而这恰恰印证了物联网感知层在物联网架构中的重要地位。感知层利用传感器、RFID 设备等实时获取物体信息，并通过蓝牙、红外线、无线传感网络等短距离传输方式传输信息，其结构如图1.2所示。

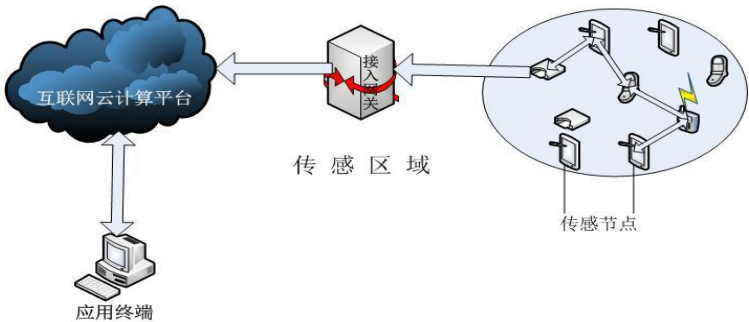


图 1.2 感知层结构图

RFID技术作为物联网中感知层中的核心技术，由于其抗污染、穿透识别性强、无屏障阅读、处理与传输速度快等特点，被广泛应用于公共交通、环境监测、医疗服务、物流运输、移动商务、生产零售等领域^[3]。随着该技术的广泛应用，系统本身的通信安全及数据隐私问

题也随之显现：在一般的RFID系统中，后台数据库服务器和标签之间进行数据交互时，由于缺乏有效的安全协议对传输数据的无线信道进行保护，交互的数据信息容易遭受攻击者截获^[4]，进而对信息隐私性造成巨大威胁。因为RFID系统环境的资源有限，目前成熟的加密算法和安全认证协议无法适应该严苛的环境^[5]，资源受限的RFID系统需要一种适用于该环境的轻量级认证和加密协议，在保证一定安全性的基础上，尽量降低内存和资源占用，提高安全效率，这对RFID技术的进一步应用推广具有深远的意义。

1.2 国内外研究现状

由于RFID技术在物联网体系中的重要地位，RFID系统环境的安全性问题也逐渐成为了国内外研究人员关注的重点。针对该系统环境的特殊性，国内外的轻量级安全协议研究层出不穷，但是因为RFID环境资源有限，现有的国内外研究在平衡安全性和实现效率方面存在不足，提出的认证和加密协议无法适应RFID系统环境。因此，适用于RFID系统的轻量级认证和加密技术还有着广阔的研究空间。

1.2.1 RFID环境中轻量级认证技术

针对适用于RFID环境中的轻量级认证和加密技术研究，国内外研究人员给与了高度关注。

国外研究人员对EPC网络模型中的轻量化安全协议研究较少，还有待进一步查阅考证。而国内的曾会等人^[6]提出了一种基于PKI的改进的EPC网络模型，该网络模型中引入了PKI机制用于对权威数字证书的管理，每一个连入EPC网络的标签对象和数据库服务器等都需要在PKI模块中进行注册得到身份数字证书，这保证的网络的安全性，但也在一定程度上增加了网络负担，同时，在现实应用中由于RFID节点比较分散，很难为分散的RFID节点提供一个固定的管理域进行注册发放证书的工作。

引入第三方认证无法适应相对分散的RFID标签节点网络，一些研究在认证协议过程中结合相关计算或者函数来实现认证。其中SARMA等^[7]提出了一种经典的前向认证协议——Hash-Lock协议，该协议保证了前向安全性，利用hash单向函数将标签的标志信息进行替换，避免标志信息泄露或被追踪，旨在防范标签被恶意追踪。但标签的ID没有动态刷新，其中metaID与ID一一映射的关系始终保持不变，恶意追踪者依然可以通过metaID来追踪标签，从而使得标签受到跟踪攻击。同时，由于认证信息通过明文传输，无法防范重传攻击和假冒攻击。有鉴于此，Henrici等人^[8]对标签ID采取了动态刷新机制，同时引入了Hash函数对存储在

后台数据库服务器端的认证消息进行简单加密计算,从而保证了ID的机密性。但是,经过分析后发现,当标签发送ID之后,若突然中断标签与读写器之间的通信,而后对标签发起持续访问,依然会使的标签陷入追踪。与此同时,该协议中仅实现了单向认证,无法验证后台数据库身份的合法性,容易遭受假冒攻击。丁振华等^[9]提出了一种基于单向Hash散列函数的RFID认证方案,其中标签端仅仅是做了两次哈希运算,比较符合RFID环境对轻量级的需求,但是通过分析发现该方案不具有前向安全性,攻击者在获取当前ID信息后,可以通过分析得出之前的认证信息,从而对标签实施跟踪攻击和重放攻击等。由于Hash函数运算量较小,同样的,张兵等^[10]在前人研究的基础上,对文献[9]中提出的RFID认证方案进行分析,并针对其缺陷进行了改进研究,引入了时间戳和一个任意数两个随机变量,通过进行异或运算实现标签和数据库的双向认证,但是在认证过程中,时间戳是通过明文进行传输的,作为认证口令的一个重要因子,明文传输很容易遭受到恶意攻击者的篡改和中间人攻击。

总结以上基于Hash函数的国内外研究发现,SARMA、丁振华等没有引入标签ID动态刷新机制,使得标签容易受到跟踪攻击;Henrici等人基于前人研究改进引入了动态刷新机制,但依然未能防范跟踪攻击,同时还容易造成标签ID与数据库存储内容刷新不同步,从而使其面临着假冒攻击和拒绝访问攻击的威胁。张兵等人引入了随机因子来防范追踪,达到了很好的效果,但是由于关键的随机因子是通过明文传递,很容易遭受恶意篡改和泄密。

为了给RFID系统提供更高的机密性和安全性,除了在认证中考虑结合Hash函数,研究人员开始考虑引入公钥加密算法到RFID认证协议中。Jue-Sam C等人^[11]将Rabin公钥加密算法加入到认证过程中,提出了一种基于公钥加密和Hash函数的RFID认证协议。该协议由于使用了公钥加密算法,具有很好的机密性和安全性。但是与此同时,标签需要进行多加解密运算以及迭代Hash运算,使得该协议实现性能大大降低,无法适应资源受限的RFID环境。文献[12]中介绍了一种基于混沌加密的RFID认证方案,该文中通过混沌加密技术产生哈希值,强调了混沌加密的安全性和轻量型,该认证加密协议的轻量性可满足RFID受限的资源环境的要求。但是,在该认证方案中标签与数据库端所产生的随机数是通过明文传输,攻击者很容易进行篡改从而导致认证失败。

以上研究将公钥加密算法应用到认证中,为认证信息的机密性和安全性提供了保障。但是通过分析不难发现,Jue-Sam C等在认证协议中引入了公钥加密体制,这使得认证过程安全有效,但由于运算太过复杂,适应性太差。而在文献[12]中,通过混沌加密技术来对认证信息进行哈希加密运算,但该协议加密范围有限,随机数这一重要的认证因子通过明文传递,未达到机密性的要求。

在公钥加密算法中,椭圆曲线密码体制(Elliptic curve cryptography, ECC)相较于其他

的同类型加密算法,有着密钥长度小、占用内存资源低以及加密强度大等优势。因此,ECC算法逐渐被引入到RFID系统认证协议中。Lawrence等人^[13]将椭圆密码算法应用到RFID系统的安全认证协议中,在此基础上提出了一种基于该密码算法的RFID双向认证协议。经分析后可知,该协议安全强度较高,认证过程安全有效;但是该协议的运行过程太过复杂,且功耗大、硬件资源消耗多,由此该协议在RFID环境中的应用性受到了很大影响,而且该协议不具备前向安全性,容易遭受跟踪攻击。Lee Y K等^[14]亦是基于椭圆密码算法提出了一种RFID安全认证协议,并指出在一般通用组模型下该协议是安全的,同时计算量也较小,但随后该方案被指出易于受到跟踪攻击和重放攻击。而后作者有针对性的提出了改进方案,该方案虽可有效避免隐私泄露的问题,但是方案中只是提到了单向认证,没有实现双向认证,依然无法避免数据库端遭受仿冒攻击。Tuyls等人^[15]在Schnorr认证协议的基础上提出了一种应用于RFID系统的认证协议,其中在认证过程中结合了ECC加密算法,虽然该协议中使用了ECC加密算法旨在保护认证消息的安全性,但是经过分析后得知,攻击者可对目标标签实施监听,截获其传送的交互信息,从中倒推计算可得其公钥信息,由于其利用公钥参与认证计算,所以很容易通过公钥区分出之前的消息,不具有前向安全性;同时该协议只实现了单向认证。Batina等^[16]在前人的研究基础上,提出了一种新的结合ECC算法的RFID安全认证协议,该协议中标签的公私密钥存储在标签端,而数据库服务器端存储标签的身份信息ID及标签对应的公钥。该协议将ECC算法结合到认证计算过程中,既保证了认证消息安全性,又能实现有效认证。但由于标签身份信息ID是明文存储,攻击者可分析ID信息从而跟踪标签,同时,该协议只实现了服务器对标签的单向认证,并不能防止攻击者假冒服务器。Chen Y等人^[17]考虑到公钥密码算法的高安全强度,提出了基于公钥加密的算法,涉及公钥加密函数、Hash函数和随机数生成函数,这使得算法占用了大量内存空间,且运算过程复杂,随后该协议被证明无法提供位置隐私保护以及容易遭受重放攻击。而康鸿雁等^[18]中考虑到椭圆密码算法的高效安全强度以及具有一定的轻量性,从而提出了基于ECC算法的组认证协议,该协议可针对多个RFID标签同时验证,其中加入了时间戳和任意数,以此来防止跟踪攻击和重放攻击,分析后发现该组证明协议的安全性较高,该认证协议针对的是组处理多个标签认证,工作强度较大,认证过程也较为复杂,但其认证中引入时间戳和任意数这两个随机因子增加了认证消息的不确定性,这一做法值得研究借鉴。

文献[13]-[18]中考虑引入了具有轻量级特性的ECC算法,但依然存在诸多问题,其中最典型的即是未实现双向认证,这说明对于RFID双向认证问题的研究目前还是较为匮乏。基于以上文献研究可知,针对RFID环境中轻量级认证问题,国内外研究都在极力寻求能够平衡安全性和适用性的认证协议,但很多都不尽人意,而本文也正是循着前人的脚步继续开展研究。

1.2.2 RFID 环境中轻量级密码算法

现有的密码算法体制大致分为两种：对称密码算法和非对称密码算法。针对 RFID 系统这种资源极端有限的环境，现有研究主要对基于成熟密码算法进行轻量化以适应该特殊环境。

对于对称密码算法，主要是通过以下两种方式进行轻量化：

(1) 对密码算法中密钥长度进行适量缩减，从而降低算法实现时的运算复杂度和占用的内存空间。对于对称密码而言，其加解密过程中的密钥是相同的，所以密钥长度与算法的安全强度有直接的关系，对于某些算法而言，减少部分密钥长度既保证了一定的安全强度，又可以达到轻量化的目的。如 DESL 算法^[19]以及 A2U2 算法^[20]均是通过改变密钥长度来达到轻量化的目的。

(2) 减少密码算法过程中的加密轮次，从而降低能耗。对于对称密码算法中的分组密码算法，其安全强度主要是依靠对明文的多次的反复加密来保证，每迭代加密一次则称为一轮，通过减少加密轮次可使算法达到轻量级水平。如 ITUbee 算法^[21]及 MIBS 算法^[22]即是如此。

在常见的非对称密码算法中，单向散列函数因其计算简单，在构建 RFID 系统安全协议时得到了广泛应用。如常见的基于 Hash 函数的安全认证机制，在 1.2.1 节介绍的文献[6]-[8]、[14]-[17]中，均涉及了 Hash 函数加密。在该种认证机制中，可实现标签和数据库服务器之间的安全认证，并且同时解决了信息隐私保护问题，其运算量一般较小，对标签要求低，但其安全性不高，无法满足 RFID 系统环境的安全需求。

随着制造业的发展，RFID 标签的存储和计算能力也不断提高，越来越多的研究人员考虑将非对称密码算法中的公钥加密技术引入 RFID 安全协议中。其中以 RSA 公钥密码体制和 ECC 公钥密码体制最为典型：RSA 算法在公钥密码体制中较为经典，技术相对完善，被广泛应用在现代安全协议中。但是由于 RSA 密钥位数过于庞大，一般都在 1024bits 以上，不适合在 RFID 系统中使用。而 ECC 算法相较于其他公钥密码算法（如 DSA），具有每比特数最高的安全强度，与此同时，其对存储空间需求较小，密钥长度和系统参数比一般的公钥密码算法如 RSA 也小得多。这一优势使得 ECC 算法对带宽和资源的要求大大降低，从而在 RFID 系统的安全协议中受到诸多青睐。文献[23]提出了一种适用于 RFID 嵌入式设备的改进 ECC 密码算法，该种算法是通过牺牲灵活性来换取面积节省的 ECC 轻量级实现。除此以外，有研究针对 ECC 算法运算过程中的标量乘运算进行改进，文献[24]、[25]即是通过对标量乘的运算过程进行分解计算，以达到降低运算量的目的。

本文亦是考虑到 ECC 算法的加密强度大、计算处理速度快、消耗内存空间小、带宽要求低等技术优势，在原有的 ECC 算法基础上，对其运算过程进行轻量化改进，以期提高该算法

在资源极端有限的 RFID 系统环境中的适应性，并将其与 RFID 认证协议相结合，在保证轻量性的前提下，提高认证协议的安全强度，从而更好地保障 RFID 环境的安全性。

1.3 研究内容和目标

1.3.1 研究内容

目前针对 RFID 这种资源受限的应用环境，在对现有的轻量级认证和加密技术进行研究的基础上，继续深入轻量化探索研究既是大势所趋，更是形势所迫，而本课题的主要研究工作是轻量级 RFID 双向认证协议，同时在研究了原有 ECC 算法的基础上，对 ECC 算法加解密过程中的标量乘运算进行改进，以期该算法能更好地适应 RFID 环境。与此同时，将改进后的算法引入 RFID 双向认证协议中，在保证轻量化的前提下，进一步提高认证协议的安全强度。最后通过逻辑证明认证协议的正确可行性，通过模拟实验对比来验证该认证协议和改进的 ECC 算法的有效性和优越性。本文具体的研究内容如下：

(1) 简要介绍 RFID 系统组成以及运行原理，分析研究现有的 RFID 环境中面临的主要的安全威胁。针对一次性口令认证技术即 OTP (One Time Password) 认证机制进行研究，探究其认证过程，分析该认证机制的优越性和局限性，并在此基础上提出一种新的适用于 RFID 环境基于 ECC 的双向认证协议，以期提高 RFID 环境的安全性。

(2) 介绍现有的轻量级加密算法，主要是研究各种算法的轻量性，并进行对比分析，给出研究结果。在重点研究了 ECC 算法加解密过程的基础上，针对影响该算法运行效率的关键因素，即标量乘运算进行改进，提出了一种高效率的新双基标量乘算法。

(3) 通过数据分析和实验来验证改进的 ECC 算法的效率，而后通过模拟实现来验证结合改进后 ECC 算法的 RFID 双向认证协议的有效性，分析验证结果。

1.3.2 研究目标

在对 RFID 系统进行分析后可知，对于资源受限的 RFID 环境而言，急需适用于该严苛环境的具有轻量化性质的认证和加密等安全协议来保障 RFID 系统运行的安全性。而轻量级安全协议的目标则是在保证适用性的前提下，为系统提供一定的安全性保护。本课题的研究目标即是研究兼顾有效性和安全性的适用于 RFID 环境的轻量级认证协议、轻量级加密算法。为此，本课题预期达到以下目标：

(1) 设计一种适用于资源受限的 RFID 系统环境的双向认证协议，满足该系统对轻量性

和安全性的需求;

(2) 对现有的 ECC 算法加解密过程中的标量乘运算进行改进, 进一步实现 ECC 算法的轻量化, 使其能更好的适应 RFID 环境。

(3) 通过逻辑证明和实验分析说明本文提出的 RFID 双向认证协议的有效性; 同时将改进后的 ECC 算法与之相结合, 提高认证协议的安全性。

1.4 论文的结构组织

本文共分六章, 详细的章节内容如下:

第一章 绪论: 本章主要阐述了研究适用于物联网 RFID 系统中的轻量级认证和加密算法的背景和意义, 以及该课题相关的国内外研究现状, 并且介绍了本文的主要研究内容、研究目标以及章节结构。

第二章 介绍了 RFID 系统结构及运行原理, 分析了 RFID 环境中主要安全威胁, 同时介绍了本文研究工作中涉及的关键技术和数学知识。

第三章 研究分析了一次性认证机制即 OTP 认证协议的运行过程, 探究 OTP 协议的原理和优缺点, 并以此为基础进行设计改进, 提出一种基于 ECC 和 OTP 认证的 RFID 双向认证协议。并对该协议进行了性能分析, 通过可行性分析可知, 本协议具有轻量化特性, 可适用于 RFID 环境中; 同时本协议的安全性与运行效率较之前文献中的多种基于 ECC 算法的认证协议更为优越。

第四章 介绍了几种主要的轻量级密码算法, 并对各种算法的轻量性进行对比分析, 而后重点针对 ECC 算法加解密过程中的关键运算也即标量乘运算进行研究, 在传统的双基标量乘算法基础上, 改进提出了一种基于新双基的标量乘算法。通过算法复杂度分析和实验验证可知, 改进后的算法相较于原算法, 其标量乘运算量明显降低, 与其他典型的密码算法相比, 在运行效率上的优势也较为突出。

第五章 通过一种逻辑分析验证方法即 BAN 逻辑验证了 RFID 双向认证协议的正确性, 在此基础上模拟实现引入改进后 ECC 算法的认证协议, 验证了本协议的有效性和实用性。

第六章 总结与展望: 对本文所做的工作以及成果进行总结分析, 指出文中存在的问题和需要改进之处, 并有针对性的提出今后有可能的改进方法和研究方向。

第二章 RFID 系统与椭圆曲线密码学基础

2.1 RFID 系统

2.1.1 RFID 系统组成

RFID 系统由于其应用场景的不同，具体的系统组成也不尽相同，但一般的 RFID 系统有三个基本的组成部分，即 RFID 电子标签（Labels）、RFID 读写器（Reader）以及后端数据库服务器（Database），如图 2.1 所示。

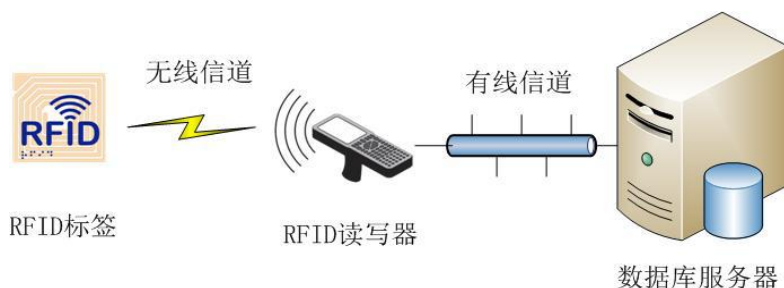


图 2.1 RFID 系统基本结构图

在图 2.1 中可以看出，一般的 RFID 读写器与后台数据库服务器之间的通信信道是有线信道，即通过有线网络设备进行连接，我们认为该信道是安全可靠信道；而 RFID 标签与读写器之间的信道一般被视为不可靠信道，因其之间通信的无线信道缺乏有效的安全防护手段。

（1）RFID 标签

标签是 RFID 系统的数据载体，内含有一个集成芯片，一般的标签芯片中写有物体的身份标识和相关信息，同时可作为标签的主要控制运算单元，标签应用时的数据传输控制、计算认证等功能均是由芯片完成。每个 RFID 标签具有唯一的电子产品编码，并附着在物体上标识目标对象，其外形也是多种多样，常见的如卡状、标签、纽扣等。

（2）读写器

RFID 读写器是负责读取（写入）RFID 标签信息的工具，同时作为标签与后端数据库服务器的通信中继。读写器一般是由天线、控制模块以及信号收发装置组成，该设备通过天线发送载波信号与标签进行通信，读取标签信息，然后将接收到的信号通过控制模块调制为数字信号，并传送给后端服务器。

（3）RFID 后端服务器

在 RFID 系统中，后台服务器的主要要完成对读写器传送过来的信息的处理和存储，并

为将处理的结果（包含认证信息）通过读写器返回给标签。对现阶段 RFID 系统而言，它是负责整个 RFID 系统的计算控制和存储任务的主要部件。

2.1.2 RFID 系统主要工作原理

关于 RFID 系统的工作原理，简而言之，在 RFID 系统开始运作后，RFID 读写器通过天线连续不断的发送出一定频率的载波信号，形成射频磁场。当 RFID 标签进入 RFID 读写器的射频磁场时，存储在芯片中的信息借助接收到的感应电流提供的能量转化为载波信号，发送给读写器（被称为被动标签，Passive Label），或者通过自己的能量主动发送某一频率的载波信号（被称为主动标签，Active Label）；随后读写器读取信息并把射频信号调制为数字信号，将数据以数字信号的形式传输到中央信息系统进行有关的数据处理。

一般的 RFID 系统都有基本的工作流程，从流程中可以看出，在 RFID 系统中，读写器通与标签之间过无线射频信号进行无线信息交互，这期间包括认证信息和物品信息的传递和读取。具体的工作流程如下^[26]：

- （1）首先读写器通过天线持续不断的发出无线射频载波信号，从而在一定范围内形成一个射频磁场；
- （2）当 RFID 电子标签进入读写器的磁场后，以主动或者被动的形式通过内置天线向读写器发送响应信息；
- （3）读写器将由标签端传来的载波信号进行解码并读取信息，而后发送给后台服务器；
- （4）服务器根据接收到的信息做出相应的控制、处理操作。

相对应的，RFID 读写器与标签之间有规范的类似于其他网络通信模型的双向通信协议，该协议模型如图 2.2 所示：

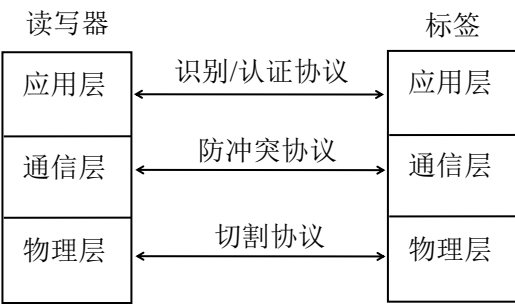


图 2.2 RFID 通信模型

由图 2.2 中可以看出，RFID 系统中的双向通信协议主要分为三层，自下而上依次为：物理层、通信层以及应用层。物理层主要涉及的是载波信号、射频频段等电气信号方面的问题；通信层规定了读写器与标签之间的交互方式，主要解决了读写器同时对多个不同标签的访问

控制问题；而应用层主要研究识别、认证以及数据逻辑处理应用的问题，本文中所研究的轻量级认证和加密问题即是工作在该层的安全协议。

2.2 RFID 系统的安全分析

由于 RFID 系统结构及所处环境的特殊性，该系统面临着诸多安全问题，如设备物理破坏、非法身份假冒、恶意跟踪等。下面我们从 RFID 系统自身结构特点以及所处环境来分析 RFID 系统目前所面临的安全威胁和问题来源。

2.2.1 RFID 系统的安全漏洞

(1) 工作环境简陋

在现有的 RFID 系统应用中，许多 RFID 设备的工作运行环境比较简陋，有些甚至工作的极端恶劣的偏远地区，该地区 RFID 设备缺乏有效的物理防护，经年累月的遭受恶劣环境的侵蚀，从而对 RFID 系统的运行造成一定的影响。

(2) 标签资源限制

标签依据调制方式的不同可分为被动式、半主动式和主动式三种。而其中被动式标签在工作时需要从读写器发出载波信号中获得能量，而其余两种所携带的能量也只能满足标签芯片发送信号的需要。这一特点决定了 RFID 标签必须是低功耗的，从而使得电子标签中电路系统的功耗和存储等资源都受到很大的限制，现有复杂的认证和加密体系无法适应资源受限的 RFID 系统环境，这使得 RFID 通信系统的安全性、有效性以及低耗性受到了严重挑战。若不采取相应措施保证 RFID 标签的安全性，标签中存储的隐私信息可能会被恶意读取、更改，严重影响了 RFID 标签的应用。

(3) 无线射频通信

RFID 系统采用无线射频通信技术实现读写器与 RFID 标签之间的非接触式通信，而由于该无线信道缺乏有效的安全协议保护，因此传输的载波信号非常容易被窃听或者被干扰，严重威胁着传输信息的机密性和可靠性。另外，如此开放的通信链路也极易使得非法用户伪造 RFID 标签，从而达到恶意欺骗用户的目的。

2.2.2 RFID 系统的安全威胁

尽管 RFID 技术得到了广泛的应用，但由于 RFID 系统存在以上所述的安全漏洞，这使得

该系统依然面临着多种安全威胁，本小节将分析几种主要的安全威胁^[27]。

（1）物理攻击

发动物理攻击的前提条件是攻击者能够直接接触到标签或者 RFID 读写器。其中物理攻击有多种方式，例如：恶意损毁标签，利用射线对标签内容进行破坏，使用相近波段的电磁波干扰标签与阅读器之间的通信信号。

（2）RFID 标签伪造

因为 RFID 标签的存储空间有限，因而其资源受到很大约束，一般标签缺乏有效的安全协议保护，很容易进行伪造。例如攻击者可以利用空白的 RFID 标签伪造为合法的电子标签，或者直接对现有的合法标签信息进行修改，从而利用修改后的标签侵入 RFID 认证系统，一旦通过认证，则该攻击者可非法获取相应的访问控制权限，对现有的 RFID 系统进行破坏或者读取隐私信息，这严重威胁着 RFID 系统有效性、可靠性。

（3）RFID 嗅探

RFID 嗅探主要是由于 RFID 认证系统的单向性造成的。由以上对 RFID 系统的基本工作流程分析可知，一般的 RFID 读写器向标签发起认证请求，而后标签响应该认证请求并发送认证信息给读写器，读写器将标签的认证信息转发给后端数据库服务器，从而由后台服务器验证标签身份的合法性。但值得注意的是，以上步骤仅仅实现了数据库对标签的单向认证，标签无法判断服务器的合法性。这一漏洞就使得恶意攻击者可利用非法的 RFID 读写器窃取标签的隐私内容，严重威胁着 RFID 系统隐私性。

（4）跟踪攻击

跟踪攻击是指恶意攻击者通过跟踪分析每个标签特有的自身信息，从而对特定的事物实施跟踪攻击。这是因为读写器可读取当前处于其射频磁场范围内的所有标签信息，同时可实时记录每个标签的所处位置。这就使得恶意攻击者可以通过移动的便携式读写器，跟踪携带贴有 RFID 标签物品的主体人的位置。

（5）欺骗攻击

在欺骗攻击中，攻击者利用某种伪装手段将自己伪造成为一个合法用户，从而实施恶意攻击。如在仅实现单向认证的 RFID 系统中，由于缺乏对后台数据库的合法性认证，攻击者可以伪装成合法的后台数据库服务器，从而对 RFID 系统造成破坏性操作。

（6）重放攻击

重放攻击是指攻击者通过截获标签与读写器之间的交互信息，同时记录下标签与读写器之间的通信序列，并在之后标签与数据库再次发起通信时，将截获的消息重传给读写器或者数据库端，从而达到伪装合法标签或数据库的目的。

2.2.3 RFID 系统的安全方案

(1) 针对 RFID 系统部署环境和物理攻击问题, 主要考虑加强 RFID 设备的物理防护, 为在恶劣环境工作的大型 RFID 系统提供完备的防护和遮挡工事; 同时研发特殊的耐磨性、防辐射性材料以替代现有的标签材质。

(2) 对于除物理攻击外的其他安全威胁, 相关研究提出可以通过物理方法对 RFID 系统进行有效的防护, 如法拉第罩法、主动干扰法等^[28]。但是物理方法在实际操作过程中, 涉及的物理设备过于繁琐庞大, 实施较为不便, 所以我们更多的考虑通过基于密码技术的安全协议体系为 RFID 系统提供一定的安全保护。而适用于 RFID 系统的认证和加密技术需要满足以下几种安全需求:

(a) 可用性: RFID 认证协议和加密算法等安全协议能够在 RFID 系统中应用, 并能有效防止恶意攻击者的一般性恶意攻击;

(b) 机密性: 标签中所存储的隐私信息以及认证和通信中的隐私信息不能被泄露;

(c) 完整性: 在通信过程中, 保证接收方收到的信息在信道传输中没有被破坏和篡改;

(d) 隐私性: 现在的 RFID 标签大都容易遭受跟踪攻击, 从而使得标签位置泄露, 无法达到用户对隐私性的要求。

2.3 椭圆曲线密码学相关理论概述

2.3.1 群和有限域基础

(1) 群

设有一非空集合 G , 在该集合上存在一种运算 “ \bullet ”, 我们称之为集合 G 上的乘法运算。现我们定义非空集合 G 与该集合上的乘法运算构成了形如 $G \bullet G \mapsto G$ 的代数结构 (G, \bullet) , 且满足如下条件:

(a) 封闭性: $\forall a, b \in G, a \bullet b \in G$ 。

(b) 结合律: $\forall a, b, c \in G, (a \bullet b) \bullet c = a \bullet (b \bullet c)$ 。

(c) 单位元存在律: $\exists e \in G$, 使得 $\forall a \in G$, 有 $e \bullet a = a \bullet e = a$, 则 e 为单位元。

(d) 逆元存在律: 对 $\forall a \in G, \exists b \in G$, 使得 $a \bullet b = b \bullet a = e$, 则 b 称为 a 的逆元, 记为 a^{-1} 。

则 (G, \bullet) 被称为群, 如果集合 G 中二元运算为乘法, G 为乘法群, 若为加法, 则为加法群。

(2) 有限域

域是由非空集合 F 、群运算中的加法运算以及乘法运算组成的，且同时满足以下三个条件：

(a) F 中的元素关于运算 “+” 构成交换群（交换群即满足交换律的群），设其单位元为 0。

(b) F 中元素排除元素 0 以外的元素关于运算 “•” 构成交换群，设其单位元为 1。

(c) 满足分配律。即 $\forall a, b, c \in F, a \bullet (b + c) = (b + c) \bullet a = a \bullet b + a \bullet c$ 。

若集合 F 中由有限个元素组成，则该集合就被称为有限域，其中集合中的元素个数为域的阶，通常椭圆曲线上的常用的有限域为素数域或二进制域。

通常阶为 2^m 的有限域被称为二进制域，用符号 $GF(2^m)$ 表示。其中 m 是任意的正整数。 $GF(2^m)$ 是椭圆曲线密码体制中最常用的有限域，可以通过多项基表示法来构建二进制域 $GF(2^m)$ ，即：

$$GF(2^m) = \{a_{m-1}z^{m-1} + a_{m-2}z^{m-2} + \dots + a_2z^2 + a_1z + a_0, a \in \{-1, 1\}\} \quad (2.1)$$

由公式中可以看出， z 的最高次幂为 $m-1$ ，本文中所选取的椭圆曲线即是在二进制有限域的基础上形成的。

2.3.2 椭圆曲线理论基础

(1) 椭圆的概念

有限域 $GF(q)$ 上的椭圆曲线 E 有如下定义：

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (2.2)$$

其中 $a_1, a_2, a_3, a_4, a_6 \in GF(q)$ ，且 $\Delta \neq 0$ ， Δ 表示 E 的判别式，具体的定义如下所示：

$$\begin{cases} \Delta = -d_2d_8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \\ d_2 = a_1^2 + 4a_4 \\ d_4 = 2a_4 + a_1a_3 \\ d_6 = a_3^2 + 4a_6 \\ d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{cases} \quad (2.3)$$

一般的我们将公式 (2.2) 中的椭圆曲线方程称为 Weierstass 方程，椭圆曲线公钥密码体制中正是应用的该形式的方程，下面主要介绍该方程在 $GF(2^m)$ 上的性质。

(2) 二进制域上椭圆曲线方程相关点运算

本文研究的是二进制有限域 $GF(2^m)$ 上的椭圆曲线，并以此为椭圆曲线密码学的基础。所以我们重点关注 $GF(2^m)$ 域上的椭圆曲线变形方程，以及椭圆曲线密码体制相关的点运算。

Weierstass 方程在 $GF(2^m)$ 有限域上的简化形式如下：

$$E: y^2 + xy = x^3 + ax^2 + b, E \in GF(2^m) \quad (2.4)$$

在 $GF(2^m)$ 有限域上，相关的点运算法则：

(a) 单位零元： $\forall P \in E(GF(2^m)), P + \infty = \infty + P = P$ ， ∞ 为椭圆曲线上无穷远点。

(b) 负元素：若 $P(x, y) \in E(GF(2^m))$, $(x, y) + (x, -y) = \infty$ ，记点 $(x, -y)$ 称为点 P 的负元素，并将其记为 $-P$ ，其中， $-P \in E(GF(2^m))$ 。

(c) 点加运算：令 $P(x_1, y_1) \in E(GF(2^m)), Q(x_2, y_2) \in E(GF(2^m))$, $P \neq \pm Q$ 则 $P + Q = (x_3, y_3)$ 。

则

$$\begin{cases} x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \\ y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \end{cases} \quad (2.5)$$

其中 $\lambda = \frac{y_1 + y_2}{x_1 + x_2}$ ，点 $(x_3, y_3) \in E(GF(2^m))$ 。

(d) 倍点运算：令 $P = (x_1, y_1) \in E(GF(2^m))$, $P \neq -P$ ，则 $2P = (x_3, y_3)$ 。其中

$$\begin{cases} x_3 = \lambda^2 + \lambda + a = x_1^2 + \frac{b}{x_1^2} \\ y_3 = x_1^2 + \lambda x_3 + x_3 \end{cases} \quad (2.6)$$

而 $\lambda = x_1 + \frac{y_1}{x_1}$ ，点 $(x_3, y_3) \in E(GF(2^m))$ 。

(3) 椭圆曲线的挠点

设在有限域 $GF(2^m)$ 上有椭圆曲线 $E: y^2 + xy = x^3 + ax^2 + b$ ，记为 $E(GF(2^m))$ ，其中 $a, b \in GF(2^m)$ 。若 $P \in E(GF(2^m))$ ，满足 $nP = e$ ， $n > 0$ ，且 e 为单位元，则称 P 为 n -挠点。

用 $E[n]$ 表示椭圆曲线 $E(GF(2^m))$ 上 n -挠点组成的群。当该椭圆曲线可由如下表示时：

$$\forall k \in \mathbf{N}: E[2^k] \approx \mathbf{Z} / 2^k \mathbf{Z} \quad (2.7)$$

$$E(GF(2^m)) = G \times E[2^k] \quad (2.8)$$

其中, G 是一个奇数阶群, $k \geq 1$, 当 $k=1$ 时, 则基于有限域 $GF(2^m)$ 上的椭圆曲线 $E(GF(2^m))$ 有极小 2-挠点。这种具有极小 2-挠点的椭圆曲线对本课题有着重要的研究意义, 本文用到的椭圆曲线即设定为具有该种性质的椭圆曲线。

2.3.3 椭圆曲线密码体制

(1) 椭圆曲线离散对数问题

求解椭圆曲线上离散对数问题 ECDLP (Elliptic Curve Discrete Logarithm Problem) 的困难复杂度是椭圆曲线密码算法的安全性研究的基础。该问题的描述是一个求解过程: 假设有 点 P, Q , $P \in E(GF(p))$, $Q \in E(GF(p))$, 其中 $E(GF(p))$ 为有限域 $GF(p)$ 上的椭圆曲线, 其中选取 P 点做为椭圆曲线上的基点。 k 为一任意整数, 已知 $Q = \underbrace{P + P + \dots + P}_k = kP$ 和点 P , 求 k 。求解该问题的时间复杂度为指数级的, 其破解运算的复杂程度远非其他公钥密码算法可比, 这也是椭圆曲线密码算法安全性的数学理论支撑。

(2) 椭圆曲线密码体制

本文我们主要关注二进制域 $GF(2^m)$ 上的椭圆曲线, 首先给出椭圆曲线密码体制运行的基本的系统参数。在 $GF(2^m)$ 上椭圆曲线的基本参数主要有一组 $T = \{f(x), a, b, P, m\}$ 这 5 个元素组成, 其中, $f(x)$ 表示构建二进制域的多项式基, a, b 两个参数决定了具体的椭圆曲线表示方程, 也即椭圆曲线的形成, P 表示在该曲线上选取的基点, 其中 $P \in GF(2^m)$, m 表示 $GF(2^m)$ 的阶。则椭圆密码体制的具体过程为:

(a) 首先由一方 L 在约定的域上主动产生一条椭圆曲线 $E(GF(2^m))$, 同时在该曲线上选取一点 P 做为基点, 在 $[1, m-1]$ 上随机产生一个 k 作为 L 的私钥, 即 $k \in [1, m-1]$, 由 k 生成 A 的公开密钥 $K = kP$, 将 $E(GF(2^m))$ 和 K, P 传给另一方 S ;

(b) 当 S 方接收到 L 方传送的信息后, 在发送消息之前, 将明文映射为 $E(GF(2^m))$ 上的一点 M , 随后随机产生一个整数 r , 并计算 $C_1 = M + rK, C_2 = rP$ 后, 将 C_1, C_2 发送给 L 方;

(c) 在 L 方收到 S 方的消息后, 计算 $C_1 - kC_2 = M + rK - k(rP) = M + rK - r(kP) = M$, 然后将点 M 进行逆映射反解即可得到明文。

由以上过程可以看出, 公开传输的参数, 只有 $E(GF(2^m))$ 、 K 、 P 、 C_1 、 C_2 。而根据椭圆曲线上求解离散对数困难性问题可知, 已知 K, P 求 k 或已知 C_1, C_2 求 r , 其求解运算量均是指数级的, 这就从理论上保证了传输过程中信息的完整性和安全性。同时, $K = kP$ 的运算过程即为标量乘运算, 从以上椭圆曲线密码体制的构建过程不难看出, 该运算是椭圆曲线密码体制运行的关键性运算, 其运算效率直接决定着整体密码算法的运行效率。

2.4 本章小结

本章主要介绍了 RFID 系统与椭圆曲线密码体制,重点分析了 RFID 系统组成以及系统现在所面临的主要安全威胁,并针对其提出了相应的安全方案。对于椭圆曲线密码体制,首先介绍了椭圆曲线的定义,密码算法中涉及的基本数学运算,主要是椭圆曲线上的点运算,最后介绍了椭圆曲线密码体制的过程,从中可以看出标量乘运算在整个密码体制运算中的重要地位。

第三章 基于 ECC 和 OTP 认证的 RFID 双向认证协议

根据第二章中对 RFID 环境特殊性的分析可知, 现有的 RFID 系统环境面临着巨大的安全威胁, 其中针对物理破坏, 需加强对 RFID 节点和设备的监控保护, 尤其是应该加强对 RFID 设备的物理保护; 而其他由于系统环境特殊性造成的安全漏洞, 如常见的假冒攻击、重放攻击等安全威胁, 主要原因是: 在存储和计算资源有限的 RFID 环境中, 缺乏适当有效的轻量级 RFID 系统安全认证机制, 而传统的认证技术已无法适应 RFID 的环境需求。针对适用于 RFID 环境的认证问题, 现有的 RFID 认证方案在平衡安全性和轻量级这两个主要性能方面普遍存在一些问题: 某些方案在充分保证了安全性的前提下, 往往无法适用于 RFID 系统环境; 而一些方案达到了轻量级的要求, 又无法保证系统环境的安全性。有鉴于此, 本文提出了一种适用于 RFID 系统环境, 基于 ECC 与 OTP 认证的双向认证协议(RFID Mutual Authentication Scheme Based on ECC and OTP, RMASBEO), 该方案实现了标签端与数据库端的双向认证, 结合 RFID 环境中对资源和能量的严苛要求, 在借鉴了计算简便、又无需十分复杂算法的 OTP 认证机制的基础上, 引入了椭圆曲线公钥加密算法来保证了认证过程中认证消息的机密性, 同时由于椭圆曲线密码算法运算速度快, 安全性强度较高, 适用于计算资源、存储资源有限的 RFID 认证环境, 具备可靠、轻量的加密性能, 这使方案整体上达到了安全、有效以及轻量级的要求。

3.1 OTP 认证机制

3.1.1 OTP 认证技术基本原理

OTP 是一种摘要认证, 其输入为长度不定的明文消息, 经摘要函数压缩处理后, 变成固定长度的密文输出。在给定一个经摘要函数处理后定长的密文后, 要求找出一个输入明文, 使得其经过函数运算后产生与给定输出相同的密文, 此过程在计算上是不可行的, 也即运算是单向不可逆的, 这保证了信息安全性^[29]。OTP 的基本思想是在认证的过程中引入随机因子(如随机数, 时间戳等), 从而使得不同认证序列所用的认证密码口令都不相同, 攻击者无法根据以往截获的认证因子来推测之后的认证信息。这一方法保证了认证信息的前向安全性, 同时防止了字典攻击、重放攻击、窃听破坏等恶意攻击, 从而提高了认证过程的安全性。

3.1.2 S/Key 一次性口令认证协议

S/Key是一种典型的OTP认证协议，亦是本文的RFID双向认证方案的基础，在一般的S/Key方案中，主要由两部分组成，分别为用户端和服务端。

用户端将自己生成的通行密语与收到的从服务器端传来的挑战消息连接起来，然后输入口令计算器计算一次性口令，并利用Hash函数对口令进行加密保护。

服务器端在接收到用户端的认证请求时，产生挑战信息，而挑战消息主要有两部分组成：种子值Seed和迭代次数N，其中Seed是由10-64个字母或者数字组成，N在每次认证成功之后依次递减1。服务器端收到用户端传来的响应消息即用户一次性口令后，对其进行正确性校验，若验证成功，则将本次认证的口令和服务序号存储起来，以便进行下一次认证服务。该认证过程如图3.1所示。

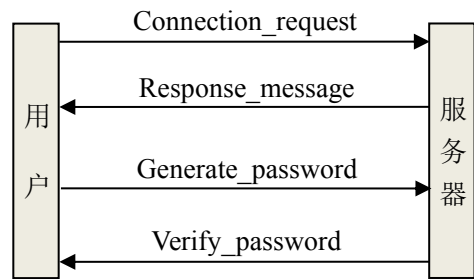


图3.1 OTP认证机制过程图

具体认证过程如下^[30]：

- （1）连接请求（Connection_request）。用户端以用户ID作为认证消息向服务器端发起认证请求；
- （2）响应请求（Response_message）。服务器在收到用户ID后，依据用户ID查找数据库中的用户对应的种子值Seed和迭代次数（N-1），并以此做为响应消息，发送给用户端，若未找到，则拒绝验证；
- （3）生成认证口令（Generate_password）。用户端在收到服务器响应信息后，将其中的种子值Seed与客户端生成的秘密用户通行短语（secret_password）连接起来，通过口令产生程序生成口令，而后再将口令做N-1次的哈希迭代运算，把计算结果发送给服务器端；
- （4）认证并存储口令（Verify_password）。服务器接收到用户端消息后，将计算结果在做一次相同的哈希运算，并与服务器端存储的认证口令比较验证。若二者相等则通过认证，并将服务器端存储的认证口令更新为本次的认证口令，同时将迭代次数减1，以便进行下一次认证服务。否则拒绝认证，即认证失败。

3.1.3 S/Key 认证协议安全性分析

从以上 S/Key 认证协议的过程描述中可以看出, 一次性口令认证协议的原理较为简单, 迭代次数随着认证成功的次数的增长而依次递减, 即认证成功次数加 1, 则迭代次数减 1。这就使得每次认证生成的口令是动态变化的, 可有效抵御重放攻击。同时在认证过程中使用的单向散列函数, 对用户的隐私信息也提供了一定保护。但是在该认证协议中, 并没有提供对数据的加密过程, 种子值 *Seed* 和迭代次数 *N* 均是明文传递, 而且该协议仅提供了服务器对用户端的单向认证。基于以上协议的过程描述和分析, S/Key 协议有可能面临的安全威胁有以下几方面:

(1) 假冒攻击

在一次性口令认证协议中, 最致命的缺点即是该协议仅实现了客户端对服务器的单向认证, 缺乏对服务器端的合法认证。若恶意攻击者假冒合法服务器, 则有可能对合法的用户端进行欺骗, 诱使其使用还未使用的有效密码口令, 而后攻击者可利用该口令向真正的服务器发起认证, 从而继续假冒合法用户, 这严重威胁协议安全性。

(2) 口令泄露

在 S/Key 协议中, 作为挑战消息的种子值 *Seed* 和迭代次数 *N* 均是明文传递, 攻击者可以轻易的获取该消息, 或者对种子值和迭代次数进行更改, 方便其发起小数攻击或者字典攻击。

(3) 小数攻击

当服务器响应了客户端的认证请求时, 由于响应消息是明文传输, 攻击者可以将其中的种子值 *Seed* 以及迭代值 *N* 截获, 并另外选取较小的数值 *N'* 来替代原迭代值 *N*, 由于服务器端缺乏合法认证, 攻击者可假冒服务器, 将种子值 *Seed* 和伪迭代值 *N'* 连接起来作为响应消息发给用户端; 由于用户端无法识别服务器的合法性, 则依据协议规则利用收到的种子和迭代值 *N'* 计算 OTP 口令发送给服务器端, 伪服务器收到 OTP 口令后, 利用公开的 Hash 函数经多次迭代计算出有效的较大迭代值 OTP 口令, 由此攻击者就可获得该用户后续的一系列 OTP 口令, 进而攻击者可在一段时间假冒合法用户与服务器进行通信。

(4) 字典攻击

由于用户端的秘密通行密语 (*secret_password*) 均是由用户端自行产生, 因此口令的复杂程度无法得到保证, 若口令过于简单, 口令产生习惯被跟踪或者泄露, 则很容易遭受字典攻击或者猜测攻击。

(5) 计算量大

在每次认证中, 用户端要进行多次迭代散列运算, 这严重影响了认证协议的运行效率。

3.2 RFID 双向认证协议

有鉴于OTP认证协议的局限性，本文提出的RFID双向认证协议是以此OTP认证机制为基础，借鉴了该认证机制的主要框架，考虑到RMASBEO协议是应用到资源受限的RFID系统环境中，摒弃了OTP认证机制中原有的用户端口令生成算法思想，在本文中，为每一个标签设定出厂的唯一标识，在认证过程中，标签端利用该标识进行简单的计算，并将其作为挑战口令向服务器端发给认证，这大大提高了该协议的轻量化程度。本文的认证协议主要由注册和认证两个阶段组成，为方便说明，符号定义见表3.1所示。

表3.1 RFID双向认证协议符号注释表

符号	符号注释	符号	符号注释
id	标签验证码 pw 的逆序串	k_{DS}	数据库私钥
pw	标签的验证码, 出厂时即与标签绑定	k_{UP}	RFID 标签公钥
T_{i-1}	注册时使用的时间戳, 同时也作为第一次认证使用的认证口令因子	k_{US}	RFID 标签私钥
T_i	上一次认证使用的时间戳	$Ek()$	椭圆曲线加密函数
T_{i+1}	用于下一次认证的时间戳	$Dk()$	椭圆曲线解密函数
$H()$	哈希函数, 为标签, 读写器, 数据库共享	R	随机数
k	数据库端生成的随机数, 作为数据库私钥	ECC	椭圆曲线密码系统的主要参数集
k_{DP}	数据库公钥	$A=?B$	判断 A 是否等于 B
$A \leftarrow B$	B 替代 A	\parallel	连接符

3.2.1 注册阶段

注册阶段的具体过程如图 3.2 所示。

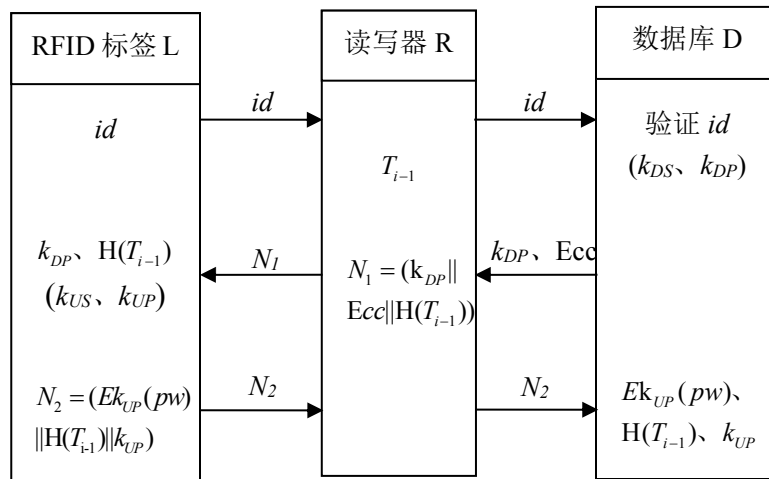


图 3.2 注册阶段示意图

注册阶段的具体步骤如下：

(1) RFID标签将自己的 id 作为注册请求信息，发送给RFID读写器，RFID读写器接收到注册请求后，主动获取当前系统时间作为时间戳 T_{i-1} 并存储，而后将标签发送来的 id 转发给数据库。

(2) 数据库接收到 id 之后，查看已有的注册列表，判断此标签是否已经注册，如果发现有相同的 id ，停止注册，若没有该 id 则数据库保存该 id ，而后生成一条安全椭圆曲线 $E(GF(2^m))$ ，在上面选取一个基点 $P(x_P, y_P)$ ，随后产生一个随机数 $k \in Z_q^*$ 作为自己的私钥 k_{DS} ，同时计算 $k_{DP} = kP$ ，作为自己的公钥，而后将 k_{DP} 以及 $E(GF(2^m))$ 、 P 点发给读写器。

(3) 读写器接收到来自数据库的消息后，对 T_{i-1} 进行一次哈希运算，而后连同 k_{DP} 和ECC组成 N_1 ，即 $N_1 = (k_{DP} || ECC || H(T_{i-1}))$ ，发送给标签。

(4) 标签在收到由读写器转发来的 N_1 后，将 $H(T_{i-1})$ 以及数据库的公钥保存在标签中，而后根据椭圆曲线相关参数生成自己的私钥 k_{US} 和公钥 k_{UP} ，通过自己的私钥对自己的唯一标识认证码进行加密并复制存储，具体加密方法与椭圆曲线公钥加密方法一致，之后连同 $H(T_{i-1})$ 以及标签公钥组成消息 N_2 ，即 $N_2 = (Ek_{UP}(pw) || H(T_{i-1}) || k_{UP})$ ，发送给读写器。

(5) 读写器将消息 N_2 转发给数据库端，数据库端在接收到消息 N_2 后，拆解消息并存储 $Ek_{UP}(pw)$ 、 $H(T_{i-1})$ 、 k_{DP} 。

3.2.2 认证阶段

在注册成功后，标签在与数据库服务器进行通信之前就必须首先通过认证，具体的认证过程见图 3.3 所示。

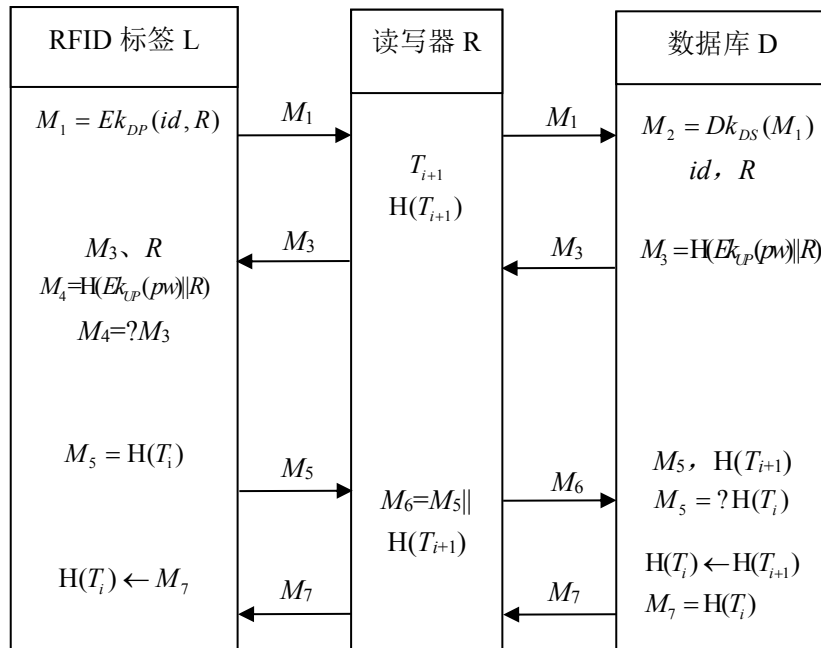


图3.3 认证阶段示意图

具体的认证过程如下：

(1) RFID标签产生一个随机数 R ，并将其与 id 通过数据库的公钥加密之后生成消息 M_1 ，即 $M_1 = Ek_{DP}(id, R)$ 。经RFID读写器发送给数据库服务器，当读写器端接收到消息后，提取出当前系统时间作为时间戳 T_{i+1} ，对其进行一次哈希运算 $H(T_{i+1})$ 并存储。

(2) 数据库服务器使用私钥进行解密，得到 $M_2 = Dk_{DS}(M_1)$ 。提取 id 和随机数 R ，而后查询该 id 绑定的 $Ek_{UP}(pw)$ 以及 $H(T_{i-1})$ 。

(3) 数据库端将 $Ek_{UP}(pw)$ 与随机数 R 连接起来，进行一次哈希运算得到 M_3 ，即 $M_3 = H(Ek_{UP}(pw)||R)$ 。而后将其传送给读写器。

(4) 标签端接收到由读写器转发来的消息后，获取信息 M_3 和随机数 R ，而后将存储的经自己公钥加密的唯一标识认证码与 R 一起进行一次哈希运算得到信息 $M_4 = H(Ek_{UP}(pw)||R)$ ，验证 M_3 和 M_4 是否相等，若相等则证明数据库服务器为合法，否则，终止与数据库服务器通信，此次认证失败。

(5) 若数据库服务器合法，则标签端提取存储的 $H(T_i)$ ，作为消息 M_5 ，即 $M_5 = H(T_i)$ 。而后将消息 M_5 发送给读写器，读写器在收到消息后，添加上暂存的 $H(T_{i+1})$ 组成 $M_6 = M_5||H(T_{i+1})$ 并发送给数据库端。

(6) 数据库接收到消息 M_6 后，拆解得到消息 M_5 ，比较里面信息与自己所存储的 $H(T_i)$ 是否相等。若相等则证明标签为合法，将 $H(T_i)$ 更新为 $H(T_{i+1})$ 作为新的 $H(T_i)$ 存储，而后将其作为消息 M_7 发送给标签端。否则，数据库终止与标签的通信，此次认证失败，认证过程结束。

(7) 标签端收到消息 M_7 后，更新标签中的时间戳 $H(T_i)$ ，至此认证成功。

3.3 协议性能分析

3.3.1 可行性分析

(1) RMA SBEO是针对RFID系统环境设计，方案中采用了椭圆曲线公钥密码算法对认证中的关键信息进行加密保护，该密码算法密钥尺寸和系统参数较小，所耗费的存储空间也较小，处理运算速度快，同时ECC具有每比特最高的安全强度^[31]。适用于计算资源、存储资源有限的RFID认证环境，具备可靠、轻量的加密功能。

(2) RMA SBEO是基于OTP即一次性口令认证进行的设计改进，本方案继承了OTP方案的方便快捷的优点。在此基础上，本文的认证协议在以下三点进行了改进：

(a) 采用了具有轻量级性质的椭圆曲线公钥加密算法，对认证过程中的信息进行加密保

护, 不同于之前的OTP中交互信息为明文传输;

(b) 为标签设置了一个唯一的验证标识 pw , 将其作为认证口令因子, 摒弃了OTP认证机制中, 用户端通过口令生成算法才能生成认证口令, 简化了口令产生过程;

(c) 有别于传统的OTP方案, RMASBEO没有采用Hash函数迭代的方法, 只是在认证过程中使用了简单的Hash计算, 简化了认证过程的计算量, 同时也避免的小数攻击。

综上所述, RMASBEO符合计算和存储资源有限的RFID系统环境的安全认证需求。

3.3.2 安全性分析

RMASBEO是基于RFID系统分析及已有认证协议研究提出的, 现对协议的安全分析如下:

(1) 双向认证

数据库服务器端接收到由标签端发送的随机数 R 后, 将其与该端存储的 $Ek_{UP}(pw)$ 进行哈希运算, 发送给标签端, 标签接收到消息后, 对自己的标识用标签公钥加密, 同样与 R 进行哈希运算, 若二者结果相同, 则服务器端合法。类似的数据库端通过对 $H(T_i)$ 进行验证, 判断标签是否合法, 至此两端双向认证结束。

(2) 信息机密性

RMASBEO认证协议中采用了椭圆曲线加密算法对认证信息进行加密, 认证过程中传输的信息不是明文传输, 而是加密后传输, 这保证了敏感信息不被外界窃取和篡改。而且, 标签的唯一标识验证码也是经过标签公钥进行加密后存储在数据库端, 除了标签本身之外, 其他人无法得知该唯一标识验证码, 保证了标签信息的机密性。

(3) 防止小数攻击

本认证协议没有采用OTP认证协议中哈希迭代的方法来实现认证, 因此攻击者无法通过修改迭代次数来实现小数攻击。认证方案中只是引进了一个随机数, 但随机数是通过加密进行传输的, 攻击者无法获得, 至此, 小数攻击无法实施。

(4) 前向安全性

在本协议中引入了Hash函数, 如标签和数据库在认证时对 $Ek_{UP}(pw)$ 和随机数 R 进行哈希运算, 以及作为认证因子之一的时间戳 T_i 也是经过哈希运算之后存储。标签中不持有之前的认证信息和作废的时间戳, 假如攻击者得到了当前的时间戳 T_i , 由于时间戳 T_i 已经过Hash计算, 因此攻击者无法计算出之前失效的时间戳, 并且就算攻击者获得了以往的认证信息, 也无法恢复进行Hash运算之前的 $Ek_{UP}(pw)$ 和随机数 R 。因此, 本协议具有前向安全性。

(5) 后向安全性

由于在认证过程中引入了随机数 R ，即使攻击者窃取了当前的认证信息 $Ek_{UP}(pw)$ 和 R ，由于 R 是通过随机函数随机产生，每两个随机数之间没有任何联系，所以攻击者根本无法通过其计算出下一轮的认证口令，因此方案具有后向安全性。

(6) 拒绝假冒攻击

假设攻击者准备假冒数据库服务器与标签进行认证，标签通过数据库的公钥对随机数 R 进行加密，但是攻击者无法得到数据库的私钥进行解密，只能自己产生一个随机数 R' 与 $Ek_{UP}(pw)$ 进行哈希运算后发送给标签端，在标签端收到消息后，用正确的随机数 R 再次进行哈希运算后，二者结果不同，从而中端认证通信，攻击者假冒数据库服务器失败。

假设攻击者假冒标签，与数据库进行认证，由于作为认证因子的时间戳 T_i 是经过加密传输，攻击者无法获得，故无法与数据库进行认证，至此，攻击者假冒攻击失败。

(7) 拒绝重放攻击

由于每次进行认证时，标签产生的随机数都不相同，即使攻击者截获了之前的认证信息 M_4 ，将其发送给标签进行认证，标签根据当前的随机数 R 与 $Ek_{UP}(pw)$ 进行哈希运算后，二者结果不同，认证失败。与此同时，因为每次认证的时间戳也是不断变化的，即使攻击者企图使用截获的之前的时间戳与数据库端进行认证，数据库端验证该时间戳与自己当前所持有的时间戳不一致，认证失败。至此，攻击者重放攻击失败。

(8) 拒绝跟踪攻击

认证协议中引入了随机因素即随机数 R ，在每次认证过程中，标签中的 R 都是随机生成，彼此之间没有任何联系，所以即使攻击者先后截获了两次认证消息 M_1 ，由于两次采用的随机数之间没有任何联系，攻击者无法通过分析两次消息之间的联系来追踪标签位置信息，同时，标签的唯一标识验证码也是通过标签公钥进行加密传输的，很好的保护了标签隐私信息。

根据上述对RMASBEO做出的安全性分析，RMASBEO与参考文献中同是基于ECC的认证协议的安全性能进行比较后，结果如表3.2所示。

表3.2 各认证方案安全性能比较

方案 安全性	文献 11	文献 12	文献 13	文献 14	文献 15	RMASBEO
双向性	√	√	√	○	√	√
机密性	○	√	√	√	√	√
前向安全	√	○	√	○	√	√
后向安全	√	√	√	√	√	√
拒绝假冒攻击	○	√	○	○	○	√
拒绝重放攻击	○	√	○	√	√	√
抵抗跟踪攻击	○	○	○	○	○	√

√: 表示满足该安全性 ○: 表示不满足该安全性

3.3.3 效能性分析

将新协议与同样基于 ECC 算法的认证协议做计算量和存储量方面的比较, 结果如表 3.3 所示。其中 h 、 r 、 e 、 s 、 x 、 g 分别表示哈希函数、随机数生成函数、ECC 加解密函数、串联操作、异或运算、获取时间戳操作, 一般的我们认为: 获取时间戳操作与串联操作属于同一运算量级; N_1 和 N_2 分别表示标签个数和 RFID 读写器个数, N_1 远远大于 N_2 。

由表中可以看出, 本协议中标签的计算量有明显的降低, 而除文献[14]外, RFID 读写器的计算量相比也有明显降低的情况, 这很好的满足了 RFID 系统中成本低、能耗资源小的要求, 虽然数据库中的计算有所增加, 这主要是因为后端数据库服务器需要在注册阶段生成安全的椭圆曲线以及密码参数, 由于后端数据库一般为大型 PC 机, 可以负担较高的计算量; 本协议中标签所需的存储量相对于其他文献来说有略微增加, 这主要是因为需存储密钥造成的, 但数据库端所需的存储空间相比于其他认证协议有大幅度降低, 这是因为其他文献中的认证协议是对 RFID 读写器进行认证, 数据库中不仅要存储标签信息, 而且还需要存储 RFID 读写器的相关认证消息, 而本协议是 RFID 标签与后端数据库服务器进行的直接认证。综合以上分析可知, 本协议在计算量和存储量上均具有一定的优越性。

表 3.3 RFID 认证协议的效能比较

认证协议	计算量			存储量		
	RFID 标签	RFID 读写器	数据库	RFID 标签	RFID 读写器	数据库
文献 11	$3h+1r+3e+3x$	$1h+3s+3x$	$O(1)$	3	1	$3N_1+2N_2$
文献 12	$2h+1r+2e+2s+2x$	$3h+1s+2e$	$O(1)$	$2+2N_2$	3	$2N_1+4N_2$
文献 13	$2h+4e+5x+2s$	$2h+1r+2s+1e$	$O(1)$	3	1	$3N_1+3N_2$
文献 14	$3h+1r+3e+2s+3x$	0	$O(1)$	4	0	$4N_1$
文献 15	$2h+1r+2e+2s$	$2h+4s+2x$	$O(1)$	3	2	$2N_1+3N_2$
本协议	$1h+1r+2e+2s$	$2h+2s+2g$	$O(N_1)$	4	1	$2N_1$

3.4 本章小结

本章中首先对经典的 OTP 认证协议进行了研究介绍，并对具有代表性的 S/Key 认证协议进行深入研究，探究了此种协议的主要认证过程，根据认证过程分析指出了该协议所面临的安全性威胁；在此基础上，提出了基于 OTP 协议，适用于资源受限的 RFID 系统环境的双向认证方案，在该方案中引入了椭圆加密算法对认证过程中的隐私消息进行加密保护，由于椭圆密码算法具有的高加密强度和轻量级特性，比较适合在 RFID 环境中使用。最后经协议整体性能分析可知，本章提出的基于 ECC 和 OTP 认证的 RFID 双向认证方案实现了 RFID 标签端和数据库服务器端的双向认证，可抵御假冒、重放、跟踪、窃听等多种恶意攻击威胁，同时该方案由于认证过程较为简练，仅使用了 Hash 函数和一次必要的加密过程，具有轻量级的特性，满足了资源受限的 RFID 环境的安全需求，由协议的效能分析进一步可以看出，本协议相较于同类型基于 ECC 算法的认证协议，协议的性能优越性较为突出。

第四章 现有密码算法轻量化分析与 ECC 轻量化改进

在物联网环境中,为了更加快捷方便的获取数据信息,其位于感知层的终端感知设备构造比较简单。一般的情况下,感知节点设备具有功能单一、携带能量少、存储空间小等特点,因其能量和资源受限,使得它们无法拥有复杂的安全保护能力,这恰恰使得恶意攻击者更能轻易的获取敏感信息,造成隐私信息泄露。具体在 RFID 系统环境中,如伪造标签等,因多数低成本标签没有使用加密,恶意攻击者很容易获取标签中信息,进行复制伪造。而轻量级器件(如 RFID 标签)有存储、价格、功耗等限制因素,现有的传统加密算法无法有效适应该限制环境,因此一些改进的轻量级加密算法应运而生,该类型的算法有效的解决了安全、应用和成本之间的协调问题,其安全模型如图 4.1 所示。

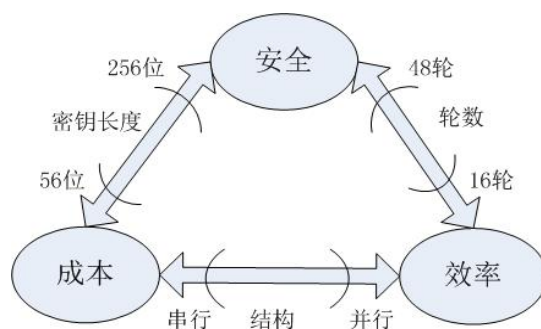


图 4.1 轻量级安全模型

4.1 现有的加密算法轻量化分析

4.1.1 对称密码算法

(1) 分组密码

现有的轻量级密码算法基于分组密码思想的较为常见,本小节简要介绍几种具有轻量化性质的分组密码算法。

DESL 算法是基于经典的 DES 密码算法改进的轻量级变体。DESL 主要是针对传统的 DES 密码算法组件进行简化,其密钥长度依然是 64bits,在保持一定安全性的基础上,使得算法整体轻量化。

轻量级分组密码 PRESENT 是一种主要面向硬件实现的超轻量级分组密码算法。PRESENT 算法分组长度为 64bits,密钥长度一般为 80bits 或 128bits,如 PRESENT-80(密钥长度为 80 bits)整体采用 31 轮的 SP 结构,该算法在硬件实现上对资源的需求很小,所以它

也被称为超轻量级密码^[32]。

ITUbee 是基于 Feistel 结构设计且面向软件实现的轻量级分组密码算法, ITUbee 的分组长度和密钥长度均为 80bits。为了减少算法运行时的功耗, ITUbee 没有密钥扩展, 但是其算法共进行了 20 轮迭代变换, 每一轮的迭代计算均需要轮常量参与异或运算, 轮常量会在算法开始之前以表格的形式存储, 算法运算过程中通过查表运算取得每一轮的轮常量, 而轮密钥则是由主密钥派生。该算法中用到的主要运算就是异或运算和查表运算, 因此运算量较小。

(2) 流密码

流密码属于对称密码算法的一种, 该算法按位或逐字节对流数据进行处理, 加解密用的是同样的密钥, 以在资源受限环境中适用性良好的 Salsa20 算法为例。

Salsa20^[33]算法是以 Hash 函数为基础进行改进设计的一种流密码算法, 其核心是一个基于 32 比特加、比特异或以及旋转操作的 Hash 函数。其密钥长度为 256bits, 可保证该算法的安全性, 而算法所采用的加法、模运算等简单操作使其算法实现运算量大为降低。但是其安全性仅基于 Hash 函数的前向安全性, 加密强度比较有限。

4.1.2 非对称密码算法

非对称密码体制近年来逐渐受到密码学研究人员的青睐, 究其原因主要是该种算法实现所消耗的能量和占用的内存空间大大低于加密强度相当的对称密码算法。同时, 在实际的数字签名和认证应用中, 非对称密码算法的优势更为明显。同样的, 在 RFID 系统环境中, 由于需要传输和加密的敏感数据较小, 我们亦可以利用轻量级非对称密码算法密钥生成和管理简单的优势, 进行相应的 RFID 标签加密、认证和鉴别数字签名操作。

(1) RSA 算法

RSA^[34]密码体制是由 Rivest、Shamir 和 Adleman 在 1977 年联合提出的。RSA 算法是公开密钥体制的典型代表, 其安全性依赖于大数的因子分解困难性, 即设 p, q 是两个互异的随机大素数, 令 $n = pq$, 欧拉函数 $\varphi(n) = (p-1)(q-1)$ 。随机选择一个大整数 d , d 与 $\varphi(n)$ 互素。但是, 现有的相关研究指出, 虽然 RSA 算法的破解难度依赖于大数分解问题的复杂度, 但无法在理论上证明二者有直接联系, 即 RSA 算法的安全强度至今没有定论。

(2) ECC 密码算法

相较于其他的非对称加密算法(如 RSA 算法), 在要求达到等量级的安全强度下, 椭圆曲线密码算法的密钥长度更短, 目前常用的 RSA 与 ECC 密钥长度比大约为 7:1^[35]。ECC 的安全基础是基于有限域上椭圆曲线点群离散对数分解问题的困难性, 该算法具体介绍已在第

二章给出，再此不在赘述。

4.1.3 现有的算法性能评估与比较

由于轻量级密码算法适用环境的特殊性，设计要求即是在保证适用性的前提下，为系统环境提供一定的安全性保护。因此，需要统一的性能评价标准对该类算法进行安全性和实用性评估比较，并将其评估结果作为如 RFID 系统等类似受限的系统环境，选择合适加密算法的参考。根据轻量级密码算法应用场景的不同，一般的将其分为面向硬件环境、面向软件环境和兼顾软硬件环境三种。因此在对不同类型算法性能进行评估比较时，所采用的评估条件和方法也有所不同。对于硬件实现，一般的评价条件包括面积，能耗，带宽，吞吐量，机器时钟周期以及等效门数（GE）等，其中，GE 基于完成一个电路功能逻辑门的数量作为统计基础，作为衡量一个数字电路的基本单位，可以用来衡量算法在硬件环境的实现性能；而对于软件实现的密码算法，主要的衡量指标有 Flash ROM、SRAM、加解密过程所耗费的时钟周期以及吞吐率等。其中，Flash ROM 主要是用来存储加解密算法的代码以及所需要的查找表等，而 SRAM 存储的是在加解密的程序运行过程中产生的中间变量，所以相对来说内存较小，而对同一明文进行加密时，根据时钟周期数亦可推出各算法运行时的吞吐率。加解密过程所需要的时钟周期长短主要用来衡量算法运行的效率，也是比较重要的一个评价指标。轻量级密码算法根据实现的软硬件环境的不同，一般可大致可分为三种，如表 4.1 所示^[36]。

表 4.1 轻量级密码分类表

类别	硬件实现	软件实现	
	等效门数(GE)	ROM(byte)	RAM(byte)
超轻量级实现	1000 内	4096	256
低成本实现	1000--2000	4096	8192
轻量级实现	2000--3000	32768	8192

对于了解算法的综合性能则需要一个综合的衡量指标，Manifavas C^[37]等人提出了一种很好的衡量指标 FOM，可以用来评价算法在硬件环境下的实现性能，FOM 具体的算法公式如（4.1）所示。

$$\text{FOM} = \text{throughput} / \text{area squared} \quad (4.1)$$

公式（4.1）中，throughput 是算法执行过程中单位时间内的资源传输率，单位为（Kb/s），area squared 是算法在实现过程中所需的硬件环境等效门数（GE）的平方。从公式中不难看出，FOM 值与算法在硬件中实现的效率成正比。

下面本文将借助以上文献[34]、[38]以及[39]的研究数据，从三个方面来总结考察上述算法的性能。一是根据各个算法 ROM 的大小来评估算法占用的内存比重，进而大致推出所需要的硬件资源和能耗量；二是评估算法运行耗费的时钟周期，考察期运行效率；最后依据综合衡量指标 FOM 给出算法的综合比较结果。

内存开销主要是考察加解密算法在编译和运行过程中，代码所占用的内存大小，主要以 ROM 和 RAM 的值作为参考；而运行效率分析则是根据加解密过程所耗费的时钟周期数进行评估，在参考了相关文献中的数据基础上，设定 CPU 的频率为 4MHz 的情况下，给出一个 256bits 的测试数据，统计出各个算法加解密过程所耗费的时钟周期数；最后根据以上所得计算出 FOM，作为综合衡量标准。具体的数据如表 4.2 所示。与此同时统计出 ROM 和 RAM 的平均值作为平均内存，加解密的平均值作为平均效率以及 FOM，绘制成柱状图，以便观察，具体如图 4.2-4.4 所示。

表 4.2 算法性能比较表

密码体制	密码算法	ROM (Bytes)	RAM (Bytes)	加密 (cycles/2 ⁵ Bytes)	解密 (cycles/2 ⁵ Bytes)	FOM	平均内存 (Bytes)	平均效率
组密码	DESL	3098	0	15759	17840	130	1549	16800
	PRESENT	1936	0	13532	26443	811	968	19987
	ITUbee	1816	20	9737	10232	608	568	9985
流密码	Salsa20	1612	36	10759	17840	275	824	14300
非对称密码	RSA	47565	658	85740	102332	13	24112	94036
	ECC	14731	172	24530	27270	359	7451	25900

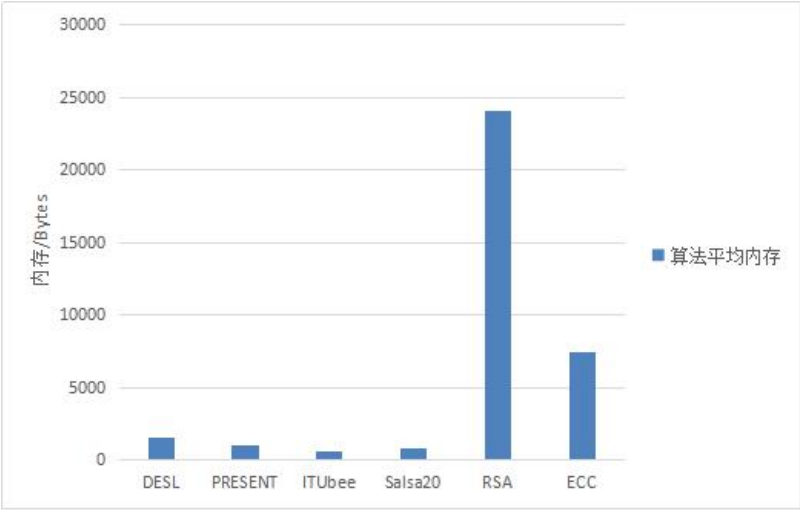


图 4.2 算法平均内存比较柱状图

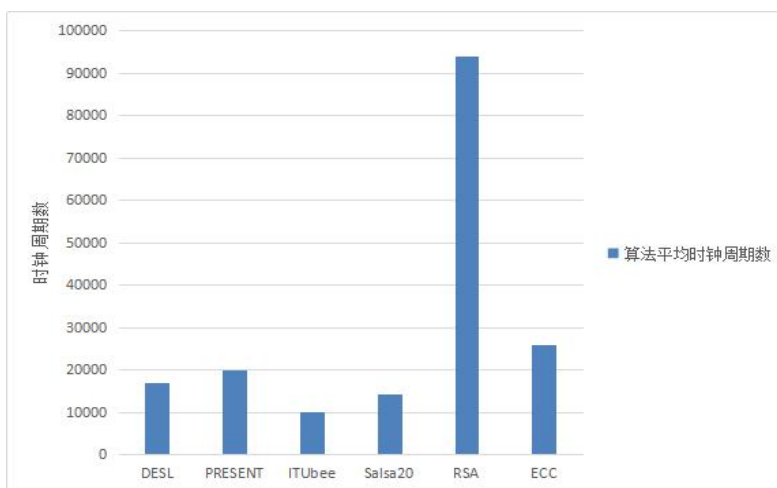


图 4.3 算法平均效率比较柱状图

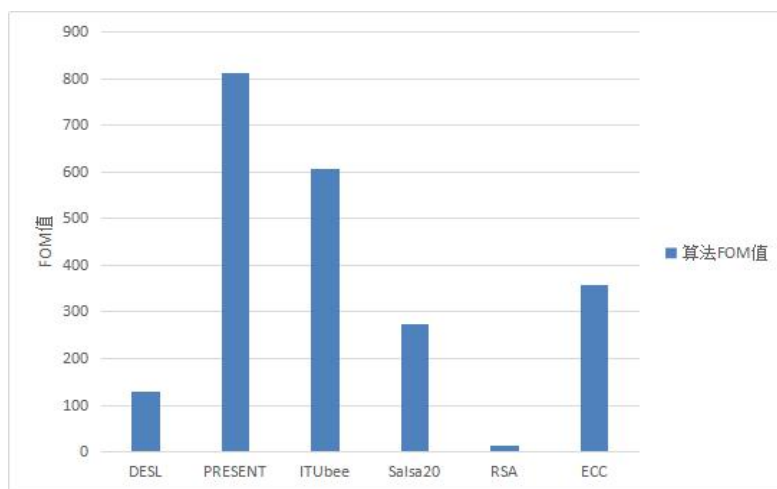


图 4.4 算法 FOM 统计比较柱状图

在上述的图表中可以看出，相对于非对称密码算法，基于对称密码算法改进和提出的轻量级算法确实比较适合资源受限的环境中。但是我们也可以看到，椭圆曲线公钥密码算法（ECC）相较于轻量级对称密码算法，亦表现出较好的轻量性和适应性，在资源受到严苛限制的环境中（如 RFID 系统），性能较同属非对称密码体制的 RSA 算法表现更为优异，由图可知，ECC 算法所占内存仅为 RSA 的 1/3，平均耗费时钟周期数仅为 RSA 的 1/4 左右，与 DES、PRESENT 时钟周期数相近，但其密码强度却是 RSA 算法的 7 倍，作为非对称加密算法的一种，安全性强度自然比对称加密算法更高。对比轻量级分类表可知，ECC 算法的性能十分接近轻量级密码算法的要求，但是其轻量性有待进一步完善改进，以期能更加适应 RFID 系统环境。

4.2 基于传统双基的椭圆曲线标量乘算法

通过第二章的椭圆曲线密码算法相关知识可知，在 ECC 算法进行加解密的过程中，椭圆

曲线上点群 G 中的标量乘计算, 即 $q = mp, q, p \in G, m \in Z$ 是必要且关键的的运算过程, 该运算过程所消耗的时间效率极大影响了整体 ECC 的算法效率。因此针对 ECC 算法的轻量化改进, 很大程度是上针对标量乘计算过程的优化与改进, 传统的标量乘计算过程主要是包括点加和倍点两种点运算。现有的相关研究工作主要关注点有两种: 一是将整数 m 基于某种形式展开表示, 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; 第二种是以空间换取时间, 通过牺牲一定的存储空间进行预计算, 省去标量乘计算过程中的复杂度, 例如滑动窗口法^[40]及结合 NAF 方法^[41]的 w-NAF 窗口法^[42]等都是基于这种思想的算法。但是我们这里主要考虑对 ECC 进行轻量化改进, 并将 ECC 运用到资源受限的环境中, 不宜采用预计算的方式, 所以, 本文研究的是基于第一种思想, 即为 m 寻求合适的展开式, 控制展开式中非零元素个数。

4.2.1 双基链表示

一个整数的双基链展开式是基于其能被双基表示而得。最早的双基系统是由 Dimitrov^[43]提出, 并给出了双基系统的性质和稀疏性证明, 而后文献^[44]中将双基系统应用到了椭圆曲线中。根据 Weger^[45]提出的 s -整数的定义, 即一个整数 s -能够被分解为多个素因子, 其最大的素因子不会超过第 s 个。则 $n = a_1^{e_{1i}} a_2^{e_{2i}}$, a_1, a_2 互为质数, $e_{1i}, e_{2i} \in \mathbb{N}$, 形如整数 n 的即为 2-整数。依据此定义, 取 $a_1=2, a_2=3$, 给出一般传统双基表示的定义。如公式 (4.2) 所示。

$$n = \sum_{i=1}^r s_i 2^{b_i} 3^{t_i}, s_i \in S, b_i, t_i \in \mathbb{N} \quad (4.2)$$

S 集合一般的取值为 $\{1, -1\}$, 此时, 该双基表示成为有符号双基表示; 当 S 取值为 1 时, 该表示形式为整数的无符号双基系统表示。一般的我们认为任何一个整数都可以被以 2,3 为底的双基系统表示, 原因是 2,3 两个数互为质数, 根据双基系统定义可得此结论。任意整数双基表示不止一种, 但是, 规定只有基底的指数为递增数列时, 其双基表示才可以成为该整数的双基链表示。即 $n = \sum_{i=1}^r s_i 2^{b_i} 3^{t_i}, s_i \in \{1, -1\}$, 且 $b_1 \leq b_2 \leq b_3 \leq \dots \leq b_r \leq 0, t_1 \leq t_2 \leq t_3 \leq \dots \leq t_r \leq 0$, 对于某个整数的双基链计算, 可以通过现有算法得出, 如贪心算法、基于树形的算法^[46]等。贪心算法最主要的思想就是求得一个整数 $k=2^b 3^t$, 使得其最接近整数 n 。以下简要给出了贪心算法求整数 n 双基链的具体算法过程。

算法 4.1 求解整数 n 双基链的贪心算法

Input: 正整数 n , 基数 2,3 的幂次上限, 即 $\max(b_i)=b_{\max}$, $\max(t_i)=t_{\max}$

Output: 整数 n 的一条双基链, $n = \sum_{i=1}^r s_i 2^{b_i} 3^{t_i}, s_i \in \{1, -1\}$, 且 $b_1 \geq b_2 \geq b_3 \geq \dots \geq b_r \geq 0, t_1 \geq$

$t_2 \geq t_3 \geq \dots \geq t_r \geq 0$

- 1) Begin
- 2) $s_1 \leftarrow 1$ and $i \leftarrow 1$
- 3) While $n \geq 0$ do
- 4) 找到最接近整数 n 的正整数 k , 使得 $k = 2^{b_i} 3^{t_i}$, $0 \leq b_i \leq b_{\max}, 0 \leq t_i \leq t_{\max}$
- 5) $b_{\max} \leftarrow b_i, t_{\max} \leftarrow t_i$
- 6) If $b_{\max} == 0 \& t_{\max} == 0$ Break
- 7) If $n < k$, then $s_i \leftarrow -s_{i-1}, i \leftarrow i+1$
- 8) Else $s_i \leftarrow s_{i-1}, i \leftarrow i+1$
- 9) End If
- 10) End While
- 11) Return $n = \sum_{i=1}^r s_i 2^{b_i} 3^{t_i}, s_i \in \{1, -1\}$
- 12) End

在以上贪心算法的过程中, 基数 a 的最大幂次数限制一般的我们取 $\left\lceil \frac{\log_a n}{2} \right\rceil$, 在这里即

$b_{\max} = \left\lceil \frac{\log_2 n}{2} \right\rceil, t_{\max} = \left\lceil \frac{\log_3 n}{2} \right\rceil$ [47], 因为基于此极限值得到的整数 n 的双基链接近于其最短双

基链表示, 展开式中的非零元素个数也是最少的, 最大程度的简化了标量乘的计算过程。

4.2.2 基于传统双基链的标量乘算法

依据 4.2.1 节中给出的贪心算法, 可求解出任意整数的最短双基链表示, 本节将给出传统的基于基数 2、3 的双基链标量乘算法。

算法 4.2 基于基底 2、3 的双基链标量乘算法

Input: $n = \sum_{i=1}^r s_i 2^{b_i} 3^{t_i}, s_i \in \{1, -1\}$, 且 $b_1 \geq b_2 \geq b_3 \geq \dots \geq b_r \geq 0, t_1 \geq t_2 \geq t_3 \geq \dots \geq t_r \geq 0, P \in G$

Output: $nP \in G$

- 1) Begin
- 2) $Z \leftarrow s_1 P, i \leftarrow 1$
- 3) While $i < r$ do
- 4) $x \leftarrow b_i - b_{i+1}, y \leftarrow t_i - t_{i+1}$
- 5) If $(x == 0)$
- 6) If $(y == 0)$ then $Z \leftarrow Z + s_i P$
- 7) Else $Z \leftarrow 3(3^{y-1} Z) + s_i P$
- 8) End If
- 9) Else $Z \leftarrow 3^y Z, Z \leftarrow 2^{x-1} Z$
- 10) End If
- 10) $Z \leftarrow 2Z + s_i P$
- 11) $i \leftarrow i + 1$
- 12) End While
- 13) Return Z
- 14) End

具体的算法实现过程通过一个例子加以说明。表 4.3 是求解大整数 841231 的标量乘运算过程。841231=2⁷3⁸+2⁶3³-2⁵3²-2⁴3⁰-2⁰3⁰，其中， i 表示迭代次数， K_i 中存放了每次迭代后数字运算结果， s, x, y 与算法中的符号相对应。

表 4.3 841231P 运算过程表

i	$K_i P$	s_i	x	y
1	P	1	0	0
2	$486K_1P + P = 487P$	1	1	5
3	$6K_2P - P = 2921P$	-1	1	1
4	$18K_3P - P = 52577P$	-1	1	2
5	$16K_4P - P = 841231P$	-1	4	0

4.2.3 传统双基链标量乘运算量分析

在有限域范围上，算法中进行一般的常数加法或乘以一个常数运算，对整个算法的运算性能基本没有影响。我们在考察标量乘的运算量时，主要的就是针对就是求逆、平方以及乘法这三种运算，分别用 I、S、M 表示，基于此对标量乘运算量进行分析研究。根据第二章中的介绍我们知道，在椭圆曲线密码算法中，主要涉及的数学运算就是点加和倍点运算，具体的运算介绍在第二章已经给出。基本的点加和倍点运算量分别为 $1I+1S+2M$ 、 $1I+2S+2M$ ，而 $I=9M$ ， $S=0.8M$ [48]。参考已有研究文献 [49][50]，通过分析点加和倍乘计算，总结出椭圆曲线上的多种基本的点运算的运算量，如表 4.4 所示。

表 4.4 有限域上的点运算开销表

点运算	运算开销
P+Q	$1I+1S+2M$
2P	$1I+2S+2M$
2P+Q	$1I+2S+9M$
3P	$1I+4S+7M$
3P+Q	$2I+4S+9M$
5P	$1I+5S+13M$
7P	$1I+6S+20M$

基于表 4.4，可大致计算出一个整数标量乘的运算量。

如： $841231=2^73^8+2^63^3-2^53^2-2^43^0-2^03^0=2^4(2^13^2(2^13^1(2^13^5+1)-1)-1)-1$ 。

则 $841231P=[2^4](2^13^2(2^13^1([2^13^5]P+P)-P)-P)-P$ ，即完成该标量乘运算需要的倍点、三倍点以及点加运算的次数分别为 7 次、8 次和 4 次，该计算过程的运算量为 $19I+50S+78M$ 。而椭圆曲线上三倍点计算需要在倍点的基础上进行，由此可以得出，倍点运算的运算效率严重影响了整个标量乘的运算速度。在文献[51]中提出了一种新的半点运算，其运算量比传统的倍点运算小得多，利用其替代倍点运算，可明显改善椭圆曲线标量乘的运算效率，进而使得整体密码算法的运行效率得到提升。与此同时，我们在表 4.4 中也可以看出，5P 的运算量要小于分别进行一次倍点和三倍点的运算量，我们可以考虑改进传统的带符号的双基链表示，缩短其展开式长度和其中的非零元素个数，并且将半点运算引入标量乘运算中，提出了一种基于新双基的广义双基链（Extended DBNS） [52] 标量乘算法。

4.3 基于新双基的椭圆曲线标量乘算法

扩展式广义双基链思想的提出，有效减少了整数双基链展开式的冗余度，简化了标量乘运算的计算复杂度，本文的算法即是基于该广义双基链思想，并且结合了椭圆曲线中的半点

运算 (Point Halving)，在此基础上提出了一种新的双基表示，而后基于该双基表示给出了改进后的双基链标量乘算法。新的双基链表示如公式 (4.3) 所示，记为 PH-EDBNS。

$$n = \sum_{i=1}^r s_i \left(\frac{1}{2} \right)^{b_i} 3^{t_i}, \quad n, b_i, t_i \in \mathbb{N} \quad (4.3)$$

其中， $b_1 \geq b_2 \geq b_3 \geq \dots \geq b_r \geq 0, t_1 \geq t_2 \geq t_3 \geq \dots \geq t_r \geq 0$ ；有集合 $S = \{1, 5, 7, 11, \dots\}$ ，集合中元素均是 2, 3 互为素数，该集合大小不固定，如 $S_2 = \{1, 5, 7\}$ ， $S_4 = \{1, 5, 7, 11, 13\}$ ，而系数 $|s_i|$ 即取自集合 S_m 中的前 $m+1$ 个元素，即 $|s_i| \in S$ 。

4.3.1 广义双基链与半点运算

(1) 广义双基链

传统的双基数系统形如 $n = \sum_{i=1}^r s_i 2^{b_i} 3^{t_i}$ ， $s_i \in \{1, -1\}$ ，该双基表示的系数 s 的取值仅为 1 或 -1。而扩展的广义双基数系统中，主要是扩大的系数的取值范围，该型双基数系统提供了一个系数集合 S ，该集合是由与基数互质的元素组成，如在 $n = \sum_{i=1}^r s_i 2^{b_i} 3^{t_i}$ 中，系数集合 S 中元素均与 2, 3 互为素数， $|s_i| \in S$ 。这一改进可有效缩短双基链的展开长度，同时非零元素个数也随之递减，降低了计算时所需的内存冗余度，提高了标量乘的运算效率。

如大整数 841231，运用广义双基链思想所得展开式为： $841231 = 2^7 3^8 + 5 \cdot 2^5 3^2 - 2^4 - 2^0$ ，相较于 4.2.2 节中的展开式： $841231 = 2^7 3^8 + 2^6 3^3 - 2^5 3^2 - 2^4 3^0 - 2^0 3^0$ ，其展开式减少了一项，大大简化了计算，提高了运算效率。

(2) 半点运算

若椭圆曲线在有限域 $GF(2^m)$ 上具有极小 2-挠点，则具有该性质的椭圆曲线在仿射坐标下，求解半点运算的速度要比倍点运算的速度快的多，本文研究的标量乘计算正是基于具有极小 2-挠点的椭圆曲线。

有点 $P(x, y) \in E(GF(2^m))$ ，且 $P \neq -P$ ，则称运算 $Q = 2P = 2(x, y) = (\bar{x}, \bar{y})$ 为倍点运算；当已知 $Q = (\bar{x}, \bar{y}) = 2P$ ，求解 $P = \frac{1}{2}Q = (x, y)$ 的过程就被称为半点运算。由以上的定义可以看出，半点运算与倍点运算二者之间互为逆运算，但是在具有极小 2-挠点的椭圆曲线上，前者的运算效率比后者更为优异，若将标量乘中涉及的倍点运算均用半点运算代替，可极大的提高标量乘运算效率。倍点 Q 的计算过程如下所示：

$$\lambda = x + \frac{y}{x} \quad (4.4)$$

$$\bar{x} = \lambda^2 + \lambda + a \quad (4.5)$$

$$\bar{y} = x^2 + (\lambda + 1)\bar{x} \quad (4.6)$$

而现在已知 Q 点, P 点的求解步骤是在倍点运算的基础上推出的, 具体计算过程如下:

1) (4.5) 式可变形为 $\lambda^2 + \lambda + a - \bar{x} = 0$, 通过求解该方程可求得 λ 的值;

2) 将 1) 中求得的 λ 带入 (4.6) 式中, 可得 $x = \sqrt{\bar{y} - (\lambda + 1)\bar{x}}$;

3) 通过 (4.4) 式可知, $y = (\lambda - x)x$, 将上两式中求得的 λ 、 x 带入可得 y , 求解完成。

以上即可求得点 $P = \frac{1}{2}Q = (x, y)$ 。

通过分析倍点运算和半点运算的计算过程, 结合 4.2 节的研究数据, 可得出半点和倍点的基域运算量, 如表 4.5 所示。

表 4.5 半点与倍点运算量比较表

点运算	运算量
P/2	2M
P/2+Q	1I+2M
2P	1I+2S+2M
2P+Q	1I+2S+9M

从表中可以看出, 半点运算的运算量仅是倍点运算量的 20% 左右, 这为标量乘的优化改进提供了基础。

4.3.2 扩展的新双基链表示方法及标量乘算法

(1) 新双基链 (PH-EDBNS) 求解算法

设 $P(x, y)$ 为曲线 $E(GF(2^m))$ 在域 $GF(2^m)$ 上的一点, 域 $GF(2^m)$ 具有极大奇数阶 p , n 为整数, 且 $0 < n < p$, 其中 2^q 为最接近域 $GF(2^m)$ 奇数阶 p 的值, 则基于新双基的 n 双基链表示求解算法如下。

算法 4.3 n 的新双基链求解算法

Input: $n' = (2^q n) \bmod p$, $n' \neq 0 \bmod 2$, 整数集 S

Output: $n = \sum_{i=1}^r s_i \left(\frac{1}{2}\right)^{b_i} 3^{t_i}$, $n, b_i, t_i \in \mathbb{N}, |s_i| \in \mathbb{S}$, $b_1 \geq b_2 \geq \dots \geq b_r \geq 0, t_1 \geq t_2 \geq \dots \geq t_r \geq 0$

1) Begin

2) $j \leftarrow 1, d \leftarrow 1, k \leftarrow n'$

3) While $k > 0$ do

4) If $3^{l_j} \bmod k == 0, l_j > 0$ then

5) $k = \frac{k}{3^{l_j}}, t_j = t_{j-1} + l_j$

6) 找到最接近 k 的值 z , 使得 $z = s_j 2^{a_j}$, $a_j < a_{j-1}$, $s_j \in \mathbb{S}$

7) If $a_j == 0$ Break

8) $s_j \leftarrow d \times s_j$

9) If $k \geq z$ then

10) Return $k - z$

11) Else Return $z - k, s \leftarrow -s$

12) End If

13) Else $j \leftarrow j + 1$

14) End If

15) End While

16) Print $n' = \sum_{j=1}^r s_j 2^{a_j} 3^{t_j}$, $a_j < a_{j-1}$, $t_j > t_{j-1}$, then

17)
$$n = \frac{n'}{2^q} = \frac{\sum_{j=1}^r s_j 2^{a_j} 3^{t_j}}{2^q} = \sum_{j=1}^r s_j \left(\frac{1}{2}\right)^{(q-a_j)} 3^{t_j} \bmod p$$

18) 令 $q - a_j = b_i$, $j = r - i + 1$, then

19) Print $n = \sum_{i=1}^r s_i \left(\frac{1}{2}\right)^{b_i} 3^{t_i}$, $n, b_i, t_i \in \mathbb{N}, |s_i| \in \mathbb{S}, b_1 \geq b_2 \geq b_3 \geq \dots \geq b_r \geq 0, t_1 \geq t_2 \geq t_3 \geq \dots \geq t_r \geq 0$

20) End

新双基链求解算法是以贪心算法为基础, 在算法的第 6 步就是利用贪心算法的思想找到 Z , 从第 6 步到 16 步得到 n' 亦是采用的贪心算法求解双基链的思想; 在得到 n' 类双基链表示

之后，17步 n' 除 2^q 从而得到了原始的整数 n ；接下来进行指数坐标替换，即 $q - a_j = b_i$, $j = r - i + 1$ ，该步实际上就是将基数 3 项倒转，而在第 17 步 n' 除 2^q 时， n' 的类双基链中基数 2 的项数已经被倒转，经 17、18 步之后得到的 n 的新双基链表示中，基数的指数项自然实现了严格的递减序列，符合双基链的定义。由算法的求解过程可知， n' 的类双基链表示求解算法利用的是贪心算法，链长 r 一定是一个确定存在的值，这也证明了新双基链算法的有穷性和合理性。

以大整数 314159 为例，即 $n = 314159$ ，给定二进制域 $GF(2^m)$ 的极大奇数阶 p 为 314161，则最接近 p 的 2 的幂次数为 2^{18} ，依据算法 4.3，计算可得 $n' = (2^{18} \times 314159) \bmod 314161 = 104034$ ，整数 n 的新双基链求解过程如表所示。其中，Step 表示算法步骤，Operation 表示每次进行的主要操作， K 是每次迭代后的值。

表 4.6 314159 的 PH-EDBNS 求解过程表

Step	Operation	K
0		104034
1	/3	3(34678)
2	$z \leftarrow 2^{15}$	$3(2^{15} + 1910)$
3	$z \leftarrow 2^{11}$	$3(2^{15} + (2^{11} - 138))$
4	/3	$3(2^{15} + (2^{11} - 3(46)))$
5	$z \leftarrow 7(2^3)$	$3(2^{15} + (2^{11} - 3((7(2^3) - 10))))$
6	$z \leftarrow 5(2^1)$	$3(2^{15} + (2^{11} - 3((7(2^3) - (5(2^1))))))$
n' 的类双基链		$2^{15}3^1 + 2^{11}3^1 - 7 \times 2^3 3^2 + 5 \times 2^1 3^2$
类双基链翻转		$5 \times 2^1 3^2 - 7 \times 2^3 3^2 + 2^{11} 3^1 + 2^{15} 3^1$
$n = n' / 2^{18}$		$5 \times \left(\frac{1}{2}\right)^{17} 3^2 - 7 \times \left(\frac{1}{2}\right)^{15} 3^2 + \left(\frac{1}{2}\right)^7 3^1 + \left(\frac{1}{2}\right)^3 3^1$

这里系数集合 $S_2 = \{1, 5, 7\}$ ，因系数集合 S 的大小不定，如当 $S_1 = \{1, 5\}$ 时，314159 的双基链表示则为： $314159 = (-5) \times \left(\frac{1}{2}\right)^{17} 3^3 + 5 \times \left(\frac{1}{2}\right)^{14} 3^3 + 5 \times \left(\frac{1}{2}\right)^{10} 3^1 + \left(\frac{1}{2}\right)^3 3^1$ ，由此可以看出，选取的系数集合不同，对标量乘的算法效率也有一定影响。

(2) 改进的基于新双基链的标量乘算法

通过算法 4.3 可以求得任意整数 n 的基于新基数 $\frac{1}{2}$ 、3 的扩展双基链表示，以下是该整数

在新双基链表示下进行的标量乘算法。

算法 4.4 新双基链标量乘算法

Input: $n = \sum_{i=1}^r s_i \left(\frac{1}{2}\right)^{b_i} 3^{t_i}$, $n, b_i, t_i \in \mathbb{N}$, $|s_i| \in \mathbb{S}$, $P \in E(\mathbb{F}_{2^n})$

Output: $nP \in E(\mathbb{F}_{2^n})$

- 1) Begin
- 2) $Z \leftarrow s_1 P$, $i \leftarrow 1$
- 3) While $i \leq r$ do
- 4) $x \leftarrow b_i - b_{i+1}$, $y \leftarrow t_i - t_{i+1}$
- 5) If $(x == 0)$
- 6) If $(y == 0)$ then $Z \leftarrow Z + s_i P$
- 7) Else $Z \leftarrow 3(3^{y-1} Z) + s_i P$
- 8) End If
- 9) Else $Z \leftarrow 3^y Z$, $Z \leftarrow \left(\frac{1}{2}\right)^{x-1} Z$
- 10) End If
- 11) $Z \leftarrow \left(\frac{1}{2}\right) Z + s_i P$
- 12) $i \leftarrow i + 1$
- 13) End While
- 14) Return Z
- 15) End

(3) 新的双基链标量乘运算复杂度分析

为了方便分析整个算法的运算量，将运算 $P/2$ 、 $P/2+P$ 、 $P+Q$ 、 $2P$ 、 $3P$ 、 $3P+Q$ 分别记为 H、HA、A、D、T，TA。根据表 4.4、4.5 可知，HA 的运算量要比 H 和 A 的运算量之和小，所以在计算中涉及点加运算的时候，都用 HA 来代替，以减少计算量。通过分析算法 4.4 的过程可以看出，该算法一共需要迭代运行 $r-1$ 次，第 i 轮迭代的运算量为：

$$W_i = \delta_{x_i,0} \left[\delta_{y_i,0} T + (1 - \delta_{y_i,0}) ((y_i - 1)T + TA) \right] + (1 - \delta_{x_i,0}) \left[\delta_{x_i,0} H + (x_i - 1)H + HA \right], \text{ 其中 } \delta_{i,j} = \begin{cases} 1; & i=j \\ 0; & i \neq j \end{cases};$$

则总运算量 $W = \sum_i^r W_i$ 。

现已以 (1) 节中的 314159 为例进行分析, 在第 (1) 节中已经求得整数 314159 的新双基链表示, 其中 S 集合取的是 $S_2 = \{1, 5, 7\}$, $314159 = 5 \times \left(\frac{1}{2}\right)^{17} 3^2 - 7 \times \left(\frac{1}{2}\right)^{15} 3^2 + \left(\frac{1}{2}\right)^7 3^1 + \left(\frac{1}{2}\right)^3 3^1$, 则根据算法 4.4 新的标量乘运算, 314159P 运算过程及运算量:

$$314159P = \left(\frac{1}{2}\right)^4 3^0 \left(\left(\frac{1}{2}\right)^8 3^1 \left(\left(\frac{1}{2}\right)^2 3^0 (5P) - 7P \right) + P \right) + P$$

其中, 该标量乘运算共需要进行 14 次 H 运算, 1 次 T 运算和 3 次 HA 运算, 涉及的 5P 和 7P 运算, 在文献[53]、[54]中已经给出了快速计算公式。具体如表所示。

其中 i 是运算迭代轮数, W_i 是每一轮的运算量, Total 指的是总的运算量, 每一轮的运算量计算是基于表 4.4、4.5 的数据。

表 4.7 求解 314159P 运算量表

i	s_i	x	y	Z	W_i
1	5	0	0	5P	1I+5S+13M
2	-7	2	0	$\left(\frac{1}{2}\right)^2 3^0 (5P) - 7P$	2I+6S+24M
3	1	8	1	$\left(\frac{1}{2}\right)^8 3^1 \left(\left(\frac{1}{2}\right)^2 3^0 (5P) - 7P \right) + P$	2I+4S+25M
4	1	4	0	$\left(\frac{1}{2}\right)^4 3^0 \left(\left(\frac{1}{2}\right)^8 3^1 \left(\left(\frac{1}{2}\right)^2 3^0 (5P) - 7P \right) + P \right) + P$	1I+8M
Total				6I+15S+70M	

而依照传统的双基链表示, $314159 = 2^{12}3^4 - 2^{11}3^2 + 2^83^1 + 2^43^1 - 2^03^0$, 相应的 314159P 为:

$314159P = 2^43^1 \left(2^43^0 \left(2^33^1 \left((2^13^2)P - P \right) + P \right) + P \right) - P$ 。其进行了 12 次 D 运算, 4 次 T 运算以及 4 次 A 运算, 则该过程中的总运算量为 20I+44S+60M, 将 I、S、M 统一按比例换算成 M 时, 总运算量为 275.2M, 而相应的基于 PH-EDBNS 标量乘算法总运算量为 136M, 仅为传统双基链标量乘运算量的 50%左右, 可见新的双基链表示有着高效的运算性能。

基于以上基本的运算量分析, 本文在 NIST B-163、NIST B-233 和 NIST B-283 三种椭圆曲线上选取 1000 组临近有限域奇数阶的大整数 n 进行实验比较, 利用 NAF、传统双基表示以及 PH-EDBNS 进行标量乘计算, 统计出各个底层的运算量, 如表 4.8 所示。

表 4.8 三种标量乘算法运算量比较表

曲线	算法	n/bits	H	HA	A	D	DA	T	TA	运算量 (M)
NIST B-163	NAF	160	—	—	81	141	112	—	—	2156
	DBNS	160	—	—	136	172	164	183	214	2360
	PH-E DBNS	160	37	84	84	—	—	132	165	1685
NIST B-233	NAF	233	—	—	152	236	197	—	—	3381
	DBNS	233	—	—	225	276	251	231	279	3652
	PH-E DBNS	233	68	116	116	—	—	166	237	2436
NIST B-283	NAF	283	—	—	243	292	257	—	—	4148
	DBNS	283	—	—	316	365	298	283	322	4682
	PH-E DBNS	283	134	185	185	—	—	216	253	2886

从表中我们可以看出，基于 PH-EDBNS 进行标量乘运算过程中，我们将其中涉及的 D 运算换成了 H 运算，同时，用 HA 运算代替了所有的 A 运算，并且由于三倍点计算中也会用到倍点计算，在对倍点运算做相应替换后，PH-EDBNS 中的 T 运算与 TA 运算量也随之得以优化，这大大降低了总的运算量。具体的在曲线 NIST B-163 上，基于 PH-EDBNS 算法运算量比基于 NAF 标量乘算法提高了 22%，比 DBNS 算法提高了 29%；在曲线 NIST B-233 上该算法比其他两种算法依次提高了 28%与 34%；而在曲线 NIST B-283 上性能更为优异，分别比 NAF 算法和 DBNS 算法提高了 31%与 38%。这说明随着正整数 n 比特长度的增加，基于改进后的新双基链标量乘算法的优越性能表现越来越突出。图 4.5 显示的是整数 n 在多个比特长度下三种算法标量乘运算量，随着比特长度的增大，效率提高程度有逐渐增大的趋势。

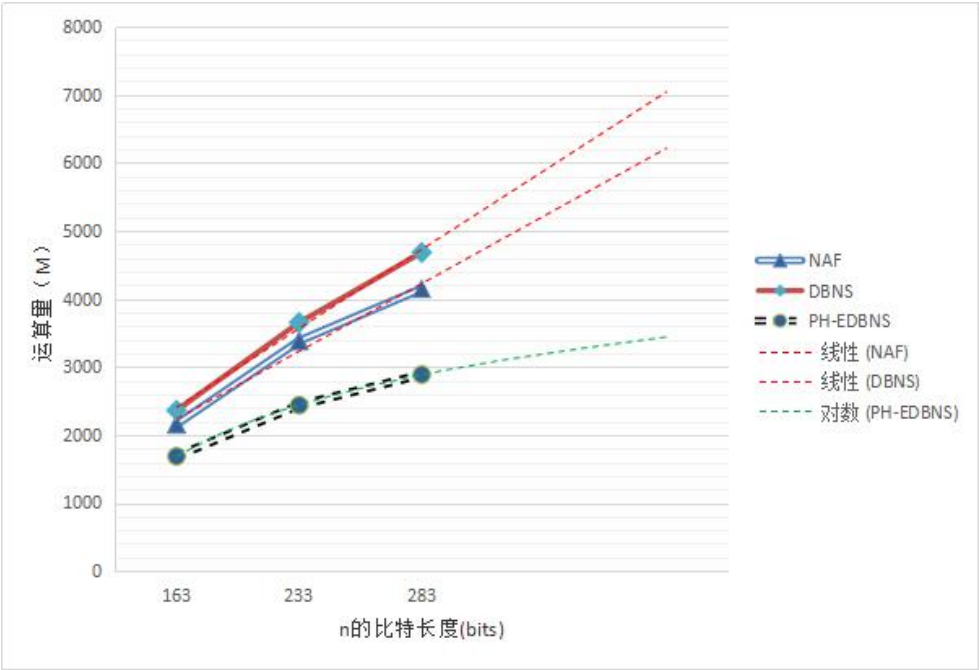


图 4.5 算法运算量比较图

4.3.3 改进后 ECC 算法与其他算法性能比较

在 4.1 节中，本文比较了 ECC 算法与其他几种典型算法的轻量化，本节将改进后的 ECC 算法与 4.1 节中提到的算法再次进行比较，并统计观察比较结果。同样在设定 CPU 的频率为 4MHz 的情况下，给出一个 256bits 的测试数据，统计出各个算法加解密过程占用内存、耗费的时钟周期数以及 FOM 值。在 4.1 节统计数据的基础上，绘制成统计柱状图，具体如图 4.6-4.8 所示。

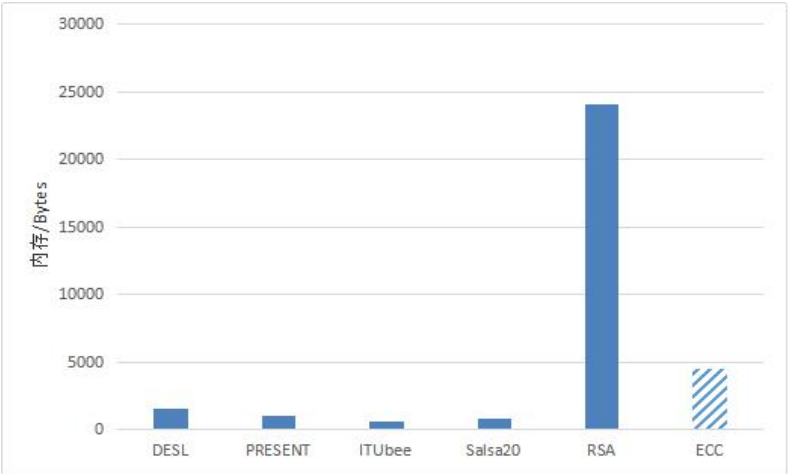


图 4.6 改进 ECC 算法与其他算法内存比较图

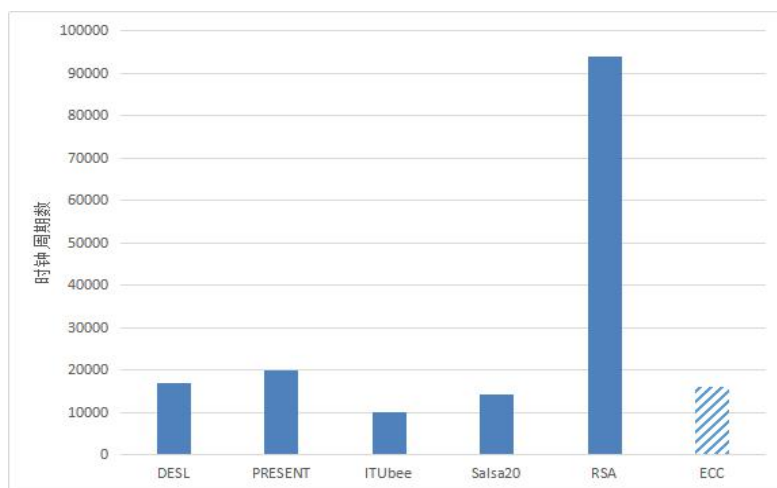


图 4.7 改进后 ECC 算法与其他算法时钟周期比较图

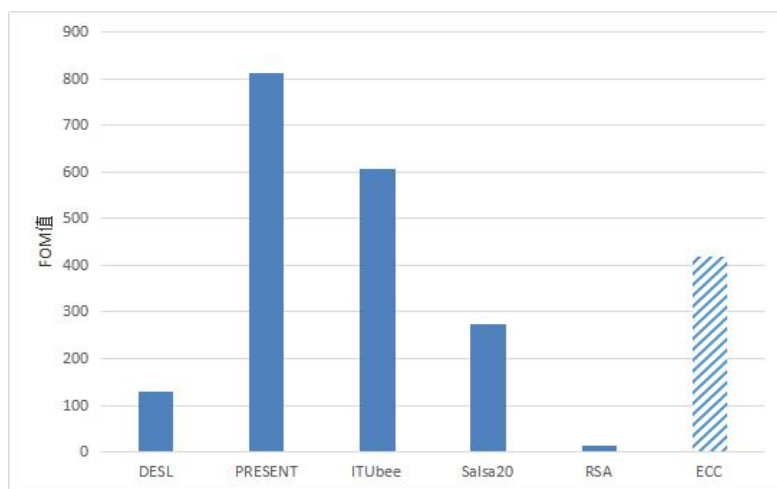


图 4.8 改进后 ECC 算法与其他算法 FOM 比较图

由统计图可以看出，改进后的 ECC 算法，在运行时占用内存情况比未改进时有明显的降低趋势，尽管对比其他对称密码算法占用的内存依旧较多，但已有较大改善；而由运行时耗费的时钟周期数统计图可以看出，改进的 ECC 算法甚至已比对称密码算法中的 DESL 算法和 PRESENT 算法运行更快，这显示出 ECC 算法改进后的良好效果；根据统计出的改进后的 ECC 算法 FOM 值的增长情况可以看出，其算法运行效率明显提高，优于对称密码算法中的 DESL 算法。综合以上分析可知，改进后的 ECC 算法尽管在内存占用问题优势并不突出，但其运行效率有明显提高，基本达到了改进 ECC 算法底层运算效率的目的。

4.4 本章小结

在本章中，首先研究了现有的轻量级加密算法，对各种经典的轻量级算法进行了简要介绍，并对各种算法的轻量化性能进行分析比较；而后针对椭圆加密算法展开深入的研究，主要是对椭圆加密算法中的标量乘运算进行改进，在研究了现有的基于传统基数 2,3 的双基链系统以及半点运算之后，将计算量更小的半点运算引入双基系统，提出了一种新的扩展双基表示方法—PH-EDBNS，并以此提出了新的双基链生成算法和基于该双基链表示的标量乘算法，通过具体分析新的标量乘算法的运算量，以及与原有的 DBNS 和 NAF 算法进行比较后，基于 PH-EDBNS 的标量乘算法运算效率更为优异，提高了原有椭圆曲线加密算法的轻量化性能。将改进后的 ECC 算法与其他典型的密码算法比较后可以看出，ECC 算法在改进后有较好的运行效率。

第五章 RFID 双向认证协议正确性证明与实现

第三章中在研究了 OTP 认证协议模型的基础上,提出了一种适用于 RFID 系统环境的基于 ECC 加密算法的双向认证协议——RMASEBEO,在该双向认证协议中,引入了具有轻量级性质的椭圆加密算法,对认证过程中的敏感信息进行加密,以保证认证过程的安全性,但传统的 ECC 加密算法轻量级程度有限,依然未能达到资源受限的 RFID 系统环境适用性需求,该算法还需要进一步的轻量化改进;因此在第四章中,对椭圆曲线加密算法过程进行了详细分析,针对 ECC 算法加解密过程中涉及的关键性运算也即标量乘进行优化改进;本章主要是利用典型的模态逻辑化验证方法——BAN 逻辑来证明认证协议的正确性,并在此基础上对该认证协议进行验证性实现探究。

5.1 认证协议正确性证明

5.1.1 BAN 逻辑

BAN 逻辑^[55]是一种基于已有规则和信念的推理验证逻辑,被广泛应用于安全协议的推理证明中。该逻辑的主要思想是以主体信念为基础,结合逻辑规则,从已知信念中推出新的信念。BAN 逻辑的应用过程:根据协议过程,将协议过程抽象成逻辑公式,并对协议条件作出逻辑假设,然后依据假设和逻辑公式,应用 BAN 逻辑的语法规则进行推理,直至推导出需要验证的结果,则表明该安全协议在逻辑上是正确可行的。

依据 BAN 逻辑中的规则而定, P , Q 分别代表安全协议的主体变量, K 为协议中的密钥(公钥)变量,若是在公钥密码体制中, K^{-1} 则代表了对应的私钥变量, A, B 表示逻辑中的公式变量,则 BAN 逻辑的具体语法和主要推导规则如下。

(1) BAN 逻辑的语法规则

$P \models A$: P 信任 A , 即 P 相信变量 A 是真实有效的。

$P \sim A$: P 曾经发送过变量 A 。

$P \triangleleft A$: 变量 A 对 P 是可见的, 即 P 曾经接收过变量 A , 同时 P 可以读出 A 的内容。

$P \models A$: P 决定变量 A 的正确与否。

$\#(A)$: 变量 A 是新鲜的。

$\{A\}_k$: 密钥 K 对变量 A 加密后的密文表示。

$\langle A \rangle_B$: 变量 A 与变量 B 的连接表示。

$P \xrightarrow{K} Q$: 密钥 K 仅为主体 P 与 Q 共享。

$\vdash \xrightarrow{K} P$: K 是主体 P 的公钥。

$P \stackrel{K}{\leftrightarrow} Q$: K 是主体 P 和 Q 之间共享的私密信息, 其他主体无从得知 K 的内容。

(2) BAN 逻辑的主要推导规则

在下列规则公式中, 只要满足了横线上半部分的公式条件, 即可推出下半部分是成立的, 根据此规则进行之后的逻辑推导证明。

共享密钥消息规则:

$$\frac{P \models Q \xleftarrow{K} P, P \triangleleft \{A\}_k}{P \models Q \sim A} \quad (5.1)$$

临时值检测规则:

$$\frac{P \models \#(A), P \models Q \sim A}{P \models Q \models A} \quad (5.2)$$

管辖规则:

$$\frac{P \models Q \Rightarrow A, P \models Q \models A}{P \models A} \quad (5.3)$$

新鲜性规则:

$$\frac{P \models \#(A)}{P \models \#(A, B)} \quad (5.4)$$

信任规则:

$$\frac{P \models (A, B)}{P \models A} \quad (5.5)$$

$$\frac{P \models Q \sim (A, B)}{P \models Q \sim A} \quad (5.6)$$

消息接受规则:

$$\frac{P \models P \xleftarrow{K} Q, P \triangleleft \{A\}_k}{P \triangleleft A} \quad (5.7)$$

$$\frac{P \triangleleft (A, B)}{P \triangleleft A} \quad (5.8)$$

补充规则^[56]:

$$\frac{P \models Q \mid \sim E(A_1, A_2, \dots, A_n), P \triangleleft A_1, P \triangleleft A_2, \dots, P \triangleleft A_n}{P \models Q \mid \sim (A_1, A_2, \dots, A_n)} \quad (5.9)$$

5.1.2 协议正确性证明

本节将根据以上小节中列出的 BAN 逻辑语法规则和推导规则，结合 RFID 双向认证协议对应的 BAN 逻辑的形式化假设语句进行验证推导，以期最终推导出预期目标公式，从而证明该协议是正确可行的。

BAN 逻辑推导步骤流程如图 5.1 所示：

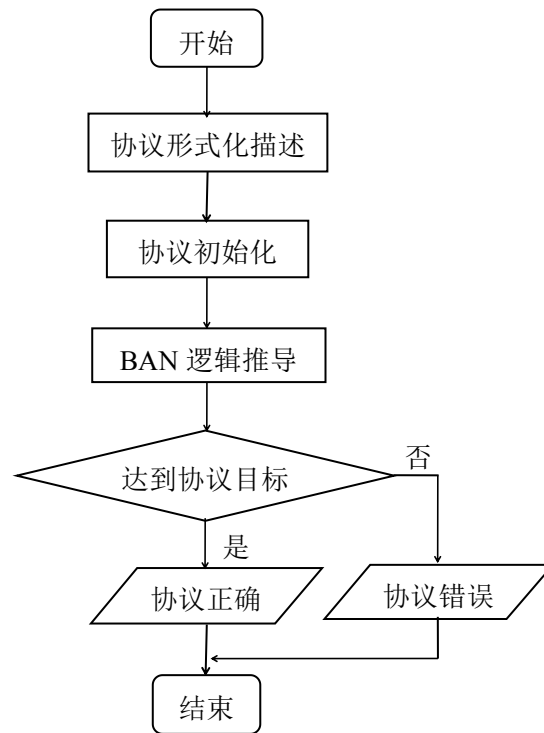


图 5.1 BAN 逻辑推导步骤流程图

具体步骤如下：

(1) 分析协议过程，以此建立理想的形式化逻辑分析模型，而后将协议主要认证过程抽象为符合 BAN 逻辑语法规则的符号表示。

(2) 依据协议内容进行合理的初始化假设，并使用 BAN 逻辑语言描述协议初始化，形

成协议的初始化假设集合。

(3) 通过分析协议具体过程, 得出协议正确性所要达到的预期目标, 并以形式化符号表示。

(4) 根据 BAN 逻辑的推导规则, 结合初始化假设进行形式化推导, 通过推导证明协议是否达到了预期的正确性目标, 得到结果。

在进行 BAN 逻辑分析验证协议之前, 为方便证明, 我们将数据库服务器端用 D 表示, L 表示标签端, 其他符号注释在第三章中已经给出, 现在对协议做以下合理性假设:

- (1) 标签端 L 在发起认证时每次产生的随机数 $R \in \mathbb{N}^+$ 是新鲜的;
- (2) 数据库端 D 保存的作为认证消息的时间戳 T_i 是新鲜的;
- (3) 数据库端保存自己的公私密钥 K_{DP} , K_{DS} 以及标签的公钥 K_{UP} ;
- (4) 同样的, 标签端保存着自己的公私密钥 K_{UP} , K_{US} 以及数据库公钥 K_{DP} ;
- (5) Hash 函数为数据库端 D 和标签端 L 之间共享。

通过分析 RFID 双向认证协议的认证过程, 抽象出下列主要认证过程的逻辑表示。

MSG1: $L \rightarrow D: M_1 = \{H(id) \| R\}_{K_{DP}}$

MSG2: $D \rightarrow L: M_3 = H(\{PW\}_{K_{US}} \| R)$

MSG3: $L \rightarrow D: M_5 = H(T_i)$

根据以上抽象化认证过程, 规范为符合 BAN 逻辑语法的符号表示模型如下:

MSG1: $D \triangleleft H(id), R$

MSG2: $L \triangleleft H(\{PW\}_{K_{US}} \| R)$

MSG3: $D \triangleleft H(T_i)$

需要我们证明的目标是参与认证的双方相信收到的认证消息是由对方发出的, 而且该认证消息是新鲜有效的, 相对应的公式化符号表示:

$$L \models D \sim \#(\{PW\}_{K_{US}}) \quad (5.10)$$

$$D \models L \sim \#(T_i) \quad (5.11)$$

参考在协议验证之前作出的合理性初始化假设, 对该双向认证协议初始化假设进行如下 BAN 逻辑形式化符号表示:

假设 1: $L \models \#(R)$

假设 2: $D \models \#(T_i)$

假设 3: $L \models L \xleftrightarrow{H} D$

假设 4: $D \models D \xleftrightarrow{H} L$

下面我们依据上述推导规则，结合做出的初始化假设进行逻辑推导分析，证明该双向认证协议的正确性。

(1) 证明 $L \models D \sim \#(\{PW\}_{k_{US}})$

由初始化假设 1 可知: $L \models \#(R)$

根据新鲜性规则 (5.4) 可得:

$$L \models \#(R, \{PW\}_{k_{US}}) \quad (5.12)$$

由模型 MSG2 可知: $L \triangleleft H(R, \{PW\}_{k_{US}})$

根据初始化假设 3、规则 (5.1) 可得: $L \models D \sim H(R, \{PW\}_{k_{US}})$

因为模型 MSG2 可知: $L \triangleleft R$, $L \triangleleft \{PW\}_{k_{US}}$

在结合补充规则 (5.9) 可得: $L \models D \sim (R, \{PW\}_{k_{US}})$

因为信任规则 (5.6) 可知

$$L \models D \sim (\{PW\}_{k_{US}}) \quad (5.13)$$

结合得到的 (5.12) 和 (5.13) 可得: $L \models D \sim \#(\{PW\}_{k_{US}})$

(2) 证明 $D \models L \sim \#(T_i)$

由初始化假设 2 可得

$$D \models \#(T_i) \quad (5.14)$$

根据模型 MSG3 可知: $D \triangleleft H(T_i)$

由初始化假设 3、规则 (5.1) 可得: $D \models L \sim H(T_i)$

由假设 D 端保存有 T_i 可知: $D \triangleleft T_i$

结合补充规则 (5.9) 可得

$$D \models L \sim (T_i) \quad (5.15)$$

由以上得到的 (5.14)、(5.15) 可知: $D \models L \sim \#(T_i)$

至此，目标公式得以成功验证。

由以上可以看出，在 BAN 逻辑推导过程中，标签端 L 与数据库端 D 之间可以进行安全

有效的认证信息传递，即证明了本文提出的应用于 RFID 环境中的双向认证协议是正确可行的。

5.2 协议的仿真系统设计

5.2.1 协议仿真环境与初始参数设置

在 5.1 节中，通过 BAN 逻辑验证方法证明了 RFID 双向认证协议的逻辑正确性。为进一步验证该协议的可用性，本节将仿真模拟 RFID 系统的通信过程，测试认证协议各个模块。本文是在 windows7 系统环境下的 myeclipse 开发工具中，使用 Java 语言对论文中提出的 RFID 双向认证协议进行仿真验证。RFID 系统的通信过程主要是通过 Socket 与 ServerSocket 两个接口进行相应的仿真模拟，该接口底层实现了 TCP/IP 协议。因此，通过 Socket 接口模拟 RFID 标签端，ServerSocket 接口模拟读写器端也即数据库服务器端。两者通过 TCP/IP 协议建立连接，按照协议中的认证过程描述进行认证通信，仿真系统的 RFID 标签端和数据库服务器端采取的有连接方式进行通信，该协议的安全性主要是基于改进后的 ECC 加密算法的认证协议，数据库服务端存储的标签的唯一标识验证码 pw 以及认证随机认证消息 R 都需要进行加密处理，以保证消息的机密性。在实现协议仿真之前，本文会对改进前后的 ECC 算法进行实验对比分析，已验证改进后的密码算法可用性。实验中所采用的是国际上常用的二进制域标准椭圆曲线 $E: y^2 = x^3 + ax + b$ ，其中该椭圆曲线的标准参数为：

$$a=1, b=6$$

$$n=0xFFFFFFFF FFFFFFFF FFFFFFFF B4D44832 147BC5B3 66EDF875$$

$$x=0x07192B9 5FFC8DA7 8631011E D6B24CDD5 73F977A1 1E794811$$

$$y=0x188DA80E B03090F6 7CBF20EB 43A18800 F4FF0AFD 82FF1012$$

其中， n 为椭圆曲线上点的阶，点 (x, y) 为选取的基点 P 。

5.2.2 认证系统总体设计

本仿真认证系统主要是由系统层、运算层以及基本运算层三部分组成。其中系统层包括注册、数据加解密处理以及认证三个模块；由于本认证协议是基于椭圆密码算法设计的，因此中间的运算层中主要是 ECC 算法过程涉及的主要算法和数学运算，如双基链运算、半点运算、点加运算等；底层为基本运算层，主要是有限域加、有限域乘、求逆和平方等基本的数学运算，为上层的运算层提供基本的运算服务。具体的系统组成如图 5.2 所示。

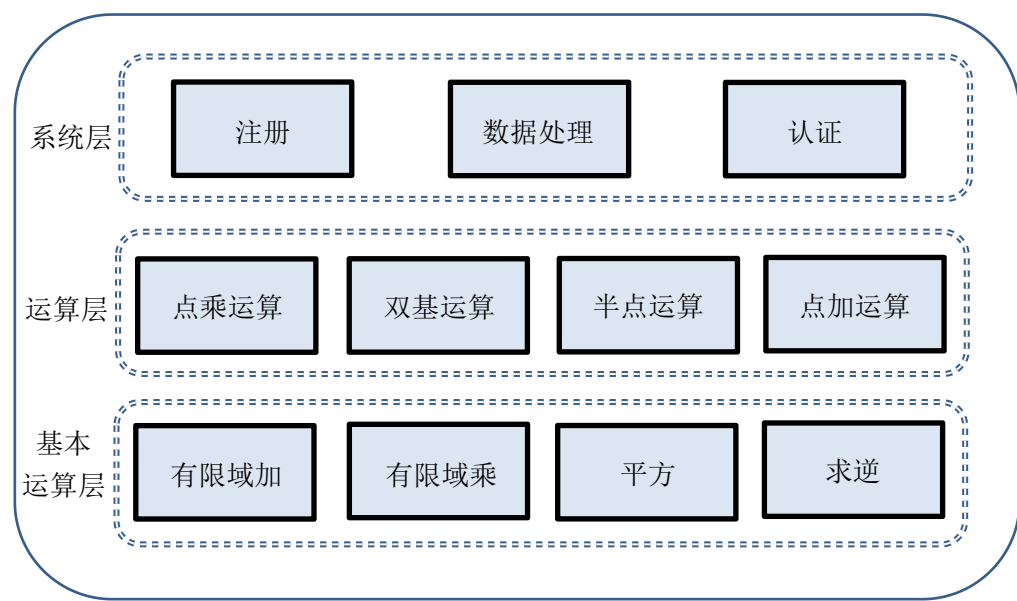


图 5.2 认证系统组成图

在该认证系统中，系统层主要是系统的主要运行模块，包括注册模块、数据加密处理模块以及认证模块。注册模块中主要实现了 RFID 标签端和数据库服务器端之间的密钥交换，以及完成数据库服务器端对标签的唯一标识验证码 pw 的存储，此为重要的认证消息；而数据处理模块主要的功能就是对整个认证系统过程中的敏感信息进行加密处理，以保证信息的机密性，这其中主要包括对注册阶段的标签的 pw 进行加密存储，认证阶段的随机因子 R 进行加密后传递；而认证模块是整个系统的核心组成部分，该模块实现了 RFID 标签与后台数据库服务器之间的双向认证。运算层以及基本运算层是整个认证系统实现的基础，主要涉及了相关的数论运算，其中基本运算层为上层的运算层提供基础的数学运算支撑，而运算层主要涉及的是椭圆曲线上点的运算，其中运算层的运行效率对整个认证过程的实现有很大影响，因为认证协议的基础—ECC 密码体制的关键性运算也即点乘运算就位于该层中。

5.2.3 认证系统的模块设计

(1) 注册模块

由 3.2.1 可知，注册模块主要是将标签 L 的 ID 信息加密存储在后台数据库 D 中，以此来作为认证口令因子，从而为认证过程中标签端对后台数据库端的合法性认证提供保障。但 ID 信息作为标签 L 的私密信息，其机密性至关重要，所以我们将其经过 L 的私钥加密后存储在后台数据库 D 中，以保证标签信息不被窃取和泄露，这其中就需要 ECC 算法进行一定的加密保护。因此，在注册模块中，另一个重要的操作即是 D 端生成相应的椭圆曲线，作为 ECC 算法的基础，而后标签 L 和数据库 D 进行密钥的生成和交互操作，从而使得两端实现密钥共享。该模块具体的流程图如图 5.3 所示。

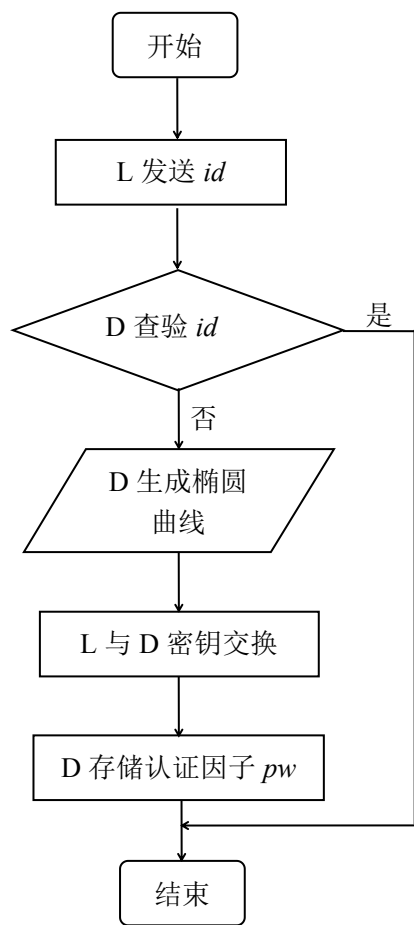


图 5.3 注册模块流程图

开始注册时，由标签端 L 通过发送 id 以发起注册请求，数据库端 D 查找注册表验证 id 是否存在，若存在则结束注册；若不存在则继续进行注册步骤：D 生成安全椭圆曲线并与 L 共享，而后标签 L 和数据库 D 依据椭圆曲线密码算法生成各自的公私密钥，进行密钥交换存储。在此之后，数据库端存储经加密后的标签 L 的唯一标识验证码 pw ，至此，注册过程结束。

（2）数据处理模块

该模块是保证认证系统安全性的基础模块，在整个认证系统中的敏感消息加解密工作均是由该模块完成。本认证协议的基础是椭圆曲线密码体制，因此，该模块中所采用的加密算法即是椭圆曲线加密算法。我们选取的是二进制域 $GF(2^m)$ 上的安全椭圆曲线 $E: y^2 = x^3 + ax + b$ ，以此作为相应的公私密钥生成的基础，具体的参数设置在 5.2.1 节中已经给出。下面介绍一下椭圆曲线加密和解密算法。

算法 5.1 椭圆曲线加密算法

Input：系统参数 a, b, P, n , 公钥 Q , 明文 m

Output: 密文 (C_0, C_1)

- 1) 把 m 映射到椭圆曲线上的一个点 $M \in E(GF(2^n))$
- 2) 随机选择一个整数 $k \in [1, n-1]$
- 3) 计算 $C_0 = kP$
- 4) 计算 $C_1 = M + kQ$
- 5) return (C_0, C_1)

算法 5.2 椭圆曲线解密算法

Input : 系统参数 a, b, P, n , 私钥 k , 密文 (C_0, C_1)

Output: 明文 m

- 1) 计算 $M = C_1 - kC_0$
- 2) 将 M 反映射得到明文 m
- 3) return m

(3) 认证模块

认证模块是整个认证系统的核心模块, 由 3.2.2 节可知, 该模块主要实现的就是 RFID 标签端与数据库端的双向认证。具体的标签端通过验证由数据库端发来的标签的唯一标识验证码 pw , 从而确定数据库的合法性; 而标签身份的合法与否是由数据库端通过校对时间戳是否一致来实施验证的。

某个标签 L 生成一个随机数 R , 而后连同 id 一起加密后作为发起认证请求的口令因子, 发送给读写器 R , 而后经由 R 转发给后台数据库 D , D 端通过其私钥解密该消息, 获取随机认证因子 R , 将其与标签 L 的唯一标识验证码 pw 一起进行哈希运算, 并将结果发送给标签 L , L 端进行同样的运算过程, 而后比对两者的结果是否一致, 若结果一致则说明读写器 R 也即数据库服务器 D 是合法的, 否则, 拒绝继续交互认证。上述过程仅仅实现了 D 端对 L 端的单向认证, 而后标签 L 将时间戳经哈希运算后发送给数据库 D , 数据库服务器通过对 L 端发送的时间戳与 D 端存储的时间戳相互比对, 从而完成对标签 L 的合法性验证, 若相同则说明标签 L 是合法标签, 通过认证; 若不同, 则说明标签 L 是可疑标签, 中断认证, 也即认证失败, 至此整个认证过程结束。具体的认证流程如图 5.4 所示。

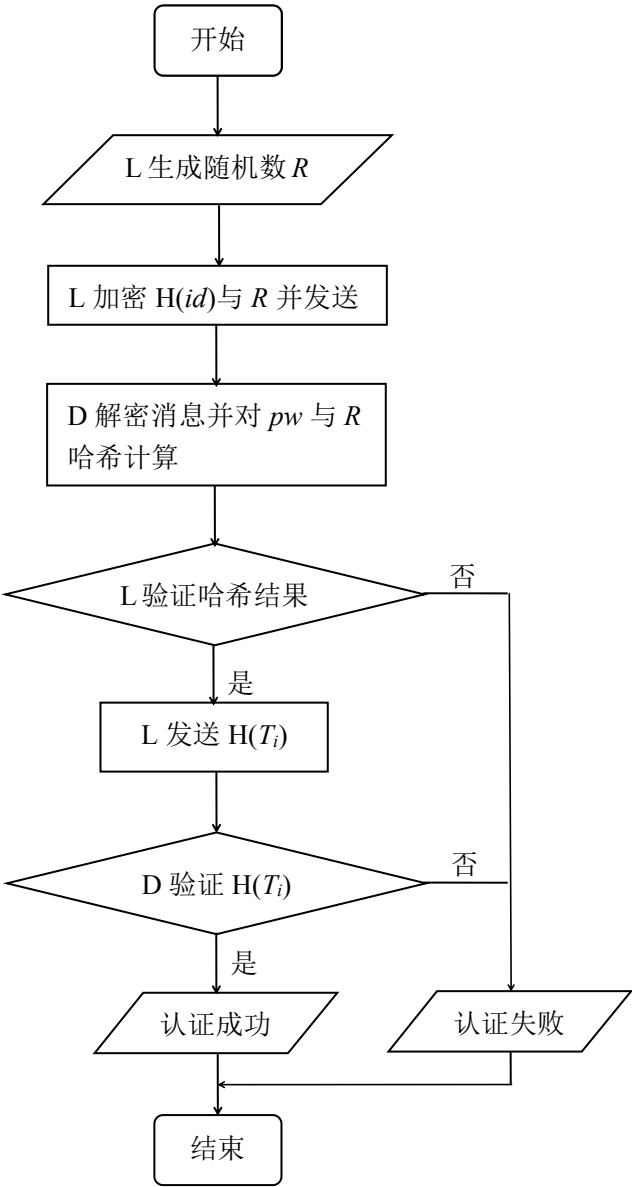
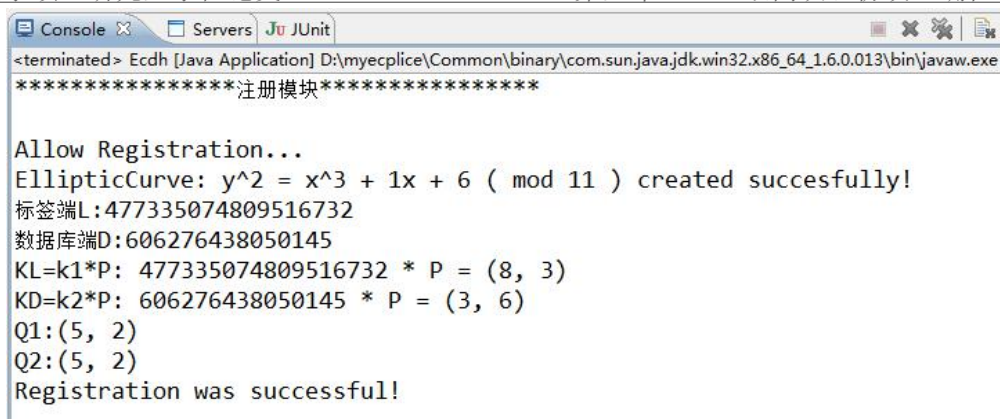


图 5.4 认证流程图

5.3 认证系统测试

5.3.1 注册模块测试

依据 5.2 节中的系统设计思想进行认证系统注册模块的编写测试，其测试结果如图 5.5 所示。



```

Console [Java Application] D:\myecplice\Common\binary\com.sun.java.jdk.win32.x86_64_1.6.0.013\bin\javaw.exe
*****注册模块*****

Allow Registration...
EllipticCurve:  $y^2 = x^3 + 1x + 6 \pmod{11}$  created succesfully!
标签端L:477335074809516732
数据库端D:606276438050145
KL=k1*P: 477335074809516732 * P = (8, 3)
KD=k2*P: 606276438050145 * P = (3, 6)
Q1:(5, 2)
Q2:(5, 2)
Registration was successful!

```

图 5.5 注册模块测试图

在注册模块测试中，数据库端在查找注册表后未发现该标签 id ，即该标签未被注册，允许继续注册。而后数据库端生成了一条安全的椭圆曲线，标签端与数据库端依据该椭圆曲线，生成自己的公私密钥，其中 KL 代表的是标签端公钥映射为椭圆曲线上的点， KD 代表的是数据库端公钥映射到椭圆曲线上的点。计算 $Q_1 = k_2 * KD$ ， $Q_2 = k_1 * KL$ ， $Q_1 = Q_2$ ，则说明两端密钥交换成功，至此，说明注册成功。

5.3.2 数据处理模块测试

在数据加密处理模块中，为了测试改进后的 ECC 算法的运行效率提升情况，本文除了使用改进前后的 ECC 算法进行测试之外，还选取了对称密码算法中的 DESL 算法以及非对称密码算法中的 RSA 算法分别对同一测试数据进行加解密测试，该测试采用了一种插件工具 JUnit，主要是针对加密的时间效率进行对比测试。具体的测试情况如图 5.6-5.9 所示。



```

Console [JUnit] G:\JDK\jre\bin\javaw.exe (2017-2-16 下午9:41:02)
*****数据处理模块*****

公钥:
MEAwEAYHKOZIzj0CAQYFK4EEAAEDLAAEA v4TwFN7vBGsqgfXk950bV5c107oAokHD7Bd0P9YMh8u
gAU21TjM2qPZ

私钥:
MDICAQAwEAYHKOZIzj0CAQYFK4EEAAEEGzAZAgEBB8TYJsR3BN7TFw7JHcAHFkwNmfi17w==

加密前: abc
加密后: [B@2d8c93dc
解密后: abc

Finished after 0.374 seconds

Runs: 1/1      Errors: 0      Failures: 0
eccText.Text [Runner: JUnit 4] (0.359 s)

```

图 5.6 基于原 ECC 的加密模块测试



```
<terminated> Text [JUnit] G:\JDK\jre\bin\javaw.exe (2017-2-16 下午9:47:18)
公钥:
MEAwEAYHkoZIzj0CAQYFK4EEAAEDLAAEA4TWN7vBGsqgfXk950bV5c107oAokHD7BdOP9YMh8u
gAU21TjM2qPZ

私钥:
MDICAQAwEAYHkoZIzj0CAQYFK4EEAAEEGzAZAgEBBBTYjsR3BN7TFw7JHcAHFkwNmfil7w==

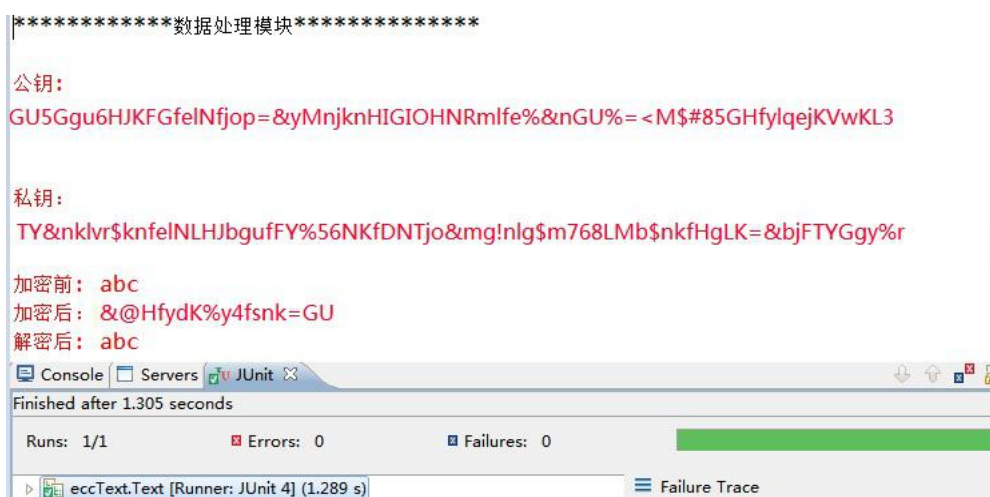
*****数据处理模块*****

加密前: abc
加密后: [B@2d8c93dc
解密后: abc

Finished after 0.234 seconds

Runs: 1/1      Errors: 0      Failures: 0
eccText.Text [Runner: JUnit 4] (0.219 s)
```

图 5.7 基于改进的 ECC 加密模块测试



```
*****数据处理模块*****

公钥:
GU5Ggu6HJKFGfelNfjop=&yMnjknHIGIOHNRmlfe%&nGU%=<M$#85GHfylqejKVwKL3

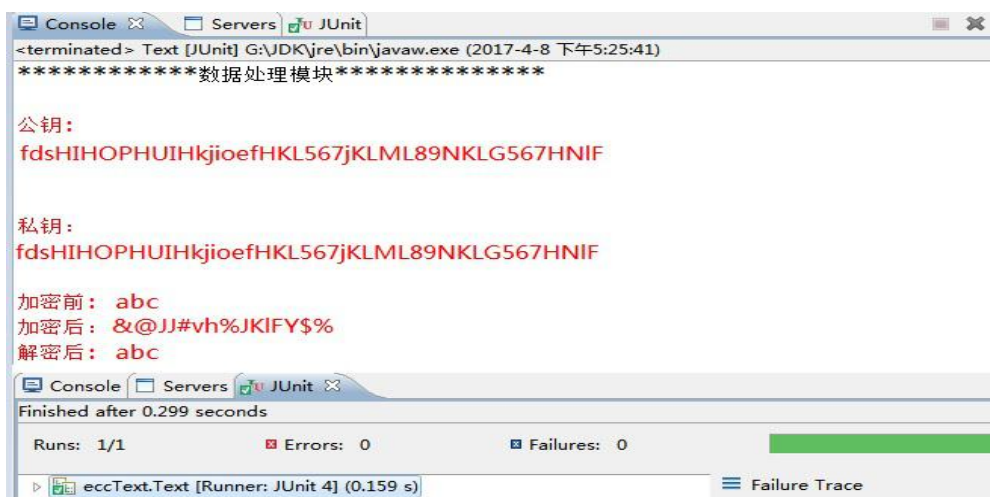
私钥:
TY&nkivr$knfelNLHJbgufFY%56NKfDNTjo&mg!nlg$m768LMb$nkfHgLK=&bjFTYGgy%r

加密前: abc
加密后: &@HfydK%y4fsnk=GU
解密后: abc

Finished after 1.305 seconds

Runs: 1/1      Errors: 0      Failures: 0
eccText.Text [Runner: JUnit 4] (1.289 s)
```

图 5.8 基于 RSA 的加密模块测试



```
<terminated> Text [JUnit] G:\JDK\jre\bin\javaw.exe (2017-4-8 下午5:25:41)
*****数据处理模块*****

公钥:
fdsHIHOPHUIHkjioefHKL567jKLML89NKL567HNIF

私钥:
fdsHIHOPHUIHkjioefHKL567jKLML89NKL567HNIF

加密前: abc
加密后: &@JJ#vh%JKIFY$%
解密后: abc

Finished after 0.299 seconds

Runs: 1/1      Errors: 0      Failures: 0
eccText.Text [Runner: JUnit 4] (0.159 s)
```

图 5.9 基于 DESL 的加密模块测试

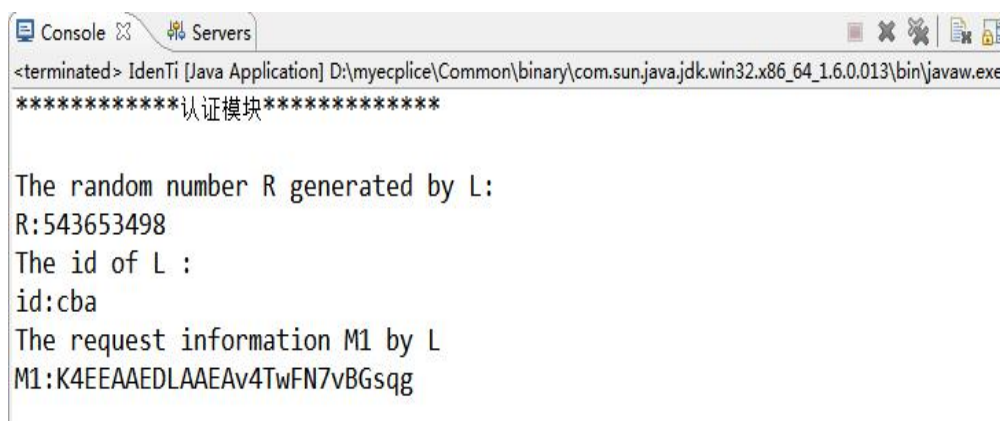
图 5.6 所示为基于原有的 ECC 加密算法的测试情况，而图 5.7 中则为基于改进后的 ECC 加密算法的测试情况，由于改进的是 ECC 密码算法过程中的标量乘运算，并未对 ECC 密码算法的密钥生成进行改动，所以二者生成的密钥和加密方法是相同的，但是运算量和运算效率却相差较大。在图中可以看出，我们采用了 JUnit 插件工具进行测试，基于原有的 ECC 算

法进行加解密所耗费的时间为 0.374s，而改进后的加密算法所耗费的时间为 0.234s，与此同时，本文选取的 RSA 算法以及 DESL 算法加解密测试时间分别为 1.305s 和 0.299s，RSA 算法作为非对称密码算法，其加解密过程所耗费的时间较多，而 DESL 算法是基于对称密码算法中的 DES 算法进行的轻量级变体，该算法的运行效率自然比较快。但是，由测试结果可以看出，改进前的 ECC 算法运行效率虽然较接近 DESL 算法，但依然是低于该算法的运行效率，而改进后的 ECC 算法运行效率较 DESL 算法相比已有明显的优势。由此可以看出，改进后的 ECC 算法密码算法效率有较大的提高。

5.3.3 认证模块测试

(1) 标签端产生随机数 R ，而后加密 id 与 R 作为发起认证的口令 M_1 发送给数据库端。

如图 5.10 所示。



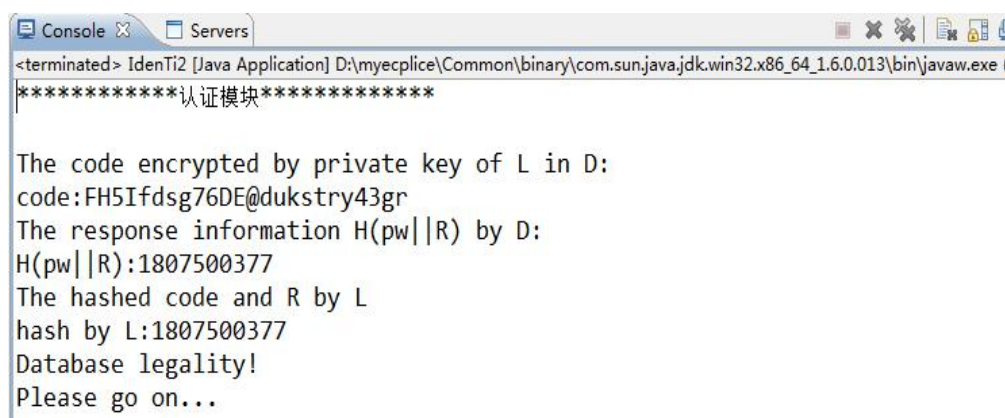
```

Console Servers
<terminated> IdenTi [Java Application] D:\myecplice\Common\binary\com.sun.java.jdk.win32.x86_64_1.6.0.013\bin\javaw.exe
*****认证模块*****

The random number R generated by L:
R:543653498
The id of L :
id:cba
The request information M1 by L
M1:K4EEAAEDLAAEA4TwFN7vBGsqg
  
```

图 5.10 认证请求测试图

(2) 后台数据库端 D 收到认证口令后，解密得到随机数 R ，而后将标签的唯一标识验证码 pw 与 R 进行哈希运算后发送给标签 L，标签做同样的计算，比较结果是否一致。如图 5.11 所示。



```

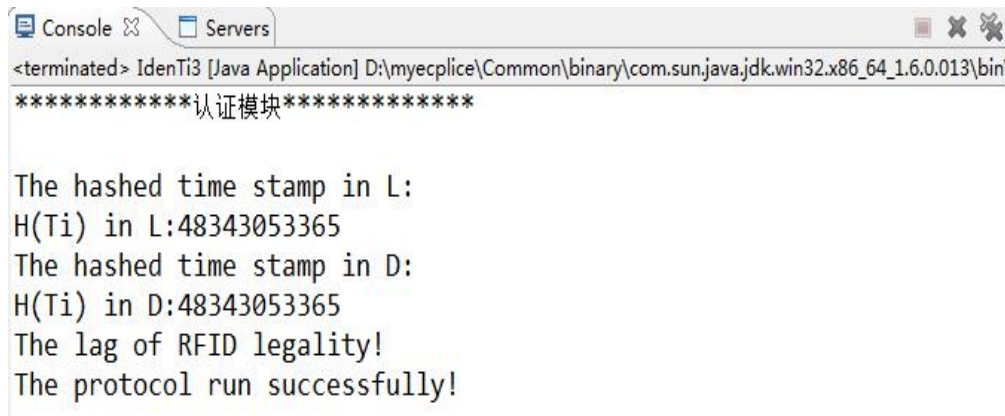
Console Servers
<terminated> IdenTi2 [Java Application] D:\myecplice\Common\binary\com.sun.java.jdk.win32.x86_64_1.6.0.013\bin\javaw.exe (
*****认证模块*****

The code encrypted by private key of L in D:
code:FH5Ifdsg76DE@dukstry43gr
The response information H(pw||R) by D:
H(pw||R):1807500377
The hashed code and R by L
hash by L:1807500377
Database legality!
Please go on...
  
```

图 5.11 数据库合法性认证测试图

(3) 完成单向认证后，标签端 L 发送 $H(T_1)$ 以提供给数据库进行验证，数据库端 D 收到

时间戳后与自己存储的时间戳进行对比, 完成双向认证。如图 5.12 所示。



```
<terminated> Identi3 [Java Application] D:\myecplice\Common\binary\com.sun.java.jdk.win32.x86_64_1.6.0.013\bin
*****认证模块*****

The hashed time stamp in L:
H(Ti) in L:48343053365
The hashed time stamp in D:
H(Ti) in D:48343053365
The lag of RFID legality!
The protocol run successfully!
```

图 5.12 标签合法性认证测试图

5.4 本章小结

在本章中主要是对基于 ECC 和 OTP 认证的双向认证协议进行仿真测试验证。在开始实验测试之前, 首先通过 BAN 逻辑对协议进行了逻辑证明, 在逻辑上验证了协议的正确性; 而后依据协议的描述进行实验系统设计与模拟实现, 该系统主要分为注册、数据处理、认证三个模块, 对三个模块进行了设计和模拟测试。验证了协议的实用性和有效性。值得注意的是在数据处理模块分别采用了原有的 ECC 算法以及改进后的 ECC 算法进行测试, 通过加解密时间效率对比可以看出基于改进后的 ECC 算法效率有明显提高。

第六章 总结与展望

6.1 总结

随着现代社会科技的不断进步与发展, IT 行业也迎来了第三次浪潮——物联网时代。作为物联网感知层核心技术的 RFID 技术也伴随着物联网技术的发展进入人们的视野, 并逐渐被应用到社会的多个行业, 可以说 RFID 技术的发展与物联网技术的发展息息相关。但随之而来的是 RFID 系统本身的安全缺陷问题以及面临的诸多安全威胁, 这正是由 RFID 自身系统结构所带来的安全漏洞。具体的来说是因为在一般的 RFID 系统中, RFID 读写器和标签之间是通过无线射频技术进行非接触式通信, 该无线信道中缺乏有效的安全协议对信道进行保护, 从而使得数据交互信息容易遭受泄露或者更改, 严重威胁着用户信息的隐私性。而目前成熟的认证和加密技术无法适应资源受限的 RFID 系统环境, 迫切需要一种适用于该环境的轻量级认证和加密协议, 这对 RFID 技术的进一步应用推广具有深远的意义, 因此研究资源受限环境下的轻量级认证和加密算法也就成为了国内外的热门课题。

在总结分析了国内外大量的关于轻量级认证和加密技术研究后, 发现目前已有的轻量级安全协议主要关注的就是平衡适用性和安全性两者的关系。因为轻量级安全协议的要求就是在保证轻量性的前提下, 提供一定的安全保护。通过比对分析相关研究文献后可以看出, 现有的许多轻量级认证和加密协议无法很好的兼顾轻量性和安全性这两方面。有鉴于此, 本文提出了一种适用于 RFID 系统环境, 基于 ECC 与 OTP 认证的认证协议。本协议实现了标签端与数据库端的双向认证, 经安全性和可行性分析可知, 该协议在保证协议轻量性也即适用性的前提下, 亦可满足 RFID 系统的安全需求。与此同时, 对影响椭圆曲线密码算法运算效率的标量乘运算进行改进, 在保证一定安全性的基础上, 进一步提高了 ECC 算法的轻量级。并将其与认证协议相结合, 从而使得认证协议整体上达到了安全、有效以及轻量级的要求。论文的主要贡献如下:

(1) 在研究分析了一次性认证机制即 OTP 认证协议的基础上, 深入探究了 OTP 认证机制的认证原理和安全性, 借鉴了 OTP 认证机制轻量简便的认证架构, 设计了一种适用于 RFID 环境的, 基于 ECC 和 OTP 认证的双向认证协议。该协议继承了 OTP 认证机制的计算简便、协议过程清晰的优良结构, 在此基础上引入具有轻量级特性的椭圆曲线加密技术保证认证过程的安全性。

(2) 本文在研究了现有椭圆曲线密码体制运行过程的基础上, 分析指出标量乘运算对密

码体制的关键性影响，并着重对其运算过程进行改进，提出了一种基于新双基的标量乘算法，这使得 ECC 算法的运算效率大幅提高。

(3) 将改进后的椭圆曲线加密算法与认证协议相结合，通过模拟仿真实现的方法证明了该协议的可行性，同时与结合了原 ECC 算法的认证协议相比较，验证分析二者的结果。

6.2 展望

本文主要是针对物联网中的 RFID 系统环境下，轻量级认证协议和加密技术进行研究，提出了一种新的适用于 RFID 系统的双向认证协议，同时对该协议中结合的 ECC 算法进行优化改进，进一步提高了 ECC 算法的轻量化水平。但是由于研究生阶段时间和精力有限，本课题还有许多方面值得我们今后继续深入研究：

(1) 本文中提出的双向认证协议虽已基本满足 RFID 系统环境的安全需求，但是，依然无法防范特殊的中间人攻击，对于防范此种攻击还需进一步考虑结合基于身份认证的方法。

(2) 在协议中引入的椭圆曲线加密技术，本身具有一定的轻量级特性，可以为认证过程提供可靠的安全保护。本文在原有 ECC 算法过程的基础上，分析改进了算法运行中的关键性运算即标量乘运算，基于新的双基表示降低运算量，但是通过相关文献发现，还有其他的基数表示形式如多项式阶乘表示法等，这有待我们进一步研究。

(3) 目前我们所进行的研究还仅仅是在 RFID 环境中，而物联网感知层中的另一个重要技术无线传感器技术也有待我们进行探究，该系统的安全性问题也十分严峻。

参考文献

- [1] International Telecommunication Union UIT.ITU Internet Reports 2005: The Internet of Things[R]. 2005.
- [2] 张凯. 物联网安全教程[M].北京: 清华大学出版社, 2014.
- [3] 白登选. 一种基于 ECC 的 RFID 认证协议[J]. 信息通信,2016,(02):58-59.
- [4] 高树静. 低成本无源 RFID 安全关键技术研究. 山东大学博士毕业论文, 2013.
- [5] Miyaji A, Rahman M S. KIMAP: key-insulated mutual authentication protocol for RFID[J]. International Journal of Automated Identification Technology, 2011,3(2) : 61-74.
- [6] 曾会, 蒋兴浩, 孙铁锋. 一种基于 PKI 的物联网安全模型研究[J]. 计算机应用于软件, 2012,29(6):271-274.
- [7] SARMA S E, WEIS S A, ENGLES D W. Radio frequency identification:secure risks and challenges[J].RSA Laboratories Cryptobytes, 2003,6(1) : 2-9.
- [8] Henrici D, Muller P. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers[C]//Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on. IEEE, 2004: 149-153.
- [9] 丁振华, 李锦涛, 冯波. 基于 Hash 函数的 RFID 安全认证协议研究[J]. 计算机研究与发展, 2009,46(4):583-592.
- [10]张兵, 马新新, 秦志光.基于 hash 运算的 RFID 认证协议分析和改进[J].计算机应用研究, 2011,28(11):4311-4314.
- [11]Jue-Sam C,SUN H M. A novel mutual authentication scheme based on quadratic residues for RFID systems[J].Computer Networks,2008,52(12):2373-2380.
- [12]王海春, 李均, 邓珊. 基于混沌加密的 RFID 认证协议设计[J]. 数字技术与应用, 2015 (11): 206-207.
- [13] Lawrence Lr, Christos P. Efficient Architectures for Elliptic Curve Cryptography Processors for RFID. PhD thesis Of Case Western Reserve University, 2009, 22(5): 410-423.
- [14]Lee Y K, Batina L, Verbauwhede I. EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol[C]//RFID, 2008 IEEE International Conference on. IEEE, 2008: 97-104.
- [15]Tuyls P, Batina L. RFID-tags for anti-counterfeiting[C]//Cryptographers' Track at the RSA Conference. Springer Berlin Heidelberg, 2006: 115-131.
- [16]Batina L, Guajardo J, Kerins T, et al. Public-key cryptography for RFID-tags[C]//Pervasive Computing and Communications Workshops, 2007.PerCom Workshops' 07. Fifth Annual IEEE International Conference on. IEEE,2007: 217-222.
- [17]Chen Y, Chou J S, Sun H M. A novel mutual authentication scheme based on quadratic residues for RFID systems[J]. Computer Networks, 2008, 52(12): 2373-2380.
- [18]康鸿雁. 基于 ECC 的 RFID 组证明协议分析及改进[J]. 计算机工程, 2013, 39(1): 153-156.
- [19]LEANDER G, PAAR C, POSCHMANN A, et al. New lightweight DES variants[C]// Fast Software Encryption, LNCS 4595. Berlin:Springer-Verlag, 2007: 196 -210.
- [20]David M, Ranasinghe D C, Larsen T. A2U2: a stream cipher for printed electronics RFID tags[C]//RFID (RFID), 2011 IEEE International Conference on. IEEE, 2011: 176-183.
- [21]Karakoc F, Demirci H, Harmanci A E. ITUbee: a software oriented lightweight block cipher[M]//Lightweight Cryptography for Security and Privacy. Springer Berlin Heidelberg, 2013: 16-27.
- [22]Lim C H, Korkishko T. mCrypton—a lightweight block cipher for security of low-cost RFID tags and sensors[C]//International Workshop on Information Security Applications. Springer Berlin Heidelberg, 2005: 243-258.
- [23]Eisenbarth T, Kumar S. A survey of lightweight-cryptography implementations[J]. IEEE Design & Test of Computers, 2007, 24(6) : 522-533.
- [24]Knuth D E. The art of computer programming: sorting and searching[M]. Pearson Education, 1998.
- [25]Cohen H. A course in computational algebraic number theory[M]. Springer,2000.
- [26]单承赣, 单玉锋, 姚磊.射频识别(RFID)原理与应用[M].北京: 电子工业出版社, 2007.
- [27]韦小妮. 物联网中 RFID 技术相关安全性问题分析[J]. 无线互联科技, 2015 (14): 38-39.
- [28]张兵, 马新新, 秦志光. 轻量级 RFID 双向认证协议设计与分析[J]. 电子科技大学学报, 2013, 42(3): 425-430.

- [29]叶锡君, 吴国新, 许勇等. 一次性口令认证技术的分析与改进[J]. 计算机工程, 2009, 26(9): 27-29.
- [30]柳景超, 宋胜锋. 一次性口令认证方案的研究与改进[J]. 计算机与网络, 2010, 36(7): 60-62.
- [31]肖攸安. 椭圆曲线密码体系研究[M]. 武汉: 华中科技大学出版社, 2006.
- [32]Rolfes C, Poschmann A, Leander G, et al. Ultra-lightweight implementations for smart devices – security for 1000 gate equivalents [M]//Smart Card Research and Advanced Applications. Springer Berlin Heidelberg, 2008: 89-103.
- [33]Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.
- [34]Structure F. Channel Coding and Modulation for Digital Terrestrial Television[J]. ETSI EN, 1996, 300(744): V1.
- [35]杨威, 万武南, 陈运, 张言涛. 适用于受限设备的轻量级密码综述[J]. 计算机应用, 2014, 34(7): 1871-1877.
- [36]Manifavas C, Hatzivasilis G, Fysarakis K, et al. Lightweight Cryptography for Embedded Systems-A Comparative Analysis[M]//Data Privacy Management and Autonomous Spontaneous Security. Springer Berlin Heidelberg, 2014: 333-349.
- [37]Eisenbarth T, Kumar S, Paar C, et al. A survey of lightweight-cryptography implementations[J]. IEEE Design & Test of Computers, 2007, 24(6): 522-533.
- [38]Katagi M, Moriai S. Lightweight cryptography for the internet of things[J]. Sony Corporation, 2008: 7-10.
- [39]Poschmann A Y. Lightweight cryptography: cryptographic engineering for a pervasive world[C]//PH. D. THESIS. 2009.
- [40]李忠, 彭代渊. 基于滑动窗口技术的快速标量乘法[J]. 计算机科学, Vol.39, No.6A, June 2012.
- [41]Joye M, Yen S M. Optimal left-to-right binary signed-digit recoding[J]. IEEE Transactions on Computers, 2000, 49(7): 740-748.
- [42]Koyama K, Tsuruoka Y. Speeding up elliptic curve cryptosystems by using a signed binary window method[C]//Advances in Cryptology-Crypto'92. 345-357.
- [43]Dimitrov V S, Jullien G A, Miller W C. Theory and applications of the double-base number system[J]. IEEE Transactions on Computers, 1999, 48(10): 1098-1106.
- [44]Ciet M, Joye M, Lauter K, et al. Trading inversions for multiplications in elliptic curve cryptography[J]. Designs, codes and cryptography, 2006, 39(2): 189-206.
- [45]Weger B. M. M. de. Algorithms for Diophantine equations, vol. 65 of CWI Tracts, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.
- [46]Doche C, Habsieger L. A tree-based approach for computing double-base chains[C]//Australasian Conference on Information Security and Privacy. Springer Berlin Heidelberg, 2008: 433-446.
- [47]于伟. 椭圆曲线密码学若干算法研究[D]. 中国科学技术大学, 2013.
- [48]Cohen H, Miyaji A, Ono T. Efficient elliptic curve exponentiation using mixed coordinates[C]//International Conference on the Theory and Application of Cryptology and Information Security. Springer Berlin Heidelberg, 1998: 51-65.
- [49]Longa P, Gebotys C. Fast multibase methods and other several optimizations for elliptic curve scalar multiplication[C]//International Workshop on Public Key Cryptography. Springer Berlin Heidelberg, 2009.
- [50]Purohit G N, Rawat A S. Fast scalar multiplication in ECC using the multi base number system[J]. International Journal of Computer Science Issues, 2011, 8(1): 131-137.
- [51]Knudsen E W. Elliptic scalar multiplication using point halving[C]//International Conference on the Theory and Application of Cryptology and Information Security. Springer Berlin Heidelberg, 1999: 135-149.
- [52]Doche C, Imbert L. Extended double-base number system with applications to elliptic curve cryptography[C]//International Conference on Cryptology in India. Springer Berlin Heidelberg, 2006.
- [53]Mishra P K, Dimitrov V. Efficient quintuple formulas for elliptic curves and efficient scalar multiplication using multibase number representation[C]//International Conference on Information Security. Springer Berlin Heidelberg, 2007: 390-406.
- [54]Ciet M, Joye M, Lauter K, et al. Trading inversions for multiplications in elliptic curve cryptography[J]. Designs, codes and cryptography, 2006, 39(2): 189-206.
- [55]赖忠喜, 张占军, 陶东娅. 椭圆曲线中直接计算 7P 的方法及其应用[J]. 计算机应用, 2013, 33(7): 1870-1874.
- [56]韩冬. RFID 安全认证协议的关键问题研究[D]. 辽宁: 辽宁工业大学, 2016.

附录1 攻读硕士学位期间撰写的论文

(1) 陈春玲, 汪洋, 余瀚, 强小辉. The RFID Mutual Authentication scheme Based on ECC and OTP Authentication, ICUWB2016, 已发表。

附录 2 攻读硕士学位期间参加的科研项目

- (1) 江苏省信息安全应急中心合作项目，物联网轻量级认证和加密技术研究

致谢

三年的研究生生活匆匆而过，想来如白驹过隙，回想起这三年在南京邮电大学的学习生活，依然历历在目。一路走来有太多的美好值得回味，有太多的人需要感谢……

首先，我最想感谢的人就是我的导师陈春玲教授。三年前，我怀着无比激动的心情来到了陈老师门下，从此，我认识了一位和蔼可亲、治学严谨的师长。从课题开题立项到最终完成，陈老师给予了我殷切的关怀和指导。每当课题遇到瓶颈而我百思不得其解的时候，陈老师总是耐心的帮我分析问题，和我一起讨论课题的难点，引导我找寻思路，陈老师严谨的治学态度，渊博的理论知识，以及平易近人的作风都深深印在了我的心里，每一次的师门交流都使我受益匪浅。陈老师不仅在学业上给予我们很大的帮助，更是对我们的生活关怀备至。在与我聊天谈心时他那关切的问候依然记忆犹新，陈老师就是这样一个温暖的长辈，在百忙之中依然关心着我们师门的每一位同学。在这里我要由衷的对陈老师说一句：谢谢您！

其次，我要对江苏省信息安全应急中心的蔡冰老师和强小辉老师表示由衷的感谢。在课题进行过程中，他们耐心的指导给了我很大的帮助，及时对我遇到的问题进行反馈，给予了我最大的支持。

而后，我想对我们师门的兄弟姐妹们表示感谢。三年前是缘分让我们走到了一块，携手在科研楼 806 教研室这个宽敞而温暖的房间度过了愉快的三年研究生生活。每次对课题中的问题迷惑不解时，出现在我身边的总是你们这一群可爱的亲人，和我一起讨论，一起欢笑，一起忧愁，谢谢你们的陪伴。

最后，我还有感谢我的家人，是他们对我的默默支持，让我能更加专心于自己的课题研究，顺利的完成学业。