分　类　号：TN918.4　　单位代码：10183
研究生学号：2014522062　　密　　级：公 开

吉林大学

硕士学位论文

（学术学位）

基于散列函数和椭圆曲线密码的RFID安全协议研究

Research on RFID Security Protocols Based on Hash Function and Elliptic Curve Cryptography

作者姓名：张磊
专　　业：信号与信息处理
研究方向：短距离无线通信技术
指导教师：于银辉　教授
培养单位：通信工程学院

2017 年 6 月

基于散列函数和椭圆曲线密码的 RFID 安全协议研究

Research on RFID Security Protocols Based on Hash Function and Elliptic Curve Cryptography

作者姓名：张磊

专业名称：信号与信息处理

指导教师：于银辉 教授

学位类别：工学硕士

答辩日期：2017年6月3日

吉林大学硕士学位论文原创性声明

本人郑重声明：所呈交学位论文，是本人在指导教师的指导下，独立进行研究工作所取得的成果。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作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

学位论文作者签名：张磊

日期：2017年6月3日

摘　　要

基于散列函数和椭圆曲线密码的 RFID 安全协议研究

近年来，随着物联网的发展，人们对无线通信技术的研究逐渐深入，特别是射频识别（RFID）技术受到了业界普遍关注。但是，由于 RFID 系统中标签和读写器认证过程工作在无线通信信道，使得系统的安全性难以得到保障，阻碍了 RFID 系统的大规模推广和应用。为此，人们已经提出了许多关于 RFID 系统的认证协议，依据系统的计算复杂度和操作复杂性，大体可分为基于简单逻辑运算的轻量级认证协议、基于散列函数的中量级认证协议、基于对称或公钥密码体制的重量级认证协议等。其中，中量级和重量级认证协议具有性能好、安全性强等优势，是近几年学者们研究的热点。然而，在现有的认证协议中，大多数协议未能够兼顾系统的安全隐私性和标签硬件成本，导致认证协议难以在系统和平台上实现。本文在归纳和总结现有的认证协议基础上，提出了两种改进协议。

（1）首先对 RFID 系统组成部分和系统工作原理进行梳理，接下来对 RFID 系统设计要求进行归纳和总结，主要考虑系统安全隐私和性能指标，详细分析系统目前所面临的安全隐患，介绍了两种 RFID 安全机制，并对两种安全机制的优缺点进行归纳和总结。

（2）简要地介绍散列函数的理论基础，针对现有的典型的基于散列函数的 RFID 安全协议，通过对认证过程、安全和性能的详细分析和总结，得出每个认证协议的优势和劣势。在此基础上，提出了一种改进的 RFID 认证协议，主要采用挑战响应机制、伪随机数发生器和散列函数等方法对认证过程进行加密，应用动态 ID 机制更新标签和后台服务器信息，运用形式化分析方法 BAN 逻辑分析和证明认证协议的正确性。在改进协议设计过程中，既考虑到 RFID 系统的局限性和特殊性，又兼顾了系统安全性和隐私性。在安全隐私方面，协议能够有效抵抗假冒、重放、去同步等攻击，在性能方面，协议中后台数据库通过简单地匹配查找和计算，将服务器加密计算的时间复杂度降低到常数阶 O(1)，同时协议利用较少比特信息参与计算、存储以及传输过程，降低了系统开销、提高了系统运行效率和可扩展性。

（3）研究了基于椭圆曲线密码机制的 RFID 认证协议，介绍了椭圆曲线理论基础和椭圆曲线离散对数问题，针对现有的典型的基于椭圆曲线的 RFID 安全协议，进行了详细地论述和分析，并且指出了不足之处。在此基础上，提出了一种基于椭圆曲线

的改进协议，采用椭圆曲线密码机制加密认证过程，给出了认证协议的算法步骤，通过安全性分析和对比，本协议具备双向认证、不可追踪性、可扩展性等明显优势。在Visual C++6.0 开发环境下，对改进协议进行软件仿真，实现改进协议的参数生成、加解密、标签和后台服务器之间相互认证过程，仿真实验表明，改进协议具有可行性。

论文的研究和实验结果表明，本文提出的两种改进协议能有效提高系统的安全性并且改善系统性能。

关键词：

RFID 系统，认证协议，散列函数，椭圆曲线密码

ABSTRACT

Research on RFID Security Protocols Based on Hash Function and Elliptic Curve Cryptography

In recent years, with the rapid development of the Internet of things, people have deeply researched on wireless communication technology. Especially Radio Frequency Identification technology has been widely used in various fields. However, because of the special non-contact between the tag and the reader, the privacy and security of user data are difficult to be guaranteed. Therefore, people propose many authentication protocols. Based on the computational and operational complexity of the system, it includes lightweight authentication protocols based on simple logic operations, middleweight authentication protocols based on hash function, heavyweight authentication protocols based on cryptosystems. Among them, the middleweight and heavyweight authentication protocols have the advantages of good performance and strong security, which is a hotspot in recent years. In the existing authentication protocols, however, most of protocols failed to take into account the security and the hardware requirements, which makes it difficult to achieve in the system. So, in this paper, we summarize the existing authentication protocols, and propose two improved protocols.

(1) Firstly, we collate and summarize the concepts of the system components and the working principle. Considering the security and performance, we describe these design requirements in RFID system. Finally, we introduce two kinds of RFID security mechanisms, and analyze the advantages and disadvantages.

(2) The theoretical foundation of hash function is introduced briefly. In the existing typical RFID security protocols based on hash function, we summarize and analysis the authentication process, the security and performance. And we draw the advantages and disadvantages of each authentication protocol. On this basis, we propose an improved RFID authentication protocol. The dynamic ID mechanism is used to update the tag and the server information. The protocol uses the challenge response mechanism, the pseudo random number generator and hash function to process the data between the tag, the reader and the server. We also give formal analysis and proof of the protocol by the tool of BAN logical. In

the improved protocol, we not only take into account the limitation and particularity of the RFID system, but combine the security and privacy. In terms of the security and privacy, this protocol can effectively resist the common attacks such as forgery, replay, de-synchronization attack and so on. In terms of the performance, index mechanism is used in the database, and the time complexity of the cryptographic computation in the database is reduced to O(1). At the same time, the improved protocol can use the computation, storage and communication with little bits, which can reduce the cost and improve the efficiency and the scalability of the system.

(3) We study some RFID authentication protocols based on elliptic curve cryptography, and introduce the definition of elliptic curve, group operation and elliptic curve discrete logarithm problem. In the existing security protocols based on elliptic curve cryptography, we analyze the authentication process in detail, and point out the deficiency. On this basis, we propose an improved RFID authentication protocol based on elliptic curve cryptography, and use the mechanism to achieve the authentication. Then we describe the implementation process and algorithm steps of the protocol. Compared with the counterparts in the security, it turns out that the improved protocol has advantages in the two-way authentication, the untraceable privacy, the extensibility and so on. Finally, we use Visual C ++ 6.0 software to achieve the simulation of the improved protocol. And we implement the generating parameters, the encryption and decryption parts and the authentication between the tag and the server, which shows that the protocol can be feasible.

Through the researches and experimentations, the two improved protocols proposed in this paper can improve the security and performance.

Key words：

RFID System, Authentication Protocol, Hash Function, Elliptic Curve Cryptography

目 录

第 1 章 绪 论

1.1 研究背景及意义

RFID 技术是一种无接触式的自动识别技术，其显著特点是无需与物体直接接触即可通过射频信号获取物体相关信息。与传统的条形码、磁卡识别、声音识别、光学识别相比，RFID 技术凭借其可操作性强、读取速度快、通讯距离远等优势，已经成为物联网的核心技术之一[1]。根据国际物联网贸易与应用促进协会（IIPA）的分析和预测，2017 年中国 RFID 行业市场规模将达 621 亿元。从 2013-2017 年，中国 RFID 行业市场规模将增长约 2.4 倍，年均增长率约为 27.88%。近年来中国的市场规模及预测如图 1.1 所示。

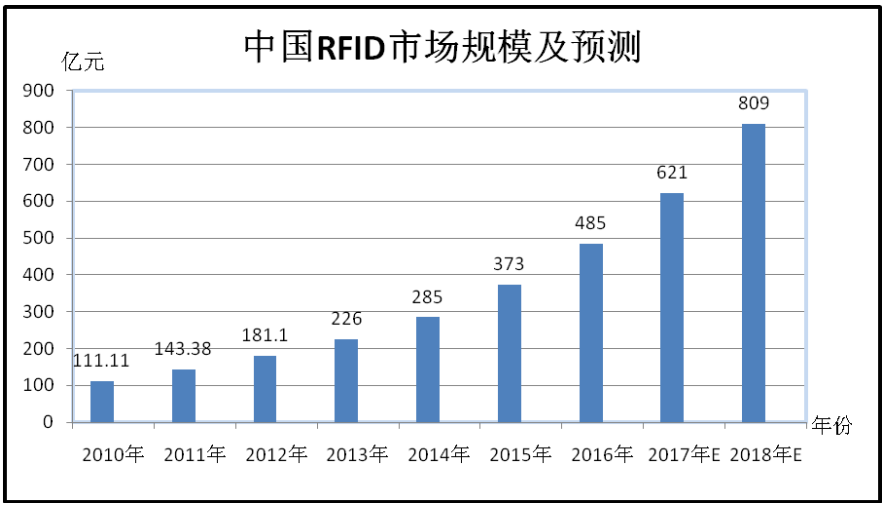

图 1.1 2010—2018 年中国 RFID 行业市场规模及预测

目前，RFID 技术已经在国内外各领域迅猛发展，其中，在身份识别、交通管理、军事与安全、资产管理、防盗与防伪、物流、工业控制等领域的应用中已经取得突破性进展，并在部分领域进入大规模应用阶段[2]。随着 RFID 技术进一步成熟以及系统成本逐渐降低，可以预见的未来，RFID 技术必将应用到各行各业中，给人们的生活带来更多的便利。

随着 RFID 技术在众多领域的广泛应用，系统本身的安全隐私问题也越来越凸显。在 RFID 系统中，读写器和标签之间的数据交互是在不安全的无线信道中进行的，攻击者很容易截获其交互信息，分析并利用获取的数据，在此基础上，攻击者可以假冒合法标签哄骗读写器抑或是假冒读写器骗取标签的信任，还可以进行定位追踪、重放

等攻击，这对 RFID 系统中信息安全造成了巨大威胁[3]。如果不能切实有效地解决 RFID 系统中的安全问题，那么系统中个人隐私、商业以及军事机密都可能被不法分子盗用，这必将严重影响社会和经济的正常发展，与此同时也制约了 RFID 技术的大规模推广和应用[4]。归根结底，RFID 系统的安全性是由其内部认证协议来保障的，只有强有效的安全认证协议，才能保证系统正常的运行。近年来，业界设计出了众多基于密码机制的认证协议，但遗憾的是，目前提出的协议经常存在基于密码算法弱、安全性能低、标签和后台服务器计算开销大、协议机制不合理等安全和效率问题。因此设计一个安全、高效的 RFID 认证协议具有深远的实际意义。

1.2 国内外研究现状

针对 RFID 系统中安全和隐私问题，国内外的学者已经提出多种认证方案，并取得一定进展。但是在设计认证协议时，大多数学者未能兼顾系统的硬件成本和系统的安全性，采用简单逻辑运算的协议往往存在安全性不够高的问题，采用复杂加密算法的协议常常是硬件成本超出预算[5]。因此需要我们仔细研究这些现有的认证方案，分析其优缺点，才能更好地设计出满足安全需求的认证协议。目前，现有的 RFID 安全方案可分为：物理机制和密码机制。其中，在物理机制中，现有的方法过于简单，无法满足日益多变的 RFID 系统的安全和隐私性；在密码机制中，我们利用加密算法保护系统安全和隐私，这种方法能够满足绝大多数应用场景。密码机制依据系统计算复杂度和操作复杂性，大体可分为基于简单逻辑运算的轻量级认证协议、基于散列（Hash）函数的中量级认证协议、基于对称或公钥密码体制的重量级认证协议等[6]。其中，中量级和重量级认证协议具有性能好、安全性强等优势，是近几年国内外学者们研究的热点。

为实现 RFID 系统传递信息完整性、真实性和隐私性，业界已经提出许多种解决方案[7]。其中，基于散列函数机制的认证方案，2003 年，Weis 等人提出了随机化 Hash-Lock 协议[8]，该协议因其标识以明文方式在不安全信道传送，导致系统容易受到追踪、假冒和重放等攻击，并且读写器的计算负担繁重，系统的运行效率较低； 2008 年，Lee Y C 等人提出的认证协议[9]，由于该协议是基于静态 *ID* 机制的认证协议，因此不存在去同步化问题，同时协议能够抵抗假冒攻击，但是系统不能抵御重放攻击，并且系统的可扩展性较差；2009 年，丁振华等人提出的 HSAP 协议[10]，研究发现该协议能有效抵御假冒攻击、追踪攻击、去同步化等攻击，但协议并未考虑系统的前向安

全性和用户标签所有权转移等问题，并且后台服务器加密计算的时间复杂度达到了线性阶 O(n)，系统的可扩展性较差、运行效率较低；2010 年，罗序斌提出了一个支持标签所有权转移的安全认证协议[11]，分析发现，该协议虽然可以有效抵御假冒、重放、追踪等各种攻击，但是协议执行过程中通信成本较高、服务器计算繁重、可扩展性较差；2015 年，Srivastava 等人提出的认证协议[12]，采用时间戳、伪随机数发生器以及更新密钥值等方法，使系统能够抵抗重放、追踪等攻击，但是系统容易受到中间人攻击并且存在密钥更新同步等问题。上述各方案未对认证协议过程进行形式化方法分析或仿真实现，无法保证在实际系统中可行性，因此以上协议方案并不能真正地适用于低成本、高效率 RFID 系统。

在基于椭圆曲线密码机制（ECC）的认证方案中，2006 年，Tuyls 和 Batina 提出的基于 ECC 的 RFID 认证方案[13]，该协议认证过程过于简单，仅仅实现了服务器对标签的单向认证，攻击者可以利用截获的认证信息对标签实施定位追踪，并且协议的可扩展性较差；在此基础上，为了抵抗追踪攻击，2008 年，Lee 等人提出了 EC-RAC 协议[14]，在性能方面较 Tuyls 的协议有所提高，但是该协议还是无法抵御追踪攻击，并且仅仅实现了单向认证；2010 年，O'Neill 等人提出的 ECC 认证方案中[15]，应用散列函数和数字签名机制，该协议能够抵御假冒、重放等攻击，并且还能够抵抗追踪攻击，然而却存在计算开销大、可扩展性差等问题；2011 年，Zhang 等人提出了一种改进协议 ECDLP−RK[16]，该协议虽然能够抵御跟踪攻击，但依然存在计算开销大、可扩展性差等问题；2014 年，何剑辉提出的改进协议[17]，由于协议执行过程中传递的信息都是新鲜的，攻击者无法成功实施对标签的追踪攻击，但是该协议不能抵御对服务器的重放攻击和对标签的假冒攻击，并且后台数据库需要通过线性搜索的方式去查询标签公钥值和标识信息，所以导致服务器计算开销较大、系统可扩展性较差；2014 年，杨玉龙等人提出的协议[18]，该协议中虽然给出了标签和读写器不可跟踪隐私的安全性证明，但是服务器无法抵御假冒、重放等攻击，并且协议认证过程和结果缺乏仿真支撑，因此无法保证协议在实际系统中的可行性。

随着标签计算存储能力的提升，硬件成本的逐渐降低，以及人们对 RFID 系统的安全和隐私的重视，基于散列函数和椭圆曲线密码机制的 RFID 认证协议已经成为目前研究的重点。从以上的各种方案中，我们可以看出，业界学者对基于散列函数和基于椭圆曲线密码机制的认证方案的研究正在逐渐深入，但是依然存在安全隐患或者性能问题。本文旨在设计出安全性强、计算存储负担计量少、可证明安全性的 RFID 认证协议。

1.3 本文主要研究内容

随着无线通信技术的发展，特别是射频识别技术的大规模应用，系统的安全隐私和性能问题受到了人们的普遍关注。本文首先介绍了研究背景和意义以及国内外的研究现状，接下来阐述系统组成和工作原理，并对系统设计要求和安全机制进行详细论述。针对现有的 RFID 认证协议存在的安全隐患以及标签计算存储性能等一系列问题，本文提出了一种基于散列函数的改进协议和一种基于椭圆曲线的改进协议。本文主要从以下几方面对 RFID 系统展开研究：

（1）针对不同的应用场景和不同的用户需求，提出了两种不同的认证方案。对于应用于制造业（装配线管理）、零售业等领域的低成本、高效率的 RFID 标签，本文提出了基于 Hash 函数改进的 RFID 认证协议；针对安防系统、金融系统等安全性要求较高的领域，本文提出了基于 ECC 改进的 RFID 认证协议。

（2）研究现有的典型的基于散列函数的 RFID 认证协议，详细分析认证过程和算法，总结安全和性能的优势和劣势。在此基础上，提出一种改进协议，采用挑战响应机制和动态 *ID* 机制实现 RFID 安全认证过程，阐述协议执行过程和算法步骤，运用形式化分析方法 BAN 逻辑分析和证明认证协议的正确性。在改进协议设计过程中，兼顾了系统安全隐私和硬件需求，在安全隐私方面，协议能够有效抵抗假冒、重放、去同步等攻击，在性能方面，协议中后台数据库通过简单地匹配查找，将服务器加密计算的时间复杂度降低到常数阶 O(1)，同时改进协议利用较少比特信息进行计算、存储以及传输，降低了系统开销、提高了系统运行效率和可扩展性。

（3）研究了现有的基于 ECC 的 RFID 安全协议，通过对认证过程和算法的分析和总结，指出了协议的优势和劣势。在此基础上，提出了一种基于 ECC 的改进协议，采用椭圆曲线密码机制加密认证过程，给出了协议具体认证过程和算法步骤。通过安全性分析和对比，本协议具备双向认证、不可追踪性、可扩展性等优势。在 Visual C++6.0 开发环境下，对改进协议进行软件仿真，实现了改进协议的参数生成、加解密、标签和后台服务器之间认证，仿真结果表明，改进协议具有可行性。

1.4 本文主要结构

本论文主要针对 RFID 认证协议进行研究，研究了基于散列函数和椭圆曲线密码

的 RFID 安全协议。论文结构如下：

第 1 章，主要介绍了 RFID 技术及其应用，以及国内外关于本课题的研究现状，并且介绍了本课题研究的主要内容。

第 2 章，首先对 RFID 系统组成和关键部件进行了梳理和总结，接下来主要对 RFID 系统工作原理和设计要求进行归纳和总结，最后对 RFID 安全机制进行了分析和总结。

第 3 章，简要地介绍散列函数理论基础，对现有的基于散列函数的 RFID 认证协议进行分析和总结，提出改进协议，阐述协议的算法步骤，利用 BAN 逻辑对协议的正确性进行分析和证明，通过安全和性能的分析对比，说明改进协议具有更快的执行效率、更高的安全性、更强的可靠性。

第 4 章，介绍椭圆曲线的理论基础，针对现有的基于 ECC 的 RFID 认证协议进行分析和总结，提出改进协议，阐述协议的算法步骤，并对协议的安全和性能进行分析和对比，通过 Visual C++6.0 开发环境进行仿真实验，说明改进协议的可行性。

第 5 章，对全文进行总结和展望，概括和总结本文的主要研究内容和成果，分析并指出本文所存在的不足，以及在下一步研究中有待改进的地方。

第 2 章　RFID 系统相关知识

2.1　RFID 系统组成

一般来说，RFID 系统由标签（Tag）、读写器（Reader）、和后台服务器（Server）三部分组成[19]。

2.1.1　RFID 标签

标签，也称射频识别卡，是 RFID 系统中认证终端，它由射频天线和芯片两部分构成。标签内置的天线用于与读写器进行信息交互，芯片用于计算和存储等操作，每个标签具有唯一的电子编码[20]。

依据标签供电形式不同，可将标签划分为三类[21]，标签的类型和以及具有的特点，如表 2.1 所示。

表 2.1 标签类型及其特点

标签类型	特点
主动标签	也称有源标签，含有内置电源，读取范围较大，但是寿命有限、体积大、成本高，并且不适合在恶劣环境下工作，一般应用较少。
被动标签	也称无源标签，无内置电源，通过电磁转换技术将接受的射频信号转换成能量为标签供电，识别距离较短，但其寿命长，成本较低，并且对工作环境要求不高，因此应用最为广泛。
半主动标签	含有内置电源，电源能量仅仅用于标签内部单元操作，向读写器发送信号仍然依靠读写器发出的电磁能转换为电能来支持，其信号传输范围以及硬件成本位于被动标签与主动标签之间。

依据标签工作频率不同，可将标签分为三类[22]，标签的分类以及具有的特点，如表 2.2 所示。

表 2.2 标签分类和主要特点

标签	主要特点
低频标签	工作频率范围：30KHz~300KHz，最常见的频率为125KHz 和 133KHz，标签成本低，存储数据较少，读写距离较短，通常小于 10cm。
中高频标签	工作频率范围：3MHz~300MHz，最常见的频率为13.56MHz，标签和读写器成本较低，存储数据量较大，读写距离较远，最远可达 1m。
微波标签	工作频率范围：433.92MHz，862（902）~928MHz，2.45GHz，5.8GHz，该频段标签和读写器天线采用的是定向天线，最远识别距离超过 10m。

2.1.2 RFID 读写器

读写器，也称阅读器，通过射频天线发射的电磁波与标签进行信息交互，完成信息的读取和写入等操作，并将这些数据传送到后台服务器。在整个系统中，读写器的工作频率决定了系统的工作频率。读写器模块主要包括射频接口、控制单元和电源等。根据读写器所使用的场景不同可将其划分为三类，即固定式读写器，手持式读写器以及移动式读写器。固定式读写器是指通过导线连接的读写器和后台服务器分别放置在不同位置的装置，日常生活中大多数 RFID 系统都属于此类；手持式读写器是读写器和后台服务器集成为一体，可以对特定的标签进行验证，其特点是简单、方便和快捷；移动式读写器是指读写器和后台服务器安装在不同位置，通过无线通信的方式进行信息的传输，以实现两者之间的信息交互[23]。

2.1.3 后台服务器

后台服务器一般指具有强大数据分析能力和存储能力的数据库系统，它能接收并处理读写器传递来的信息，进而实现对标签的管理和控制，这一过程涉及到相关信息的查找、判断、更新等安全验证操作。后台服务器可以根据实际需求来选择其硬件平台，在不同的应用环境，它可以是一台电脑，或是一台大型机，抑或是云平台，在其数据库中存储着 RFID 系统中所有标签标识信息[24]。

2.1.4　RFID 工作原理

在 RFID 系统中，如图 2.1 所示，读写器通过射频天线向自由空间发射一定频率的电磁波，当标签处在射频天线辐射区域内，标签将接收来自无线信道的电磁能量并将其转化为电能，标签内部芯片由于获得能量而被激活，经过加密计算后，标签利用内置天线将标签标识等数据信息发射到自由空间，读写器的接收天线将接收来自标签发送的信号，经过解调器和解码器等处理过程，再将信息传送至后台服务器，后台数据库进行相关的计算、查找和验证工作，从而做出相应的处理[25]。

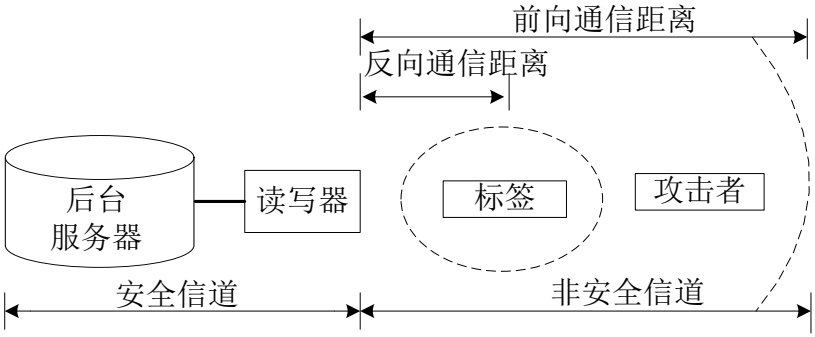

图 2.1 RFID 系统工作原理

一般来讲，读写器和后台服务器之间的有线信道被视为安全信道，标签和读写器之间的无线信道则被认定为不安全信道，不安全信道是攻击者获得有用信息的主要来源[26]，本文提出的改进 RFID 认证协议基于以上合理假设。

2.2　RFID 系统设计要求

为保证 RFID 系统的完整性、真实性和隐私性，RFID 系统设计主要从计算、存储、通信成本等性能方面和安全隐私性方面进行考量[27]，具体的设计需求主要从以下几方面进行。

2.2.1　性能方面

在 RFID 系统中，认证协议主要考虑以下性能方面需求：

1．存储成本：标签内存储信息尽量少。由于标签内逻辑门电路规模和安全隐私等因素的限制，标签内应该尽量减少复杂计算和隐私信息的存储，仅保留必要加密信息以确保标签正常工作。

2．计算成本：标签的计算强度以及服务器的时间复杂度尽量小。考虑到低成本被

动标签并没有内置能量源，标签仅仅依靠读写器供给的能量正常工作，因此标签的计算能力是有限的；服务器的计算复杂度决定了 RFID 系统的可扩展性[28]。随着 RFID 系统应用规模逐渐庞大，在服务器的数据库中，如果不采用合理的标签查找算法，那么加密计算的时间复杂度将会达到线性阶 O(n)以上，将导致系统的可扩展性较差，所以应该降低服务器加密计算的时间复杂度，从而确保系统的运行效率。

3．通信成本：标签、读写器以及后台服务器在执行一次完整的验证过程中，应该尽量减少三者所需要传递信息的长度和交互回合数。为了保障传输信息安全和提高信息传输效率，在满足系统正常需求的前提下，RFID 系统应该尽量减少三者之间的通信成本。

2.2.2 安全隐私方面

随着 RFID 系统应用规模日益庞大，RFID 系统安全隐私方面的问题进一步凸显，如果不能保障系统的安全和隐私，那么系统中涉及到的个人隐私、商业以及国家机密等信息将会被不法分子获取并加以利用，必将造成人身财产安全、商业机密和国家安全等一系列危机[29]。因而，RFID 系统的安全和隐私问题在某种程度上决定了 RFID 技术能否更大规模应用和推广。

由于标签和读写器之间通过无线信道通信，因此攻击者比较容易截获两者之间的交互信息并加以利用，从而导致系统的完整性、真实性和隐私性遭到破坏[30]。所以针对标签和读写器之间无线信道通信这一薄弱点，我们应该采取相应措施和方法进行保护，目前，保护机制主要分为物理机制和密码机制。现有的基于物理机制的方法无法满足日益多变的 RFID 系统的安全性，因此，从事密码安全机制的研究势在必行。此外，低成本被动标签存在诸多限制，要求 RFID 系统安全机制的选择不易过于复杂。因此，在合理的假设前提下，设计出一种满足安全和隐私方面要求的认证协议是具有挑战性的。现阶段，RFID 系统所面临的攻击手段可分为两大类：主动攻击和被动攻击。主动攻击是攻击者访问所需信息的故意行为，包括假冒攻击，重放攻击、中间人攻击以及去同步攻击等；被动攻击是攻击者窃听或截获所需信息的行为，包括窃听、定位跟踪等[31]。针对以上两类攻击方式，具体分析如下：

1．重放攻击：在 RFID 认证协议中，重放攻击是指攻击者通过窃听等方式获取认证信息，冒充合法个体不断恶意或欺诈性地重复某一消息，欺骗系统并破坏系统认证过程。从攻击对象的角度来看，重放攻击可分为对标签的重放攻击、对读写器的重放攻击以及对服务器的重放攻击。

2．假冒攻击：假冒攻击可分为假冒标签和假冒读写器攻击。在协议执行过程中，攻击者通过一定手段获取标签或读写器的认证信息，在下一个验证回合，攻击者冒充标签或读写器，与读写器或标签进行信息交互，合法的读写器和标签做出响应，从而达到欺骗读写器和标签的目的。

3．不可追踪隐私：不可追踪隐私通常指攻击者使用非法读写器向标签发起询问，得到标签响应信息后，分析加密信息数据特征以实现对标签的位置隐私进行追踪。例如，在协议执行过程中，标签的响应信息一直不变，将会导致标签易受到定位追踪，用户的位置隐私将被暴露。

4．前向安全性：在协议执行过程中，攻击者截获本次会话过程中信息，并且分析和破解当前会话信息，得到用户相关的历史有用信息。例如，当协议不满足前向安全性，攻击者窃听到当前时刻用户标签发出的信息，它便有能力获取前一时刻用户标签的敏感信息，这将危及到用户的人身和财产安全。

5．去同步化攻击：安全协议执行过程中，后台服务器与标签之间由于硬件故障或者人为破坏等因素，导致系统中标签、读写器、服务器之间联系中断，使得标签和后台服务器之间的认证标识未及时更新，系统失去同步，严重情况下，可造成系统瘫痪。因此，在设计认证协议过程中，应考虑到去同步化攻击的影响。

2.3　RFID 安全机制

针对上述一系列安全问题，业界学者们已经提出了许多种解决方案并且取得了一定成果。目前来讲，物理安全机制和密码安全机制是 RFID 安全机制中两大分支[32]。虽然物理机制和密码机制有着各自的优势，但是基于密码机制的安全协议是近年来研究的热点。

2.3.1　物理安全机制

物理安全机制是指用物理方法使电子标签和读写器无法正常通信，主要包括：Kill 指令机制、阻止标签法、电磁屏蔽法等[33]。在某些领域，比如零售、物流等行业，考虑到标签成本问题，物理安全机制并不适合大范围推广和应用。表 2.3 列出了一些物理机制的优缺点。

表 2.3 RFID 物理安全机制的比较

物理机制	优点	缺点
Kill 指令机制	可阻止扫描及被追踪	标签不可重复使用
阻止标签法	成本低	可被用于恶意攻击
电磁屏蔽法	可阻止扫描	增加成本，使用不便
标签剪裁法	可阻止远端扫描和跟踪	无法防止近处攻击
主动干扰法	可屏蔽标签	实现成本高

从以上几种物理机制可以看出，物理安全机制虽然简单方便并且一定程度上解决了现存的安全隐私问题，但是这些方法只能提供简单的保护，同时还存在应用环境等方面因素的限制[34]。总而言之，现有的基于物理机制的方法无法满足日益多变的 RFID 系统的安全性，因此，从事密码安全机制的研究势在必行。

2.3.2 密码安全机制

随着 RFID 技术的广泛应用和快速发展，大量学者提出了基于密码安全机制 RFID 认证方案。但遗憾的是，厂商和供应商主要考虑标签成本而忽视系统的安全隐私问题，学者则更多从安全隐私角度研发 RFID 系统各部件而忽略成本问题，由于设计者的出发点不同，现阶段 RFID 系统的解决方案并不尽人意。因此，只有根据具体的应用环境和不同的安全指标，才能设计出安全隐私和硬件成本均衡的认证协议[35]。一般情况下，根据系统计算复杂度和操作复杂性可将协议划分为三类：轻量级、中量级和重量级认证协议。

轻量级认证协议主要采用计算存储量较小的简单逻辑运算、移位运算等操作，用简单易行的操作代替复杂的加密算法。其中，HB 族协议[36]和物理不可克隆函数协议[37]具有代表性，此类协议的显著特点是计算、存储以及通信量小，但是抵御攻击能力较差，安全性受到了业界学者的质疑，因此限制了轻量级认证协议的应用和发展。

中量级认证协议主要采用散列函数和简单的逻辑运算等操作，其中，散列函数的计算复杂度以及操作复杂性介于轻量级和重量级之间。基于散列函数的 RFID 认证协议依据协议中标签标识 *ID* 是否更新大致可分为：静态 *ID* 机制和动态 *ID* 机制[38]。其中，静态 *ID* 机制在每一轮的认证过程中标签标识 *ID* 始终保持不变，其优点是计算步骤简单并可以抵抗去同步攻击，缺点是容易被窃听、定位追踪以及重放攻击；而动态 *ID* 机制在完成每一轮的认证过程后标签标识 *ID* 发生变化，其优点是可以抵御重放攻击

和定位追踪，并且标签所有权可转移，缺点是容易遭到去同步攻击[39]。综上所述，中量级认证协议既可以保障一定的安全性又能满足较高性能需求，并且可以应用到制造业、零售业、物流等领域，所以此类协议是当前研究的热点之一。

重量级认证协议主要采用计算复杂但安全系数高的加密算法，例如数据加密标准（DES）、公钥加密算法 RSA、椭圆曲线密码机制等[40]。在 RFID 系统中，DES 算法可以有效抵御假冒攻击，但是其密钥空间太小易受蛮力攻击；RSA 算法虽然安全强度较高，但要求标签电路拥有 10000 以上逻辑门，低成本标签无法实现；与以上两种算法比较，基于椭圆曲线密码机制的 RFID 认证协议，在计算存储开销、处理速度上都具有明显优势。此类协议非常适用于安全级别要求较高的应用场景，例如，安全防伪系统、军事安防系统、金融系统等领域[41]。

2.4 本章小结

本章主要对 RFID 系统的相关基本知识进行介绍，这些是后续课题研究的理论基础。首先对 RFID 系统组成部分和系统工作原理进行介绍，分别阐述标签、读写器和后台服务器的类型、属性以及特点。接着介绍 RFID 系统设计要求，从性能和安全隐私角度出发，考量标签计算存储成本以及系统通信成本，详细分析系统所面临的安全隐患，并给出了两种应对机制：物理机制和密码机制，对其优缺点进行归纳和总结。分析表明，Hash 函数和椭圆曲线密码机制在 RFID 认证协议中具有诸多优点，是目前研究此领域的热点。

第 3 章　基于散列函数的 RFID 认证协议

散列函数由于具备单向性、输出长度固定等一系列安全优势，常常被用作 RFID 安全认证协议之中，基于散列函数的 RFID 认证协议可以分为基于静态 *ID* 机制的认证协议和基于动态 *ID* 机制的认证协议。其中，静态 *ID* 机制，在每一轮的认证过程中标签标识 *ID* 始终保持不变，其优点是计算步骤简单并可以抵抗去同步攻击，缺点是容易被窃听、定位追踪以及重放攻击；而动态 *ID* 机制在完成每一轮的认证过程后标签标识 *ID* 发生变化，其优点是可以抵御重放攻击和定位追踪，并且标签所有权可转移，缺点是容易遭到去同步攻击。目前为止，基于散列函数机制的安全认证协议尚缺乏统一的标准。

为了满足人们对 RFID 系统的各种需求，业界学者们已经设计出多种基于散列函数的认证协议，但遗憾的是，大多数协议未够兼顾系统的安全隐私性和标签硬件需求，并且缺少必要的仿真验证环节，导致协议难以在实际系统和平台上实现。本章首先介绍散列函数的理论基础，分析现有的认证协议执行过程和安全性能需求，并指出其优势和劣势，在此基础上提出了一种改进协议。阐述协议执行过程和算法步骤，介绍一种形式化分析方法—BAN 逻辑，并采用 BAN 逻辑对本协议正确性加以证明，最后通过与现有的认证协议在安全性和性能方面比较，得出本协议具有安全隐私和性能等方面的优势。

3.1　散列函数理论基础

散列函数，又称哈希（Hash）函数，用于将任意长度的消息 *m* 映射为固定长度的、较短的消息摘要 H(*m*)。对于某个特定的消息而言，消息摘要可以看作是该消息的指纹，即消息的唯一表示[42]。散列函数的计算模型示意图如图 3.1 所示。从图中我们可以看出，散列函数的运算结果是通过其内部的压缩函数经过多轮的压缩而得出。由此可知，散列函数的核心是压缩功能，它可以顺序地处理这些分组，上一轮压缩函数的输出可以定义为本轮压缩函数的输入。

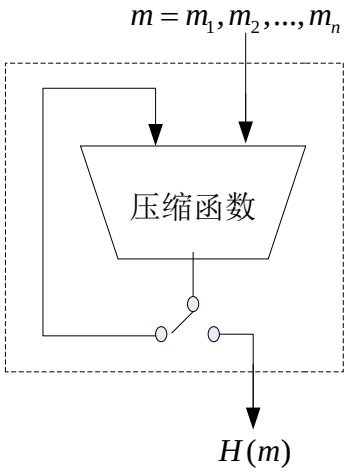

图 3.1 散列函数计算模型

散列函数可以处理任何长度的消息，并产生固定长度的输出。实际中，这主要通过将输入分割成一系列大小相同的分组实现的。散列函数的属性有如下几点[43]：

1．任意长度的消息大小，H(*m*)对任何大小的消息 *m* 都适用。

2．固定的输出长度，H(*m*)生成的散列值 *z* 的长度是固定的。

3．抗第一原像性，给定一个输出 *z*，找到满足 H(*m*)=*z* 的输入 *m* 是不可能的，即 H(*m*)具有单向性。

4．抗第二原像性，给定 m_1 和 $H(m_1)$，找到满足 $H(m_1)=H(m_2)$ 的 m_2 在计算上是不可能的。

5．抗冲突性，找到满足 $H(m_1)=H(m_2)$ 的一对 $m_1 \neq m_2$ 在计算上是不可行的。

由于散列函数具有如上特性，在设计 RFID 认证协议过程中，我们可以使用散列函数对明文信息进行加密，其计算存储开销较小，安全性较高，非常适合应用于 RFID 认证系统。

3.2 基于散列函数的 RFID 认证协议分析

基于散列函数的 RFID 认证协议可以分为基于静态 *ID* 机制以及基于动态 *ID* 机制。其中，典型的基于静态 *ID* 机制的认证协议包括：Hash-Lock 协议[44]、随机化 Hash-Lock 协议、Lee Y C 等人提出的协议、HSAP 协议等；基于动态 *ID* 机制的认证协议包括：Hash-Chain 协议[45]、LCAP 协议[46]、Osaka 等人提出的协议[47]。以上各个协议均有各自的优势和劣势，本节将介绍几种典型的基于散列函数的 RFID 安全认证协议，分析协议具体执行过程，指出认证协议的安全和性能方面的不足，在此基础上，提出一种基

于散列函数机制的改进协议。在认证协议中，*H*( )表示具有计算 Hash 函数的能力，*PRNG*( )表示伪随机数发生器。

3.2.1　随机化 Hash-Lock 协议

Weis 等人提出一种基于静态 *ID* 机制的随机化 Hash-Lock 协议，认证协议中使用 Hash 函数和伪随机数生成器对信息进行加密处理。初始状态，后台服务器存储着每个标签的标识 *ID*，认证协议的执行过程如图 3.2 所示。

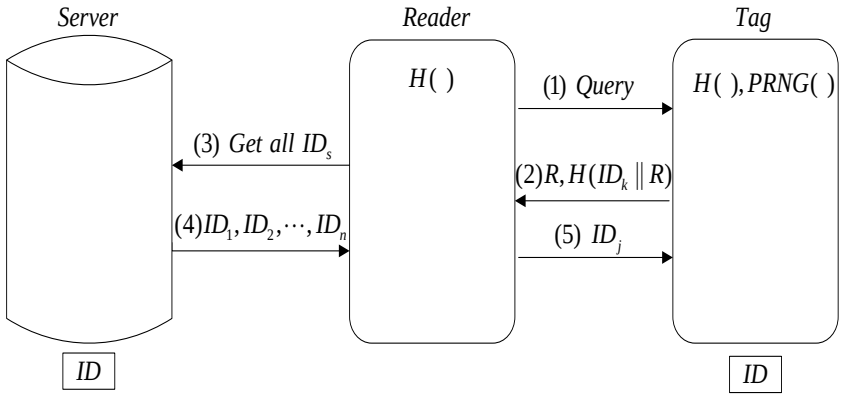

图 3.2 Hash-Lock 协议

随机化 Hash-Lock 协议具体认证过程如下：

1. 读写器向标签发送查询请求 *Query* 并等待标签响应；

2. 标签接收到读写器请求后，生成一个伪随机数 *R* 并计算 $H(ID_k \| R)$，其中，ID_k 表示第 *k* 个标签标识，标签将 *R* 和 $H(ID_k \| R)$ 发送至读写器；

3. 读写器接收到标签信息后，向后台服务器发出请求指令：提供所有标签标识 *ID* 信息；

4. 后台服务器收到请求信息后，将所有 *ID* 信息传送至读写器，读写器接收到所有 *ID* 信息后，计算满足等式 $H(ID_j \| R) = H(ID_k \| R)$ 成立的 ID_j，其中，$ID_j (1 \le j \le n)$，并将找出的 ID_j 发送至标签，否则认证失败。

5. 标签接收到认证信息 ID_j 后，验证 ID_j 是否等于 ID_k，如果相等，认证成功，否则认证失败。

随机化 Hash-Lock 协议是在 Hash-Lock 协议基础上改进而来，从安全性角度来看，随机化 Hash-Lock 协议在标签内部加入了伪随机数发生器，在每一轮认证过程中，标签发出的认证信息都是新鲜的，因此攻击者无法直接实施标签定位追踪攻击，但是在认证过程最后阶段，读写器直接向标签发送标签标识 *ID*，攻击者可以轻而易举的获取标签的标识信息，在此基础上，攻击者可以利用此标识信息对系统进行假冒、重放等

攻击。

从性能方面来看，随机化 Hash-Lock 改进了 Hash-Lock 协议中后台服务器的设置，减轻了后台服务器的计算负担，但是，读写器的计算复杂性明显提升。在每一轮的认证过程，读写器需要进行多次 Hash 运算，计算开销较大，并且后台服务器需要向读写器传递所有标识 *ID* 信息，通信量较大，导致系统的可扩展性较差并且运行效率较低，可以看出，系统的性能问题并没有真正得到解决。因此，随机化 Hash-Lock 协议不适用于低成本、高效率的 RFID 系统。

3.2.2 HSAP 协议

丁振华等人提出一种基于静态 *ID* 机制的 HSAP 协议，协议中标签和读写器使用伪随机数发生器和散列函数对信息进行加密处理，读写器具备过滤非法标签的能力。初始状态，后台服务器存储着每个标签的标识信息和相关信息，认证协议执行过程如图 3.3 所示。

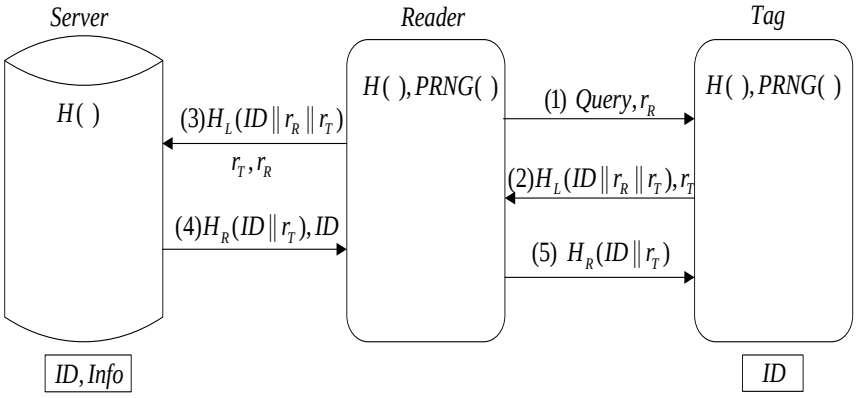

图 3.3 HSAP 协议

HSAP 协议具体认证过程如下：

1. 读写器生成一个随机数 r_R，向标签发送请求信息，同时将 r_R 发给标签；

2. 标签接收到读写器请求后，生成伪随机数 r_T 并计算 $H_L(ID\|r_R\|r_T)$，而后将 r_T 和 $H_L(ID\|r_R\|r_T)$ 发送给读写器；

3. 读写器接收到标签信息后，首先完成一个过滤操作：读写器根据前一次认证过程中缓存 ID' 计算 $H_L(ID'\|r_R\|r_T)$，如果 $H_L(ID'\|r_R\|r_T)=H_L(ID\|r_R\|r_T)$，那么过滤掉该标签，如果 $H_L(ID'\|r_R\|r_T)\neq H_L(ID\|r_R\|r_T)$，则读写器将信息 $H_L(ID\|r_R\|r_T),r_R,r_T$ 发送至后台服务器；

4. 后台服务器收到请求信息后，查找数据库中是否有 $ID_j(1\le j\le n)$，使得等式 $H_L(ID_j\|r_R\|r_T)=H_L(ID\|r_R\|r_T)$ 成立，如果有，后台数据库计算 $H_R(ID\|r_T)$，并将

$H_R(ID\|r_T)$ 和 ID 发送给读写器，否则认证失败；

5. 读写器收到 $H_R(ID\|r_T)$ 和 ID 后，首先存储标签标识 ID，并将 $H_R(ID\|r_T)$ 发送给标签，标签验证等式 $H_R(ID_j\|r_T)=H_R(ID\|r_T)$ 是否成立，如果成立，则认证通过，否则认证失败。

HSAP 协议是基于挑战—响应机制来实现双向认证的协议，协议过程简单明了，值得一提的是，RFID 系统通过读写器中的过滤操作，可以有效降低后台服务器的计算负载，并且避免攻击者对读写器的重放攻击。但是，在步骤 3 中 RFID 读写器仅仅缓存了前一次的标签标识信息，去判断等式 $H_L(ID'\|r_R\|r_T)=H_L(ID\|r_R\|r_T)$ 是否成立，依此过滤标签的做法具有一定的局限性。例如，攻击者使用非法的标签信息攻击读写器，此时读写器的过滤操作将会失效，并且会将非法的认证信息发送到后台服务器；此外，当后台服务器验证非法信息无效时，是否将非法标签标识 ID 发送至读写器也将成为问题。认证协议的过滤操作只对以往验证成功的标签有效，并不能抵抗非法标签的攻击。

从安全性来看，HSAP 协议利用伪随机数和散列函数实现双向认证，能有效防止定位追踪和假冒等攻击，但是，从以上分析可知，读写器的过滤操作并不能真正抵抗重放攻击，并且认证协议受制于静态 ID 机制，不能实现前向安全性和标签所有权转移等目标。

从性能方面来看，在后台服务器中查找某个标签标识 ID_j 过程中，需要运用线性搜索的方法，去验证等式 $H_L(ID_j\|r_R\|r_T)=H_L(ID\|r_R\|r_T)$ 是否成立，这种做法是不可取的，因为在每轮认证过程中，后台服务器需要平均进行$(n+1)/2$ 次 Hash 运算，其散列函数运算的时间复杂度达到了线性阶 $O(n)$，这将影响后台服务器的可扩展性，并且导致系统的运行效率大大降低，因而，此认证协议并不适用于低成本、高效率的 RFID 系统。

3.2.3　基于密钥更新协议

Srivastava 等人提出一种基于密钥值更新的认证协议，协议中标签使用伪随机数发生器和时间戳的方法对信息进行加密处理。初始状态，后台服务器存储着每个标签标识信息和密钥值，认证协议执行过程如图 3.4 所示。

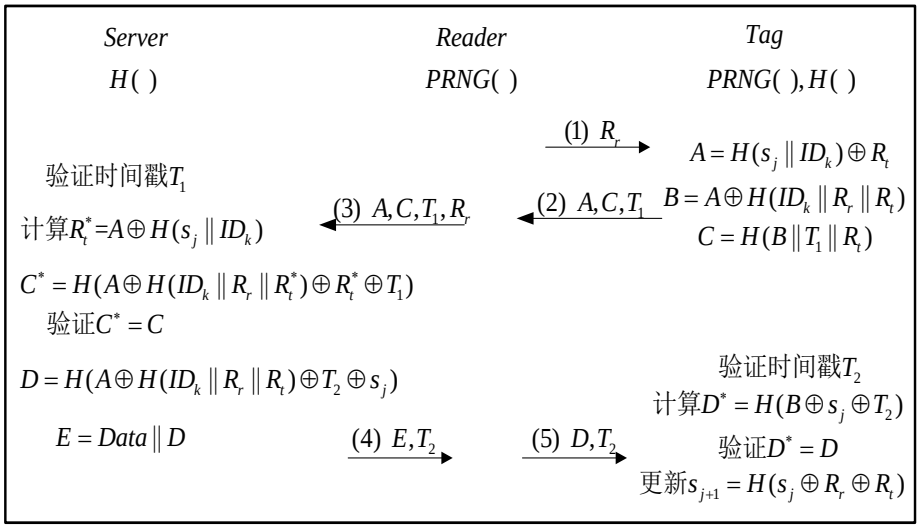

图 3.4 Srivastava 等人提出的协议

Srivastava 等人的认证协议具体认证过程如下：

1. 读写器生成一个伪随机数 R_r，并向标签发送查询请求，同时将随机数 R_r 发给标签；

2. 标签接收到请求后，生成伪随机数 R_t 并计算认证信息 $A=H(s_j \| ID_k)\oplus R_t$，$B=A\oplus H(ID_k \| R_r \| R_t)$，$C=H(B \| T_1 \| R_t)$，其中，$ID_k$ 表示第 k 个标签标识，T_1 是标签内部产生的时间戳，而后将 A,C,T_1 发送给读写器；

3. 读写器收到来自标签信息后，将认证信息 A,C,T_1 连同随机数 R_r 一起发送至后台服务器；

4. 后台服务器收到信息后，验证时间戳 T_1 是否有效，如果 $T_2-T_1\le\Delta T$，服务器计算 R_t^*=$A\oplus H(s_j \| ID_k)$，接着对找数据库中标签进行匹配查找，验证等式 $C^*=C$ 是否成立，如果成立，标签匹配成功，继续计算认证信息 D 并将时间戳 T_2 和消息 $E=Data \| D$ 发送至读写器，其中 $Data$ 是标签信息，否则认证失败；

5. 读写器收到认证信息 E 后，从 E 中解析出 $Data$ 信息，将 D 和 T_2 发送给标签；标签接收到信息后，首先验证时间戳 T_2 是否有效，如果 $T_3-T_2\le\Delta T$，标签计算认证信息 $D^*=H(B\oplus s_j \oplus T_2)$，并验证等式 $D^*=D$ 是否成立，如果成立，则说明后台服务器合法，此时更新服务器和标签两者之间的密钥值 s_j，$s_{j+1}=H(s_j \oplus R_r \oplus R_t)$，否则认证失败。

从安全性角度出发，Srivastava 等人提出的协议，采用时间戳、伪随机数发生器以及更新密钥值等方法，使系统能够抵抗重放、追踪等攻击，但是必须指出，认证协议还是存在部分安全隐私问题。其中，后台服务器和标签之间密钥更新存在同步问题，即标签认证成功后还需要通知后台服务器更新密钥，这使得系统更新很容易被攻击者

阻止，导致标签在下次认证时失效。此外，Sun 等人通过理论推导方式，已经证明该协议容易受到中间人攻击[48]。

从性能方面来看，在后台服务器中查找某个标签标识信息 ID_k 时，需要运用线性搜索方法，去验证等式 $C^* = C$ 是否成立，在每轮认证过程中，后台服务器平均进行 (n+1)/2 次 Hash 运算，其散列函数运算的时间复杂度达到了线性阶 O(n)，这将影响后台服务器的可扩展性，并且导致系统的运行效率大大降低。在此认证协议中，可以看出，标签具备生成时间戳和随机数的能力，这使得标签的硬件成本和复杂性大大提升，因而，此认证协议并适用于低成本、高效率的 RFID 系统。

3.3　基于散列函数的改进协议

3.3.1　协议初始条件和算法步骤

在认证协议初始阶段，服务器的数据库中存储 n 个标签标识、新旧索引值和秘密值，主要包括 $ID_{old}, ID_{new}, M'_{old}, M'_{new}, Key_{old}, Key_{new}$，其中 Key_{old} 表示前一次成功认证的秘密值，初始值为 0，Key_{new} 表示本次进行安全认证过程中新生成的秘密值，M'_{new}, M'_{old} 分别表示服务器通过 Hash 函数运算产生的新旧索引，ID_{old} 表示前一次成功认证的标识，初始值为数据库与标签共享的随机关键字，ID_{new} 表示本次进行安全认证过程中新生成的标识。标签存储着自己的标识 ID 和秘密值 Key，符号 ⊕ 表示异或操作，符号 ‖ 表示连接操作，X_L, X_R 分别表示信息 X 的左半部分和右半部分[49]。RFID 标签具备计算散列函数、产生随机数以及异或操作的能力，改进协议具体执行过程如图 3.5 所示，算法步骤如表 3.1 所示。

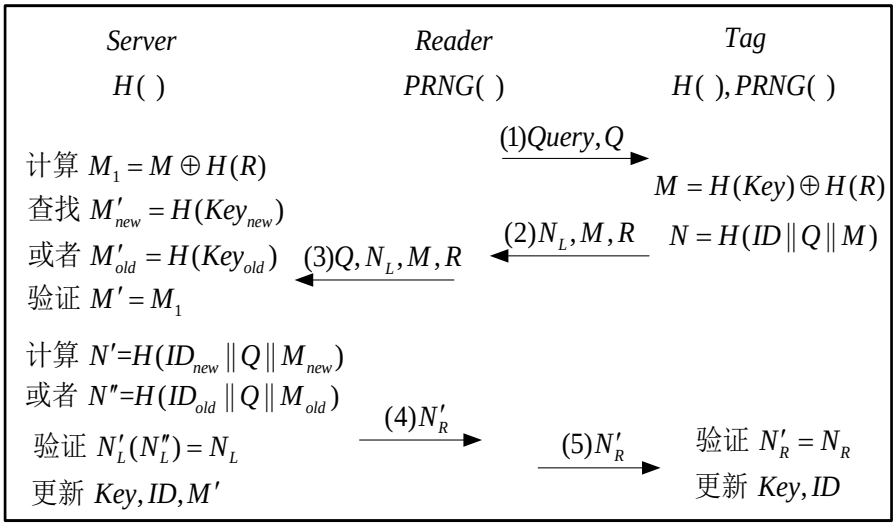

图 3.5 协议执行流程

表 3.1 改进协议算法步骤

Step1：	读写器向标签发送查询请求信息和随机数 Q，并等待标签响应；
Step2：	标签接收到请求信息后，生成随机数 R，并执行两次散列函数运算 $M = H(Key) \oplus H(R)$ 和 $N = H(ID \| Q \| M)$，并把认证信息 N_L、M 和 R 传回读写器；
Step3：	读写器收到来自标签信息后，将认证信息 M，N_L，R 连同 Q 一起发送至后台服务器；
Step4：	后台服务器收到信息后，首先计算 $M_1 = M \oplus H(R)$，然后在数据库中进行相关的匹配查找、计算、比较和更新： ➢ *If* $M'_{new} \neq M_1$，$M'_{old} \neq M_1$，认证失败，结束。 ➢ *If* $M'_{new} = M_1$，继续计算 $N' = H(ID_{new} \| Q \| M_{new})$，并且判断 N'_L 和 N_L 的关系， ➢ *If* $N'_L \neq N_L$，认证失败，结束。 ➢ *else* $N'_L = N_L$，标签被服务器认定为合法标签；并在数据库中做出更新 $Key_{old} = Key_{new}, M'_{old} = H(Key_{new}), Key_{new} = Key_{new} \oplus Q, M'_{new} = H(Key_{new} \oplus Q)$，$ID_{old} = ID_{new}, ID_{new} = ID_{new} \oplus M_R$； ➢ *If* $M'_{old} = M_1$，继续计算 $N'' = H(ID_{old} \| Q \| M_{old})$，并且判断 N''_L 和 N_L 的关系， ➢ *If* $N''_L \neq N_L$，认证失败，结束。 ➢ *else* $N''_L = N_L$，标签被服务器认定为合法标签，并在数据库中做出更新 $Key_{new} = Key_{new} \oplus Q, M'_{new} = H(Key_{new} \oplus Q), ID_{new} = ID_{new} \oplus M_R$； 当服务器认定此标签为合法标签并且在后台数据库中做出相应更新后，服务器将认证信息 N'_R 发回读写器，读写器接收到消息后，将认证信息 N'_R 转发给标签；
Step5：	标签收到信息后，依据步骤 2 计算的 $N = H(ID \| Q \| M)$，判断 N'_R 和 N_R 的关系， ➢ *If* $N'_R = N_R$，实现了标签和服务器之间的双向认证，做出相应的更新，$Key_{new} = Key_{new} \oplus Q$，$ID_{new} = ID_{new} \oplus M_R$； ➢ *else* $N'_R \neq N_R$，认证失败，结束。
结束	

3.3.2　协议的 BAN 逻辑分析和证明

认证协议的目标不单单是为了实现信息的加密传输，更重要的是为了解决 RFID 系统中的安全问题，它的正确性对于系统安全是极其关键的[50]。但是认证协议的设计是困难且易于出错的，直观的原因是认证协议是在攻击者存在的情况下的异步通信，攻击者能够窃取、截获以及篡改所交换的信息。因此认证协议的执行具有高度的不确定性，即便是对有限约束条件下的认证协议也要求分析潜在无限可能的攻击者行为。也就是说，有些认证协议往往不如它们的设计者所期望的那样安全，其实，认证协议中的很多缺陷和漏洞往往不是因为协议中使用的密码算法引起的，而是由协议自身的结构引起的[51]。

因此，我们有必要利用形式化的分析方法对认证协议的正确性进行一系列分析和验证。形式化分析方法 BAN 逻辑是在抽象层面上分析和验证协议执行过程的安全问题[52]。BAN 逻辑基本符号和术语如表 3.2 所示。

表 3.2 BAN 逻辑基本符号和术语

符号或术语	含义
P,Q	通信主体
X,Y	一般意义上的语句
(X,Y)	X 和 Y 的连接
$P\mid\equiv X$	P 相信 X，P 认为 X 为真
$P\lhd X$	P 看到过 X，P 曾收到包含 X 的消息，P 能读出并重复 X
$P\mid\Rightarrow X$	P 对 X 有控制权，或有管辖权
$P\mid\sim X$	P 曾经说过 X，P 在某一刻曾发送过包含 X 的信息
$\#(X)$	X 是新鲜的，指协议执行之前未被传送过
$\langle X\rangle_Y$	X 和 Y 的组合，Y 是一个秘密，它的出现证明是 $\langle X\rangle_Y$ 的身份
$P\overset{X}{\rightleftharpoons}Q$	X 是 P，Q 之间的共享秘密，且除 P 和 Q 以及他们相信的主体之外，其他主体都不知道 X

BAN 逻辑的推理规则

下面仅列举与本协议相关的 5 条规则：

1. 消息含义规则 $\dfrac{P\mid\equiv P\overset{Y}{\rightleftharpoons}Q,P\lhd\langle X\rangle_Y}{P\mid\equiv Q\mid\sim X}$

规则含义：若 P 相信 Y 是 P 与 Q 的共享秘密信息，并且 P 接收了信息 X 和秘密 Y 的级联$\langle X\rangle_Y$，则 P 相信 Q 发送过信息 X，以及秘密 Y 可以证明使用$\langle X\rangle_Y$ 的身份。

2. 新鲜性规则 $\dfrac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$

规则含义：若 P 相信 X 是新鲜，则 P 同样相信 X 和 Y 的级联的整体信息也是新鲜的。

3. 随机数验证规则 $\dfrac{P|\equiv \#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$

规则含义：若 P 相信 X 是新鲜，且 P 相信 Q 曾经传送过 X，则 P 相信，Q 相信 X。

4. 信仰规则 $\dfrac{P|\equiv Q|\equiv (X,Y)}{P|\equiv Q|\equiv X}$

规则含义：若 P 相信，Q 相信 X 和 Y 的级联整体信息，则 P 相信，Q 相信 X。

5. 管辖权规则 $\dfrac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$

规则含义：若 P 已经相信 Q 有权控制消息 X，且 P 相信 Q 也相信消息 X 时，则 P 相信消息 X，这条规则延拓了主体的推知能力。

改进协议的形式化模型

$S\rightarrow T$: Q

$T\rightarrow S$: $\{TID, Q, M\}_K, M, R$

$S\rightarrow T$: $\{SID, Q, M\}_K$

其中 S 表示后台服务器，T 表示标签，K 表示秘密值 Key，R，Q 表示随机数，在 BAN 逻辑形式化分析时，不影响协议流程和安全性的前提下，为了形式化表达简洁，常常将信息进行如下抽象，将读写器和后台服务器视为统一整体，其认证标识 SID，标签的认证标识为 TID。

本协议的安全目标：

$S|\equiv TID$

$T|\equiv SID$

其中 $S|\equiv TID$ 表示后台服务器相信标签的认证信息，$T|\equiv SID$ 表示标签相信后台服务器的认证信息。

协议的初始假设条件：

P1： $S|\equiv S\overset{K}{\rightleftharpoons}T$ 表示 S 相信 Key 是 S 和 T 的共享秘密；

P2： $T|\equiv T\overset{K}{\rightleftharpoons}S$ 表示 T 相信 Key 是 T 和 S 的共享秘密；

P3：$S \mid\equiv \#(Q)$　　表示 S 相信随机数 Q 是新鲜的；

P4：$T \mid\equiv \#(R)$　　表示 T 相信随机数 R 是新鲜的；

P5：$S \mid\equiv T \mid\Rightarrow TID$　　表示 S 相信 T 对认证标识 TID 有控制权限；

P6：$T \mid\equiv S \mid\Rightarrow SID$　　表示 T 相信 S 对认证标识 SID 有控制权限；

协议推理证明过程：

根据消息含义规则 $\dfrac{P \mid\equiv P \overset{Y}{\rightleftharpoons} Q, P \lhd \langle X \rangle_Y}{P \mid\equiv Q \mid\sim X}$，由假设条件 P1：$S \mid\equiv S \overset{K}{\rightleftharpoons} T$ 和已知条件 $S \lhd \langle TID, Q, M \rangle_K$，可得 $S \mid\equiv T \mid\sim (TID, Q, M)$；

根据新鲜性规则 $\dfrac{P \mid\equiv \#(X)}{P \mid\equiv \#(X, Y)}$，由假设条件 P3：$S \mid\equiv \#(Q)$，可得 $S \mid\equiv \#(TID, Q, M)$；

根据随机数验证规则 $\dfrac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$，由上述规则推得结果 $S \mid\equiv \#(TID, Q, M)$ 和 $S \mid\equiv T \mid\sim (TID, Q, M)$，可得 $S \mid\equiv T \mid\equiv (TID, Q, M)$；

根据信仰规则 $\dfrac{P \mid\equiv Q \mid\equiv (X, Y)}{P \mid\equiv Q \mid\equiv X}$，由 $S \mid\equiv T \mid\equiv (TID, Q, M)$，可得 $S \mid\equiv T \mid\equiv TID$；

根据管辖权规则 $\dfrac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$，由假设条件 P5：$S \mid\equiv T \mid\Rightarrow TID$ 和推得结果 $S \mid\equiv T \mid\equiv TID$，可得 $S \mid\equiv TID$，证毕。根据以上假设和规则，同理可证，$T \mid\equiv SID$。

认证协议设计过程中，容易出现逻辑错误、安全和性能问题，本文运用形式化分析方法 BAN 逻辑分析和证明认证协议，根据 BAN 逻辑规则和合理的初始假设条件，最终推导协议的安全目标：$S \mid\equiv TID$ 和 $T \mid\equiv SID$，为认证协议的正确性和安全性提供了可靠保障。

3.3.3　协议安全性分析

现有的基于 Hash 函数的认证协议，大多数都存在安全隐患或性能问题，本文提出的改进协议在保证低成本标签的条件下，能够有效抵御假冒、重放等各种攻击，具体分析如下：

（1）假冒攻击

在认证协议的执行过程中，攻击者向标签发送查询请求及随机数 Q，并且获得了标签响应信息。在下一个认证过程中，攻击者可以利用响应信息 M，N_L，R 假冒合法标签对读写器实施攻击。然而协议中每个验证回合标签和读写器都会产生新鲜的随机

数 R 和 Q，当读写器接收虚假信息并把此信息传给服务器，服务器首先计算 $M_1 = M \oplus H(R)$，由于攻击者得到的上一轮响应信息已经失效，后台数据库并没有与之匹配的索引信息 $H(Key)$，服务器和读写器不会做出任何响应，所以攻击者不能成功实施对读写器的假冒攻击。

（2）重放攻击

在 RFID 认证协议中，重放攻击是指攻击者通过窃听等方式获取认证信息，冒充合法个体不断恶意或欺诈性地重复某一消息，以达到欺骗系统的目的。在认证协议的执行过程中，攻击者向标签发送查询请求和随机数 Q，并且获得标签的响应信息 M，N_L，R，在接下来的过程中，攻击者可以利用标签响应信息对读写器和服务器发动重放攻击。由于协议认证过程中所传输的消息具有不可逆性，并且每轮认证过程中 Q，R，M 和 N_L 都是新鲜性，重放信息并不会通过服务器验证，所以攻击者的重放攻击是无效的。

（3）去同步化攻击

安全协议的执行过程中，服务器与标签之间由于硬件故障或者人为破坏等因素，导致系统中标签、读写器、服务器之间联系中断，使得标签和后台服务器之间的认证标识未及时更新，系统失去同步并造成系统瘫痪，这种攻击称之为去同步化攻击。在本协议中，由于后台服务器的数据库中存储着本次和前一次成功认证的标识 ID、秘密值 Key 以及索引信息 M'，即使 RFID 系统意外失步，合法标签和后台服务器仍然可以根据前一次的认证信息完成系统认证更新，因此系统可以抵御去同步化攻击。

（4）前向安全性

在协议执行过程中，攻击者截获本次会话过程中信息，并且分析和破解当前会话信息，得到用户相关的历史有用信息。在安全协议中，用户标签的标识 ID 和 Key 值是通过 Hash 函数加密双向认证后进行动态更新的，由于 Hash 函数是具有单向不可逆性，攻击者不能根据信息 N_L，M 和 R，在多项式时间内得到标签的标识 ID 和秘密值 Key，因此不能获取用户标签相关的历史信息，从而有效地确保了整个 RFID 系统的前向安全性。

（5）标签所有权转移

标签所有权转移的实质是新使用者 C 从旧使用者 B 接管了与标签进行交互验证的权限，将标签管理权限由旧使用者 B 服务器转移到新使用者 C 服务器上，标签所有权转移具体过程如下：服务器 B 首先执行一次标签验证更新过程，将认证信息 $ID,\ Key,\ M'$ 更新为 $ID_1,\ Key_1,\ M_1'$，服务器 B 通过安全信道将认证信息 $ID_1,\ Key_1,\ M_1'$

发送给服务器 C，其中，服务器 B 与服务器 C 通过对称密钥加解密等操作完成数据传输，新的所有者立即执行一次标签验证更新，至此标签所有权得到转移。

（6）可证明安全性

现有的大多数认证协议缺乏安全证明方法,仅仅对协议执行过程加以阐述和分析，导致协议容易出现原则性和逻辑性错误。本文提出的改进协议，利用形式化分析方法 BAN 逻辑对协议认证过程进行分析和验证，证明协议执行过程逻辑性是正确的，为 RFID 系统的安全提供了保障。

本文提出的改进协议和其他基于 Hash 函数的 RFID 认证方案从安全方面进行分析，可得比较结果如表 3.3 所示。通过比较我们发现，本协议能够有效抵御假冒、重放、去同步化等攻击，并且具备前向安全性、可证明安全性、标签所有权可转移等明显优势。

表 3.3 安全性比较

安全要求	文献[8]	文献[9]	文献[10]	文献[12]	本文方案
假冒攻击	N	Y	Y	Y	Y
重放攻击	N	N	N	Y	Y
前向安全性	N	N	N	Y	Y
去同步化攻击	Y	Y	Y	N	Y
可证明安全性	N	N	Y	N	Y
标签所有权转移	N	N	N	Y	Y

其中，Y 表示满足该安全需求； N 表示不满足。

3.3.4 协议性能分析

本文主要从协议的存储成本、计算成本、传输成本、硬件需求、时间复杂度等性能方面与其他协议进行比较，如表 3.4 所示，分析发现，在存储成本方面，标签内部需要长度为 $2l$ 的存储空间，很好地满足存储资源受限的低成本 RFID 系统。在硬件需求方面，标签仅需使用散列函数和随机数生成器，并不需要生成时间戳等其它功能，使硬件成本得到较大节省。在计算成本方面，每轮认证过程中，标签仅仅需要计算 3 次散列函数并产生一次随机数，较好地控制了标签的计算成本。在传输成本方面，协议传输过程中，我们将散列函数计算结果拆分成左右两部分，并传送其中一部分，从而有效降低服务器和标签的传输成本。对于服务器的时间复杂度方面，服务器将收到

加密信息在数据库中进行简单地匹配查找和计算，使得后台数据库中散列函数计算的时间复杂度降低为常数阶 O(1)，这不仅让系统的运行效率大大提升，而且使系统具有良好的可扩展性。

表 3.4 性能比较

性能要求	对比项	文献[8]	文献[9]	文献[10]	文献[12]	本文方案
存储成本	Tag	1*l*	2*l*	1*l*	2*l*	2*l*
计算成本	Tag	1*h*+*r*	4*h*	2*h*+*r*	5*h*+*r*	3*h*+*r*
	Server	0*h*	(*n*+3) *h*	(*n*+1) *h*/2	(*n*+1)*h*/2	3*h*
传输成本	Total	2*l*	3*l*	1*l*	3*l*	2*l*
硬件需求	Tag	*h* , *P*	*h*	*h* , *P*	*h*, *P*, *T*	*h* , *P*
时间复杂度	Server	0*h*	O(*n*)	O(*n*)	O(*n*)	O(1)

其中，‘*l*’表示标签标识长度或密钥长度抑或是 Hash 函数输出长度，’*r*’表示随机数生成操作，’*n*’表示标签数量，’*h*’表示 Hash 函数操作，’*P*’表示随机函数生成器，’*T*’表示时间戳，传输成本是指标签和读写器之间总共的传输成本。

3.4 本章小结

本章主要研究了基于散列函数的 RFID 认证协议，简要地介绍散列函数的理论基础，针对现有的典型的基于散列函数的 RFID 安全协议，进行详细的分析和总结。在此基础上，提出了一种改进协议，阐述协议执行过程和算法步骤，运用形式化分析方法 BAN 逻辑分析和证明认证协议的正确性。在改进协议设计过程中，我们既考虑到 RFID 系统的局限性和特殊性，又兼顾了系统安全和隐私性。通过安全性分析和比对，可以看出本协议能有效抵抗重放、假冒、去同步等攻击，通过性能分析和对比，能够得出本协议具有计算、存储、传输成本少，标签硬件要求低，可扩展性强等优势。分析表明，本协议适用于低成本、高效率的 RFID 系统。

第 4 章　基于椭圆曲线的 RFID 认证协议

RFID 技术发展初期，由于标签硬件资源和计算存储能力有限，基于简单逻辑运算和单向函数的 RFID 认证协议是业界学者的研究重点。随着科技的发展，微电子技术和芯片工艺的进步，标签的计算存储能力显著提升，复杂的密码算法在标签上应用成为可能。目前，对 RFID 系统认证协议的研究，部分学者热衷于公钥密码体制。相比基于简单逻辑运算和单项函数的认证协议，公钥密码体制具有公私钥分离、密钥管理简单、扩展性良好等优势[53]。根据底层设计不同，将公钥算法总共分三类：整数分解方案、离散对数方案和椭圆曲线方案。在使用公钥算法时，常常需要考虑安全等级和密钥长度的问题，三种方案的安全等级和位长度的对比如表 4.1 所示，可以看出，在相同的安全级别情况下，椭圆曲线密码体制所要求的密钥长度最短。椭圆曲线密码体制凭借性能（更少的计算量）和带宽（更短的签名和密钥）优势，在现今的各种领域得到了广泛应用，尤其在无线通信、物联网等领域[54]。其中比较有代表性的方案是将椭圆曲线密码机制应用到 RFID 认证协议，由于 ECC 和 RFID 系统的结合，能够满足较高的安全需求并且适用于多种工作环境，所以设计出一个基于 ECC 的 RFID 认证协议具有现实意义。

表 4.1 不同算法的安全等级所要求的密钥长度

算法家族	安全级别（位）			
	80	128	192	256
整数分解	1024 位	3072 位	7680 位	15360 位
离散对数	1024 位	3072 位	7680 位	15360 位
椭圆曲线	160 位	256 位	384 位	512 位

4.1　椭圆曲线理论基础

椭圆曲线密码机制的理论基础是数论，ECC 是基于推广的离散对数问题，离散对数往往涉及到循环群上的操作，因此，我们首先要找到一个可以构建密码体制的循环群[55]。接下来介绍群、环、域的定义及属性。

1. 群

定义：群是一种代数结构，由一个非空的对象集合以及一个二元运算组成。群具

有以下属性和分类：

（1）封闭律：$\forall a,b \in G$，都有 $aob = c \in G$。

（2）结合律：$\forall a,b,c \in G$，都有 $ao(boc) = (aob)oc$。

（3）单位元律：$\exists e \in G$，使得 $\forall a \in G$，都有 $aoe = eoa = a$，其中，元素 e 称为单位元。

（4）可逆律：$\forall a \in G$，$\exists a^{-1} \in G$，使得 $aoa^{-1} = a^{-1}oa = e$，其中，元素 a^{-1} 称为 a 的逆元。

（5）有限群：如果在集合 G 中元素个数是有限的，则称该群 G 为有限群，反之，称为无限群。

（6）阿贝尔群（交换群）：对于 $\forall a,b \in G$，都满足 $aob = boa$，则称该群 G 为阿贝尔群或可交换群。

（7）循环群：$\exists a \in G$，使得 G 的任意元素都是由 a 的幂组成，则称该群为循环群，元素 a 称为循环群 G 的生成元或本原元。

2. 环

定义：一个具有加法（+）和乘法（$\bullet$）两种运算的集合，如果满足如下性质，则称为环 R，

（1）R 在加法运算下是阿贝尔群，加法单位元记为 0（称为零元）；

（2）R 在乘法运算下满足封闭律、结合律、单位元律，乘法单位元记为 1（称为单位元），$1 \neq 0$。

（3）交换律：$\forall a,b \in R$，都有 $a \bullet b = b \bullet a$。

（4）分配律：$\forall a,b,c \in R$，都有 $a \bullet (b+c) = a \bullet b + a \bullet c$。

3. 域

定义：如果一个环中的非零元在乘法运算下构成群，那么该环被称为域。域 F 具有以下特征：

（1）域 F 中的所有元素形成一个加法群，对应的群操作为“+”，中性元为 0。

（2）域 F 中除 0 外所有元素构成一个乘法群，对应群操作为“$\bullet$”，中性元为 1。

（3）当混合使用这两种群操作时，分配律始终成立，即对 $\forall a,b,c \in F$，都有 $a \bullet (b+c) = a \bullet b + a \bullet c$。

（4）有限域：只有有限个元素的域称为有限域或伽罗瓦域，记为 $GF(p^n)$。域中所包含的元素个数称为有限域的阶或基。令 $m = p^n$，当且仅当 m 是素数幂时，阶为 m 的域才存在，其中，n 为正整数，p 为素数，并称 p 为有限域的特征。

（5）素域：在有限域中，当 $m = p^n$ 中 n=1，p 为素数时，这种有限域被称为素域，记为 $GF(p)$ 或 $\mathbb{Z}_p$。

4.1.1　椭圆曲线定义

椭圆曲线并不是圆锥曲线中的椭圆曲线，而是因为其曲线方程是一个三次方程，与计算椭圆周长的积分表达式十分相似，故称之为椭圆曲线[56]，它由如下方程：

$$y^2 + axy + by = x^3 + cx^2 + dx + e \quad \text{.....(4.1)}$$

以及一个无穷远点 ∞ 构成，其中 a, b, c, d, e 是满足一定条件的实数。

在实数域上定义的椭圆曲线都是连续的曲线，实数域上的椭圆曲线如图 4.1 所示。

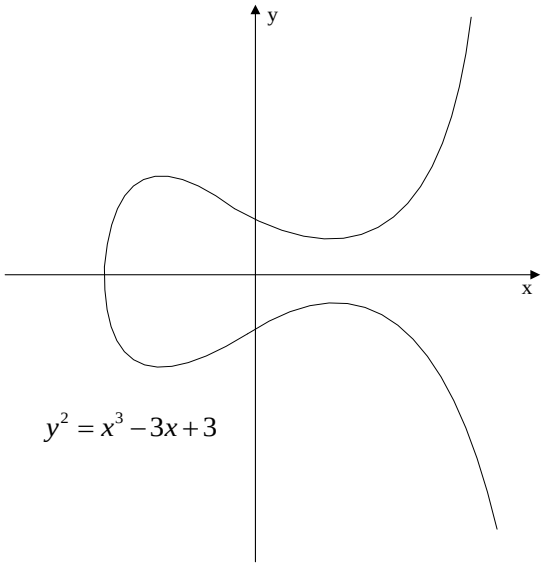

图 4.1 实数域上椭圆曲线示意图

椭圆曲线是一种特殊的多项式方程，密码学中使用的通常不是实数域内曲线，而是有限域内的曲线。在有限域 $GF(p^n)$ 中，素数域 $\mathbb{Z}_p$ 上的椭圆曲线是经常用于加密体制中的一种。接下来介绍素数域上的椭圆曲线方程。

定义：素数域 $\mathbb{Z}_p(p > 3)$ 上的椭圆曲线是指满足以下条件所有坐标 $(x, y) \in \mathbb{Z}_p$ 的集合

$$y^2 = x^3 + a \cdot x + b \bmod p \quad \text{.....(4.2)}$$

以及一个无穷大的虚数点 ∞，其中 $a, b \in \mathbb{Z}_p$，并且满足条件 $4 \cdot a^3 + 27 \cdot b^2 \neq 0 \bmod p$。

在上述定义中，要求椭圆曲线具有非奇异特性（椭圆曲线上的点有且仅有一条切线），此性质表明椭圆曲线不相交且没顶点，条件 $4 \cdot a^3 + 27 \cdot b^2 \neq 0 \bmod p$ 可以保证非奇异特性。

4.1.2 椭圆曲线上群操作

目前已经找到大循环群上的曲线，即确定了一组元素的集合。在椭圆曲线中，这些群元素指的是满足等式 4.2 的点。接下来，使用几何图形的方法，去定义这些点的群操作和相关运算[57]。

假设使用符号“+”表示群操作，在给定两点坐标 $P(x_1,y_1)$ 和 $Q(x_2,y_2)$ 的条件下，计算第三点 R 的坐标 (x_3,y_3)，即 $P+Q=R$，

$$(x_1,y_1)+(x_2,y_2)=(x_3,y_3) \quad (4.3)$$

考虑定义在实数域上的曲线，对应的几何图形可以更直观地说明加法操作。下面还以曲线 $y^2=x^3-3x+3$ 为例，介绍椭圆曲线上的群操作。在此之前，必须先区分两种不同的情况：两个不同点的加法（即相异点相加）和两个相同点相加（即相同点相加）。

相异点相加 $P+Q$：针对 $P+Q=R$，且 $P\neq Q$ 的情况。构建方法：画一条经过椭圆曲线不同位置 P,Q 的直线，该条直线与椭圆曲线相交于第三点，此点关于 x 轴的对称点即是点 R，如图 4.2 所示。

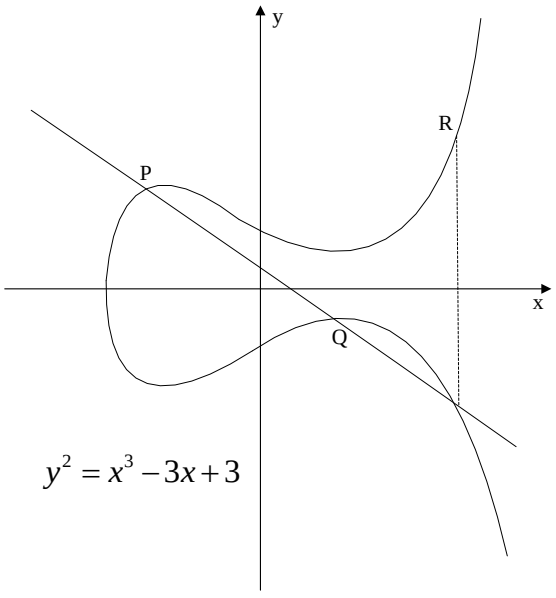

图 4.2 实数域上椭圆曲线相异点相加

相同点相加 $P+P$：针对 $P+Q=R$，且 $P=Q$ 的情况。构建方法：画一条经过 P 点的切线，该条切线与椭圆曲线相交于一点，此点关于 x 轴的对称点即是点 R，如图 4.3 所示。

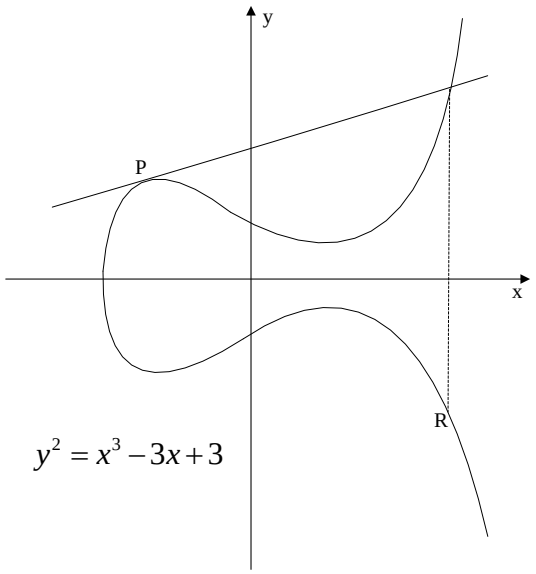

图 4.3 实数域上椭圆曲线相同点相加

当然，椭圆曲线密码体制的构建不可能使用这种简单的几何方法，有限域内椭圆曲线 E 的群操作需要使用如下群运算代数公式。

1. 单位元：任意的点 $P \in E\left(GF(p)\right)$，都有 $P+\infty=\infty+P=P$，将一个无穷的抽象点定义为单位元 ∞，这个无穷点可以看作是位于 y 轴正半轴或负半轴的无穷远处。

2. 逆元：若点 $P(x,y) \in E\left(GF(p)\right)$，且 $P+(-P)=\infty$，则群元素 P 的逆元是 $-P$，其坐标为 $(x,-y)$。

3. 点加：椭圆曲线上两个相异点 $P(x_1,y_1)$ 和 $Q(x_2,y_2)$，设 $P+Q=R$，R 的坐标为 (x_3,y_3)，可得：

$$x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2 \bmod p \quad \text{.....(4.4)}$$

$$y_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3)-y_1 \bmod p \quad \text{.....(4.5)}$$

4. 点倍：椭圆曲线上两个相同点 $P(x_1,y_1)$，设 $P+P=2P=R$，R 的坐标为 (x_3,y_3)，可得：

$$x_3=\left(\frac{3x_1^2+a}{2y_1}\right)^2-2x_1 \bmod p \quad \text{.....(4.6)}$$

$$y_3=\left(\frac{3x_1^2+a}{2y_1}\right)(x_1-x_3)-\mathrm{y}_1 \bmod p \quad \text{.....(4.7)}$$

4.1.3 椭圆曲线离散对数问题

定理 4.1 椭圆曲线上的点与无穷大的虚数点∞一起构成了循环子群，在某些条件下，椭圆曲线上所有的点可以形成一个循环群。

由定理可知，本原元一定存在，并且它的幂值生成了整个群。

定理 4.2 Hasse′s 定理

给定一个椭圆曲线 E 模 p，曲线上点的个数表示为 $\#E$，并且在以下范围内，

$$p+1-2\sqrt{p} \le \#E \le p+1+2\sqrt{p} \quad \text{.....(4.8)}$$

Hasse′s 定理也称为 Hasse′s 边界，它说明了点的个数大概在素数 p 的范围内。这个结论具有实用性，例如，如果需要一个包含 2^{160} 个元素的椭圆曲线，必须使用一个长度大约为 160 位的素数。

椭圆曲线离散对数问题（ECDLP）

已知一条椭圆曲线 E，椭圆曲线上的本原元 $P \in E(GF(p))$，P 的阶为 n，群 $\langle P \rangle = \{P, 2P \cdots, nP\}$是由 P 生成的循环子群，给定另一个元素 $Q \in \langle P \rangle$，则椭圆曲线离散对数问题是求整数 $k \in [0, n-1]$，使其满足 $kP = Q$。在密码体制中，k 是私钥，公钥 $Q(x, y)$ 是曲线上的一点。

椭圆曲线密码体制的安全隐私性是基于椭圆曲线离散对数问题，在求解大素数和模运算过程中，给定 P 和 Q，求 k 是非常困难的事情，目前还没有找到计算离散对数问题的快速算法。

4.2 基于椭圆曲线的 RFID 认证协议分析

近年来，业界学者已经提出多种基于 ECC 的 RFID 认证协议，其中，Tuyls 和 Batina 提出的基于 ECC 的 RFID 认证方案，该协议认证过程过于简单，仅仅实现了服务器对标签的单向认证，攻击者可以利用截获的认证信息对标签实施定位追踪，并且协议的计算开销较大、可扩展性较差；在此基础上，为了抵抗追踪攻击，Lee 等人提出了 EC-RAC 协议，在性能方面较 Tuyls 的协议有所提高，但是该协议还是无法抵御追踪攻击，并且仅仅实现了单向认证，难以确保系统的安全和稳定；O'Neill 等人提出的 ECC 认证方案中，应用散列函数和数字签名机制，该协议能够抵御假冒、重放等攻击，并且还能够抵抗追踪攻击，然而却存在计算开销大、可扩展性差等问题；何剑辉提出的改进协议，由于协议执行过程中传递的信息都是新鲜的，攻击者无法成功实施对标

签的追踪攻击，但是该协议不能抵御对服务器的重放攻击和对标签的假冒攻击，并且后台数据库需要通过线性搜索的方式去查询标签公钥值和标识信息，所以导致服务器计算开销较大、系统可扩展性较差；本节将介绍几种典型的基于椭圆曲线的 RFID 认证协议，给出协议算法步骤，分析协议的执行过程，指出协议的安全和性能等方面的优劣。由于攻击者仅在标签和读写器之间无线信道进行攻击，因此可以把读写器和后台服务器视为统一整体，以便更清楚地研究整个认证过程。

1．EC-RAC 协议

Lee 等人提出的 EC-RAC 协议，初始状态，后台服务器存储着自己的公私钥信息 $\{y, Y(=yP)\}$ 以及每个标签标识信息 $\{x_1, X_1(=x_1P)\}$ 和公钥值 $X_2(=x_2P)$，标签存储着自己的公私钥信息 $\{x_2, X_2(=x_2P)\}$、标签标识信息 $\{x_1, X_1(=x_1P)\}$ 以及后台服务器的公钥值 $Y(=yP)$，认证协议执行过程如图 4.4 所示。

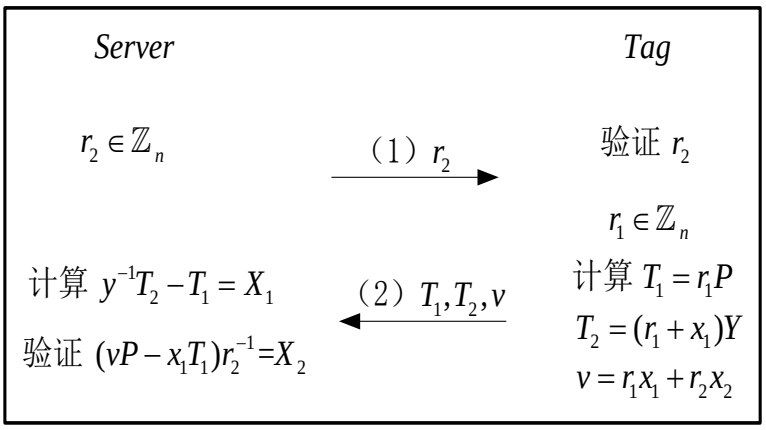

图 4.4 EC-RAC 协议

协议的具体认证过程如下：

（1）后台服务器生成一个随机数 $r_2 \in \mathbb{Z}_n$，向标签发送请求信息，同时将随机数 r_2 发送给标签；

（2）标签接收到请求后，首先检验 r_2 是否为零，如果 $r_2 = 0$，认证失败；如果 $r_2 \neq 0$，标签生成一个随机数 $r_1 \in \mathbb{Z}_n$，计算：

$$T_1 = r_1P \quad \text{.....(4.9)}$$

$$T_2 = (r_1 + x_1)Y \quad \text{.....(4.10)}$$

$$v = r_1x_1 + r_2x_2 \quad \text{.....(4.11)}$$

并将信息 T_1，T_2，v 发送给服务器；

（3）后台服务器接收到信息后，计算：

$$y^{-1}T_2 - T_1 = X_1 \quad \text{.....(4.12)}$$

并根据 X_1 检索数据库，查找与其匹配的信息 x_1 和 X_2，验证 $(vP-x_1T_1)r_2^{-1}$ 是否与 X_2 相等，如果相等，此标签被认定为合法标签，否则认证失败。

其中，验证过程中具体计算如下：

$$y^{-1}T_2-T_1=(r_1+x_1)P-r_1P=X_1 \quad \text{.....(4.13)}$$

$$(vP-x_1T_1)r_2^{-1}=[(r_1x_1+r_2x_2)P-x_1r_1P]r_2^{-1}=X_2 \quad \text{.....(4.14)}$$

在性能方面，Lee 等人提出的 EC-RAC 协议，由于协议中后台数据库需要通过线性搜索的方式查询标签公钥值和标识信息，所以导致后台服务器计算开销较大、系统可扩展性较差。在安全性方面，该协议容易受到攻击者的跟踪攻击，具体攻击方式如下，攻击者产生随机数 n 并向标签连续两次发出认证请求信息，攻击者可以得到两组不同的认证信息，在两次认证过程中，假设标签产生两个不同的随机数 r_1 和 r_2，并且回传的信息分别为 $\{T_1,T_2,v\}$ 和 $\{T_1',T_2',v'\}$，其中：

$$\{T_1,T_2,v\}=\{r_1P,(r_1+x_1)Y,r_1x_1+nx_2\} \quad \text{.....(4.15)}$$

$$\{T_1',T_2',v'\}=\{r_2P,(r_2+x_1)Y,r_2x_1+nx_2\} \quad \text{.....(4.16)}$$

攻击者根据两次收到的信息计算：

$$(v-v')^{-1}\cdot(T_2-T_2')=\{(r_1-r_2)x_1\}^{-1}\cdot(r_1-r_2)Y=x_1^{-1}Y \quad \text{.....(4.17)}$$

其中 $x_1^{-1}Y$ 是固定值，因而攻击者能够据此对标签实施跟踪攻击，并且该协议仅仅是一个单向认证协议，难以确保系统的安全和稳定。

2．O’Neill 等人的协议

在 O’Neill 等人提出的 ECC 认证方案中，应用散列函数和数字签名机制，初始状态，后台服务器存储着每个标签的公钥信息 $V_i(=-s_iP)$，标签存储着自己的私钥信息 s 和公钥信息 $V(=-sP)$，认证协议执行过程如图 4.5 所示。

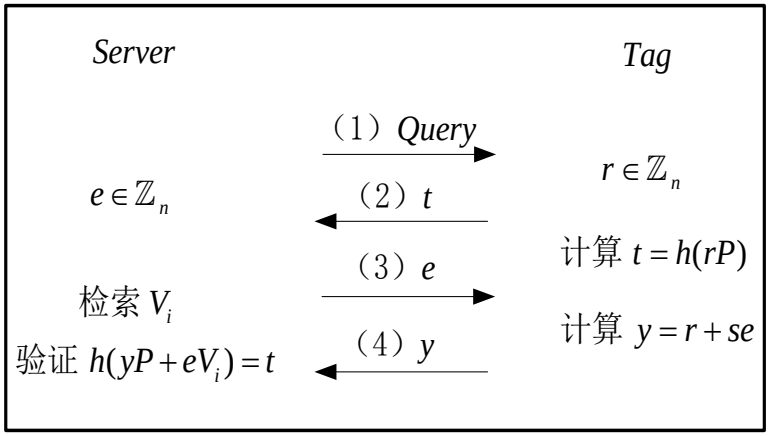

图 4.5 O’Neill 等人的协议

协议的具体认证过程如下：

（1）后台服务器向标签发送查询请求 *Query*，并等待标签响应；

（2）标签接收到请求后，标签当即生成随机数 $r \in \mathbb{Z}_n$，计算 $t = h(rP)$，并将信息 t 发送给后台服务器；

（3）后台服务器接收到消息后，首先暂存认证信息 t 并生成随机数 $e \in \mathbb{Z}_n$，然后将随机数 e 发送给标签；

（4）标签接收到随机数 e 后，计算认证信息 $y=r+se$，并将认证消息 y 发送给后台服务器；

（5）后台服务器接收到信息后，首先检索后台数据库中的公钥 V_i 信息，计算 $h(yP+eV_i)$，并验证 $h(yP+eV_i)$ 与 t 之间的关系，如果等式 $h(yP+eV_i)=t$ 成立，标签匹配成功，服务器对标签认证成功；如果数据库中没有找到匹配的公钥信息，则表示认证失败。

其中，验证过程具体计算如下：

$$h(yP+eV_i)=h[(r+se)P+eV_i]=h(rP)=t \quad \text{.....(4.18)}$$

在安全性方面，在认证协议执行过程中，该协议利用散列函数机制和密钥随机化的方法，保证认证执行过程的安全性，即使攻击者获取了认证消息 t，e，y，也无法解析出标签和服务器的私钥信息，因而攻击者无法对标签和服务器成功实施假冒和重放攻击，亦无法成功实施对标签的追踪攻击。

在性能方面，由于协议中后台数据库需要通过线性搜索的方式去查询标签标识信息，所以导致后台服务器计算开销较大、系统可扩展性较差，并且协议仅仅实现单向认证，难以确保系统的安全和稳定。

3．何剑辉的协议

由于 EC-RAC 协议存在跟踪攻击等安全问题，O'Neill 等人的协议存在性能方面问题，在此基础上，何剑辉提出了一种基于 ECC 的 RFID 双向认证协议。初始状态，后台服务器存储着自己的公私钥信息 $\{s_S, P_S(=s_S P)\}$ 以及每个标签标识信息 *ID* 和公钥值 $P_T(=s_T P)$，标签存储着自己的公私钥信息 $\{s_T, P_T(=s_T P)\}$、标签标识信息 *ID* 以及后台服务器的公钥值 P_S，认证协议执行过程如图 4.6 所示。

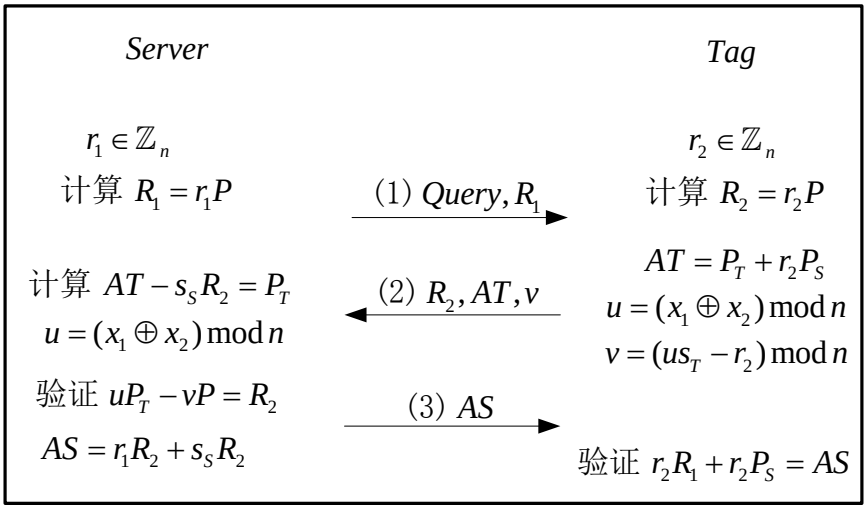

图 4.6 何剑辉的改进协议

（1）后台服务器生成一个随机数 $r_1 \in \mathbb{Z}_n$，并计算 $R_1 = r_1 P(x_1, y_1)$，向标签发送请求信息 *Query* 并将 $R_1 = r_1 P$ 发送给标签；

（2）标签接收到请求后，首先生成一个随机数 $r_2 \in \mathbb{Z}_n$，并且计算：

$$R_2 = r_2 P(x_2, y_2) \quad (4.19)$$

$$AT = P_T + r_2 P_S \quad (4.20)$$

$$u = (x_1 \oplus x_2) \bmod n \quad (4.21)$$

$$v = (us_T - r_2) \bmod n \quad (4.22)$$

并将信息 $\langle R_2, AT, v \rangle$ 发送给服务器；

（3）后台服务器接收到信息后，计算并判断等式 $AT - s_S R_2 = P_T$ 是否成立，如果成立，继续计算 $u = (x_1 \oplus x_2) \bmod n$，并验证等式 $uP_T - vP = R_2$ 是否成立，如果成立，则服务器认定此标签是合法标签，计算 $AS = r_1 R_2 + s_S R_2$，将信息 $\langle AS \rangle$ 发送给标签，否则认证失败，结束。

（4）标签接收到请求后，计算并判断等式 $r_2 R_1 + r_2 P_S = AS$ 是否成立，如果成立，则双向认证成功，否则认证失败，结束。

其中，验证过程中具体计算如下：

$$AT - s_S R_2 = P_T + r_2 s_S P - s_S r_2 P = P_T \quad (4.23)$$

$$uP_T - vP = uP_T - (us_T - r_2)P = R_2 \quad (4.24)$$

$$AS = r_1 R_2 + s_S R_2 = r_1 r_2 P + s_S r_2 P = r_2 R_1 + r_2 P_S \quad (4.25)$$

在安全性方面，该协议每一次认证过程中传递的信息 $\langle R_1, R_2, AT, v, s \rangle$ 都是新鲜的，并且攻击者无法从两次或多次交互信息中获取到固定信息，因此攻击者无法成功实施对标签的追踪攻击。但是该协议却不能抵御对服务器的重放攻击和对标签的假冒攻击，

原因在于后台服务器初次验证过程，等式 $AT-s_S R_2=P_T$ 中仅仅含有标签的公钥信息 $P_T(=s_T P)$、服务器的公私钥信息 $\{s_T, P_T(=s_T P)\}$ 和标签产生的随机数 r_2，缺乏验证过程的随机性和新鲜性，攻击者通过窃听等方式获取步骤 2 的信息 $\langle R_2, AT, v\rangle$，很容易对服务器进行重放攻击，这使得系统的安全性无法得到保障。在性能方面，由于协议中后台数据库需要通过线性搜索的方式去查询标签公钥值和标识信息，所以导致后台服务器计算开销较大、系统可扩展性较差，由此可知，此协议不适用于大型分布式 RFID 系统。

4.3　基于椭圆曲线的改进协议

针对现有的基于 ECC 认证协议的安全和性能问题，本文提出一种改进协议，该协议既兼顾系统性能和硬件成本，又满足 RFID 系统的安全需求。

4.3.1　协议初始条件和算法步骤

后台服务器选择一个定义在素数域 $\mathbb{Z}_p(p>3)$ 上的椭圆曲线 E，并且选择 E 上一个循环点子群的本原元 G，阶为 n，在认证协议初始阶段，服务器数据库中存储着自己的公私钥信息 $\{k, Q(=kG)\}$ 以及每个标签的标识信息 M，标签存储着自己的标识信息 M 以及服务器的公钥值 $Q(=kG)$，协议的算法步骤如表 4.2 所示，协议认证过程如图 4.7 所示。

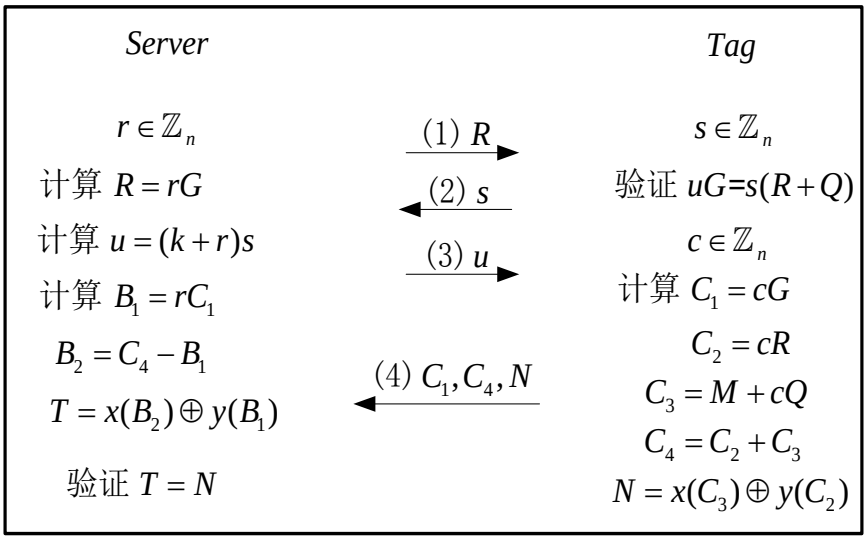

图 4.7 本文提出的改进协议

表 4.2 改进协议算法步骤

Step1：	后台服务器生成一个随机数 $r \in \mathbb{Z}_n$，计算 $R=rG$，向标签发送请求信息，同时将认证信息 R 发给标签；
Step2：	标签接收到请求后，暂存认证信息 R，生成一个随机数 $s \in \mathbb{Z}_n$ 并将 s 发送给服务器，服务器接收到信息后，计算 $u=(k+r)s$ 并将认证信息 u 发送给标签；
Step3：	标签收到来自服务器的信息后，将根据服务器的公钥 Q，来验证 u 的有效性； ➢ *If* $uG \neq s(R+Q)$，认证失败，结束。 ➢ *else* $uG=s(R+Q)$，标签将接受服务器为有效个体，标签产生一个随机数 $c \in \mathbb{Z}_n$，并且计算 $C_1=cG$，$C_2=cR$，$C_3=M+cQ$，$C_4=C_2+C_3$，$N=x(C_3)\oplus y(C_2)$，其中，$x(i)$ 和 $y(j)$ 分别表示椭圆曲线上点 i 的横坐标和点 j 纵坐标，标签将认证信息 C_1，C_4，N 发送给服务器；
Step4：	后台服务器接收到标签发来的信息后，在数据库中进行相关的计算和比较，计算 $B_1=rC_1$，$B_2=C_4-B_1$ 和 $T=x(B_2)\oplus y(B_1)$， ➢ *If* $T \neq N$，认证失败，结束。 ➢ *else* $T=N$，此标签被后台服务器认定为合法标签，服务器继续计算 $B_2-kC_1=M$，利用它的密钥 k 恢复出标签的明文信息 M。
结束	

4.3.2 协议安全性分析

现有的基于 ECC 的认证协议，大多数都存在安全隐患或性能问题，本文提出的改进协议能够有效抵御假冒攻击、重放攻击等各种攻击，具体分析如下：

（1）双向认证

双向认证包括标签对服务器的认证和服务器对标签的认证。其中，通过服务器向标签发送 R 和 u，标签计算并判断等式 $uG=s(R+Q)$ 是否成立，这一过程实现了标签对服务器的认证；通过标签计算 $C_1=cG$，$C_2=cR$，$C_3=M+cQ$，$C_4=C_2+C_3$，$N=x(C_3)\oplus y(C_2)$，将信息 C_1，C_4，N 发送给后台服务器，服务器计算 $B_1=rC_1$，$B_2=C_4-B_1$ 和 $T=x(B_2)\oplus y(B_1)$，并判断等式 $T=N$ 是否成立，这一过程完成了服务器

对标签的认证。从而实现了标签和服务器之间的双向认证。

（2）追踪攻击

通过对现有的认证协议分析可见，大多数基于椭圆曲线的认证协议抗追踪攻击能力较差，本文提出的改进协议可以有效抵御对标签的追踪攻击。假设攻击者连续两次截获步骤 3 中标签发给后台服务器的信息，将得到两组认证信息 C_1, C_4, N 和 C_1', C_4', N'，攻击者试图分析和验证两组信息之间的关联得出结果，然而，认证信息 $C_1 = cG$、$C_4 = C_2 + C_3$ 和 N 在每一轮的认证过程中均是新鲜的，并没有关联性，因此攻击者无法根据两组或多组的认证信息对标签实施定位追踪攻击。

（3）假冒攻击

在改进协议中，攻击者能够实施的假冒攻击可分为假冒服务器攻击和假冒标签攻击。在假冒服务器攻击过程中，攻击者首先窃听到服务器的响应信息，在下一轮的认证过程中假冒服务器，以骗取标签的有用信息。本协议中，即使攻击者获取了服务器响应信息 R 和 u，也不能哄骗到标签，因为协议执行的每一轮标签都需要通过 $uG = s(R + Q)$ 验证服务器身份，因此攻击者无法成功实施假冒服务器攻击；在假冒标签攻击过程中，攻击者首先窃听到标签的响应信息，在下一轮的认证过程中假冒标签，以骗取服务器的有用信息。本协议中，即使攻击者获取了标签响应信息 s，C_1，C_4，N，也不能哄骗到服务器，因为协议执行的每一轮服务器都需要计算 B_1，B_2 和 $T = x(B_2) \oplus y(B_1)$，并且通过判断等式 $T=N$ 是否成立从而验证标签身份，假冒的标签不会通过验证，因此攻击者无法成功实施假冒服务器攻击。

（4）重放攻击

在 RFID 认证协议中，重放攻击是指攻击者通过窃听等方式获取认证信息，冒充合法个体不断恶意或欺诈性地重复某一消息，以达到欺骗系统的目的。对于本协议而言，重放攻击可分为对标签的重放攻击和对服务器的重放攻击。

在对标签的重放攻击过程中，攻击者首先窃听到服务器向标签传递的信息 R 和 u，并在下一轮的认证过程中利用信息 R 和 u 对标签进行重放攻击，达到破坏系统的目的，然而每次执行协议时标签都需要验证服务器身份，这使得攻击者无法成功实施对标签的重放攻击；在对服务器的重放攻击过程中，攻击者首先窃听到标签向服务器传递的信息 s，C_1，C_4，N，并在下一轮的认证过程中利用信息对服务器进行重放攻击，然而每次执行协议时服务器都需要验证标签身份，这使得攻击者对服务器的重放攻击也是无效的。

（5）可扩展性

在 RFID 系统中，可扩展性是其中一个重要性能指标，只有具备较好的可扩展性，系统才能够在复杂的环境下得以应用。现有的基于椭圆曲线认证协议，大多数都需要在后台服务器中进行线性搜索，使得系统的可扩展性较差。本协议中，后台服务器认证标签的过程仅需要简单两步计算和匹配判断，就可以识别标签是否合法，并且认证结束后标签和服务器也不需要动态更新，从而减少了计算开销，因此系统的可扩展性良好。

（6）效率分析

针对认证协议的效率分析，主要从存储成本、通信成本以及计算成本等方面说明。在存储成本方面，认证协议的标签端存储着标签标识 M 和服务器公钥值 $Q(=kG)$，后台服务器端存储着自己的公私钥信息 $\{k,Q(=kG)\}$ 以及每个标签的标识信息 M，大体来说，系统的存储成本相对较低。在计算成本方面，本协议标签端的运算仅仅需要 5 个点乘和 3 个点加，后台服务器的运算主要涉及 2 个点乘和 1 个点加。现有的认证协议中后端服务器计算繁重，本协议中服务器仅需要简单两步计算和匹配判断，使得计算成本大大降低，这将有利于系统后续扩展。在通信成本方面，假定在认证协议过程中每个消息长度为 l 比特，本协议通过 4 轮的信息交互完成标签和后台服务器之间的双向认证，所以认证协议的通信成本为 $4l$ 比特，在 RFID 双向认证协议系统中，通信成本的花销是合理的。

本文提出的改进协议和其他基于 ECC 的认证方案从安全和性能方面进行分析，可得比较结果如表 4.3 所示。

表 4.3 安全和性能比较

安全要求	文献[14]	文献[15]	文献[16]	文献[17]	本文方案
假冒攻击	Y	Y	Y	N	Y
重放攻击	Y	Y	Y	N	Y
追踪攻击	N	Y	Y	Y	Y
双向认证	N	N	N	Y	Y
可扩展性	N	N	N	N	Y

其中，Y 表示满足该安全需求；N 表示不满足。

4.3.3　协议仿真与分析

现有的大多数基于椭圆曲线的认证协议仅仅提供协议逻辑证明和安全性能分析，往往缺乏仿真实验或硬件平台实现。本文提出的改进协议不但给出了协议的算法流程和安全性能分析，而且使用仿真工具进行仿真实现。本文运用 C++语言在 Visual C++ 6.0 开发环境进行仿真认证协议执行过程，算法的程序流程如图 4.8 所示。

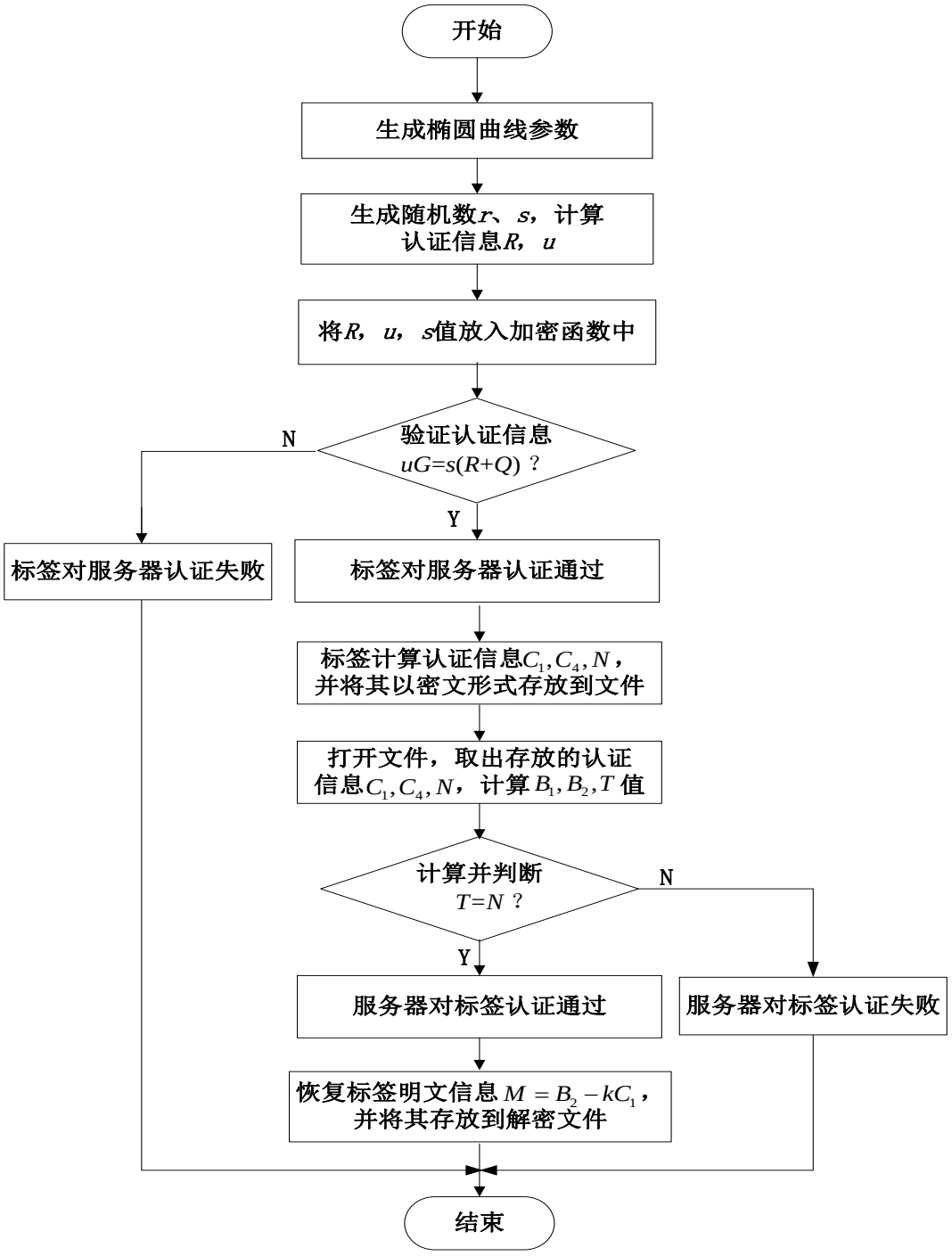

图 4.8 改进协议算法程序流程图

系统仿真主要分为三部分：椭圆曲线各参数生成、标签对服务器的认证、服务器对标签的认证。

（1）椭圆曲线各参数生成

在执行认证协议之前，首先应该生成椭圆曲线各参数，认证协议中椭圆曲线参数包括：有限域 P、椭圆曲线方程系数 a 和 b、本原元 G、后台服务器私钥 k 和公钥 Q 的横纵坐标，仿真结果如图 4.9 所示。

图 4.9 椭圆曲线参数生成

（2）标签对服务器的认证

在标签对服务器的认证阶段，需要生成两个随机数 r 和 s，并计算 $R=rG$ 和 $u=(k+r)s$，通过传送 R,s,u 信息到加密函数中，模拟后台服务器向标签发送信息的过程。标签接收到服务器认证信息后，首先对服务器合法性进行验证，计算并判断等式 $uG=s(R+Q)$ 是否成立，若不成立，认证失败，结束；若成立，则服务器合法，继续计算如下信息：

$$C_1=cG \quad (4.26)$$

$$C_2=cR \quad (4.27)$$

$$C_3=M+cQ \quad (4.28)$$

$$C_4=C_2+C_3 \quad (4.29)$$

$$N=x(C_3)\oplus y(C_2) \quad (4.30)$$

把计算结果 C_1，C_4，N 以密文的形式存放到文件里，模拟标签向后台服务器发送信息的过程，仿真结果如图 4.10 所示。

图 4.10 标签对服务器的认证

（3）服务器对标签的认证

在服务器对标签的认证过程中，首先输入要解密的文件名，将存有标签发送的密文文件打开，从中取出认证信息 C_1，C_4，N，模拟后台服务器接收标签发送信息的过程，成功接收到信息后，服务器将对标签的合法性进行验证，计算如下信息：

$$B_1 = rC_1 \quad (4.31)$$

$$B_2 = C_4 - B_1 \quad (4.32)$$

$$T = x(B_2) \oplus y(B_1) \quad (4.33)$$

并验证 T 和 N 是否相等，如果不等，认证失败，结束；如果相等，则此标签被认定为合法标签，服务器继续计算 $M = B_2 - kC_1$，利用它的密钥 k 恢复出标签的明文信息 M，并将标签的明文信息存储到解密文件中，仿真结果如图 4.11 所示。

图 4.11 服务器对标签的认证

4.4 本章小结

本章主要研究基于 ECC 的 RFID 认证协议，简要地介绍椭圆曲线的定义、群操作、椭圆曲线离散对数问题，针对现有的典型的基于 ECC 的 RFID 安全协议，进行了详细地分析并且指出了不足之处。在此基础上，提出了基于 ECC 的改进协议，给出协议的具体认证过程和算法步骤，通过安全性分析和对比，本协议具备双向认证、不可追踪性、可扩展性等优势。在 Visual C++6.0 开发环境下，实现了改进协议的软件仿真，仿真结果表明，改进协议的参数生成、加解密部分、标签和后台服务器之间认证均能实现，协议具有可行性。

第 5 章　总结与展望

5.1　总结

近几年，物联网、车联网和互联网＋行业快速兴起，一些新技术特别是射频识别技术受到了人们的普遍关注。伴随着 RFID 系统的大规模应用，系统的安全和隐私问题成为其发展的瓶颈，由于 RFID 系统中标签和读写器认证过程工作在无线通信信道，无线信道容易受到攻击者恶意攻击，使得系统的安全性难以得到保障。为此，人们提出了许多关于 RFID 系统的认证协议，依据系统的计算复杂度和操作复杂性，大体可分为基于简单逻辑运算的轻量级认证协议、基于散列函数的中量级认证协议、基于对称或公钥密码体制的重量级认证协议等。其中，中量级和重量级认证协议具有性能好、安全性强等优势，是近几年学者们研究的热点。但是，在现有的认证协议中，大多数协议未能够兼顾系统的安全隐私性和标签硬件需求，导致认证协议难以在系统和平台上实现。在此背景下，本文提出了两种改进的认证协议。

本文的主要研究工作如下：

（1）介绍 RFID 系统组成部分、关键部件和系统工作原理，对 RFID 系统设计要求进行归纳和总结，主要考虑系统安全隐私和性能指标，详细分析系统目前所面临的安全隐患，介绍了两种 RFID 安全机制，并对两种机制的优缺点进行归纳和总结。

（2）简要地介绍散列函数的理论基础，针对现有的典型的基于散列函数的 RFID 安全协议，通过对认证过程、安全和性能分析和总结，得出各认证协议的优势和劣势。在此基础上，提出了一种改进的 RFID 认证协议，阐述协议执行过程和算法步骤，运用形式化分析方法 BAN 逻辑分析和证明认证协议的正确性。在改进协议设计过程中，我们既考虑到 RFID 系统的局限性和特殊性，又兼顾了系统安全和隐私性。在安全隐私方面，本协议能够有效抵抗重放、假冒、去同步等攻击，通过性能分析和对比，本协议具有计算、存储、传输成本少，标签硬件要求低，运行效率高，可扩展性强等优势。由此可见，本协议适用于低成本、高效率的 RFID 系统。

（3）研究了基于椭圆曲线密码机制的 RFID 认证协议，介绍了椭圆曲线的定义、群操作、椭圆曲线离散对数问题，针对现有的典型的基于 ECC 的 RFID 安全协议，进行了详细地分析和总结，并且指出了不足之处。在此基础上，提出了一种基于 ECC 的改进协议，给出了协议具体认证过程和算法步骤，通过安全性分析和对比，能够得出

本协议具备双向认证、不可追踪性、可扩展性等明显优势。在 Visual C++6.0 开发环境下，对改进协议进行软件仿真，实现了改进协议的参数生成、加解密、标签和后台服务器之间的双向认证，由此说明协议具有可行性。

5.2 展望

由于本人的水平和研究时间有限，本文仅从 RFID 系统通信模型中应用层的角度进行研究的，因此还存在以下不足之处：

（1）本文仅从应用层角度研究认证协议的执行过程，并未考虑物理层和通信层等因素，因此在后续的研究中，应该将物理层的接口、编码以及通信层的防碰撞、冲突等因素考虑进来，而且需要针对特定的工作环境展开研究，这样才更合理；

（2）当前仿真环境过于理想，并没有考虑到攻击者攻击的情况，应将仿真环境设置在接近实际环境或者存在恶意攻击的条件下，验证方案的可行性；

以上不足之处，我将在今后的学习中更进一步地研究、充实和完善。

参考文献

[1] Tewari A, Gupta B B. Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags[J]. Journal of Supercomputing, 2016:1-18.

[2] Tsudik G. YA-TRAP: Yet Another Trivial RFID Authentication Protocol[C]// IEEE International Conference on Pervasive Computing and Communications Workshops, 2006. PERCOM Workshops. IEEE, 2006:4 pp.-643.

[3] Mujahid U, Najam-Ul-Islam M, Shami M A. RCIA: A New Ultralightweight RFID Authentication Protocol Using Recursive Hash[J]. International Journal of Distributed Sensor Networks, 2015, 2015(3):1-8.

[4] Cong G, Zhang Z J, Zhu L H, et al. A novel secure group RFID authentication protocol[J]. Journal of China Universities of Posts & Telecommunications, 2014, 21(1):94-103.

[5] Safkhani M, Peris-Lopez P, Hernandez-Castro J C, et al. Cryptanalysis of the Cho etal. protocol: A hash-based RFID tag mutual authentication protocol[J]. Journal of Computational & Applied Mathematics, 2014, 259(6):571-577.

[6] Staake T, Fleisch E. Extending the EPC network:the potential of RFID in anti-counterfeiting[C]// Proceedings of the 2005 ACM symposium on Applied computing. ACM, 2005:1607-1612.

[7] Chatmon C, Le T V, Burmester M. Secure anonymous RFID authentication protocols[J]. Florida State University, 2006, 14(1 Supplement):51-84.

[8] Weis S A, Sarma S E, Rivest R L, et al. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems[J]. Lecture Notes in Computer Science, 2003, 2802:201--212.

[9] Lee Y C, Hsieh Y C, You P S, et al. An Improvement on RFID Authentication Protocol with Privacy Protection[C]// Third International Conference on Convergence and Hybrid Information Technology. IEEE Computer Society, 2008:569-573.

[10] 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.

[11] 罗序斌. 一种动态 ID 机制的 RFID 安全协议[D]. 中山大学, 2010.

[12] Srivastava K, Awasthi A K, Kaul S D, et al. A Hash Based Mutual RFID Tag Authentication Protocol in Telecare Medicine Information System[J]. Journal of Medical Systems, 2015, 39(1):153.

[13] Tuyls P, Batina L. RFID-Tags for Anti-counterfeiting[M]. Topics in Cryptology – CT-RSA 2006. Springer Berlin Heidelberg, 2006:115-131.

[14] Yong K L, Batina L, Verbauwhede I. EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol[C]// IEEE International Conference on Rfid. IEEE, 2008:97-104.

[15] O'Neill M, Robshaw M J B. Low-cost digital signature architecture suitable for radio frequency identification tags[J]. Computers & Digital Techniques Iet, 2010, 4(1):14-26.

[16] Zhang X, Li L, Wu Y, et al. An ECDLP-Based Randomized Key RFID Authentication Protocol[C]// International Conference on Network Computing and Information Security. IEEE, 2011:146-149.

[17] 何剑辉. 基于 ECC 的 RFID 双向认证协议的研究[D]. 西安电子科技大学, 2014.

[18] 杨玉龙, 彭长根, 周洲,等. 基于 Edwards 曲线的移动 RFID 安全认证协议[J]. 通信学报, 2014, 35(11).

[19] Klaus Finkenzeller, 王俊峰. 射频识别技术原理与应用[M]. 电子工业出版社, 2015.

[20] Domdouzis K, Kumar B, Anumba C. Radio-Frequency Identification (RFID) applications: A brief introduction[J]. Advanced Engineering Informatics, 2007, 21(4):350-355.

[21] 高树静. 低成本无源 RFID 安全关键技术研究[D]. 山东大学, 2013.

[22] 周晓光 王晓华 王伟. 射频识别(RFID)系统设计.仿真与应用[M]. 人民邮电出版社, 2008.

[23] Wu X, Min Z, Yang X. Time-stamp based mutual authentication protocol for mobile RFID system[C]// Wireless and Optical Communication Conference. IEEE, 2013:702-706.

[24] Zhu W, Yu J, Wang T. A security and privacy model for mobile RFID systems in the internet of things[C]// IEEE, International Conference on Communication Technology. IEEE, 2012:726-732.

[25] 何加亮. 基于散列函数的 RFID 安全协议研究[D]. 吉林大学, 2012.

[26] Huo L, Jiang Y L, Hu L Q. Research on Hash-Based Low-Cost RFID Security Authentication Protocol[J]. Advanced Materials Research, 2013, 846-847:1524-1530.

[27] Chou J S. An efficient mutual authentication RFID scheme based on elliptic curve cryptography[J]. The Journal of Supercomputing, 2014, 70(1):75-94.

[28] Ko W T, Chiou S Y, Lu E H, et al. An improvement of privacy-preserving ECC-based grouping proof for RFID[C]// Cross Strait Quad-Regional Radio Science and Wireless Technology Conference. IEEE, 2011:1062-1064.

[29] Cho J S, Yeo S S, Kim S K. Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value[J]. Computer Communications, 2011, 34(3):391-397.

[30] 周景贤. RFID 系统安全协议研究[D]. 北京邮电大学, 2013.

[31] Liu H, Ning H. Zero-Knowledge Authentication Protocol Based on Alternative Mode in RFID Systems[J]. IEEE Sensors Journal, 2011, 11(12):3235-3245.

[32] Liu H, Ning H, Zhang Y, et al. Grouping-Proofs-Based Authentication Protocol for Distributed RFID Systems[J]. IEEE Transactions on Parallel & Distributed Systems, 2013, 24(7):1321-1330.

[33] Lu L, Han J, Hu L, et al. Dynamic Key-Updating: Privacy-Preserving Authentication for RFID Systems.[J]. International Journal of Distributed Sensor Networks, 2012, 2012(4):13-22.

[34] 龚圆圆. RFID 安全认证协议的研究[D]. 西安电子科技大学, 2014.

[35] 邓淼磊，马建峰，周利华. RFID 匿名认证协议的设计[J]. 通信学报，2009, 30(7):20-26.

[36] Hopper N J, Blum M. Secure Human Identification Protocols[C]// International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology. Springer-Verlag, 2001:52-66.

[37] 刘伟强，崔益军，王成华. 一种低成本物理不可克隆函数结构的设计实现及其 RFID 应用[J]. 电子学报, 2016, 44(7):1772-1776.

[38] Zhou S, Zhang Z, Luo Z, et al. A lightweight anti-desynchronization RFID authentication protocol[J]. Information Systems Frontiers, 2010, 12(5):521-528.

[39] 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 Conference on. IEEE, 2004:149-153.

[40] Zhao Z. A Secure RFID Authentication Protocol for Healthcare Environments Using Elliptic Curve Cryptosystem[J]. Journal of Medical Systems, 2014, 38(5):1-7.

[41] 朱雪瑗. 基于ECC的物联网RFID安全认证协议的研究与应用[D]. 大连海事大学, 2013.

[42] 周琴琴. 基于 Hash 函数的 MD5 和 SHA-1 加密算法研究及其硬件实现[D]. 安徽大学, 2012.

[43] 张佳宁. 基于 SHA-3 的 RFID 认证协议设计与实现[D]. 西安电子科技大学, 2013.

[44] Sarma S E, Weis S A, Engels D W. RFID Systems and Security and Privacy Implications[M]. Cryptographic Hardware and Embedded Systems - CHES 2002. Springer Berlin Heidelberg, 2002:454--470.

[45] Ohkubo M, Suzuki K, Kinoshita S. Hash-chain based forward-secure privacy protection scheme for low-cost RFID[C]// Proceedings of the SCIS. 2004, 2004: 719-724.

[46] Su M L, Hwang Y J, Dong H L, et al. Efficient Authentication for Low-Cost RFID Systems[M]. Computational Science and Its Applications – ICCSA 2005. Springer Berlin Heidelberg, 2005:619-627.

[47] Osaka K, Takagi T, Yamazaki K, et al. An Efficient and Secure RFID Security Method with Ownership Transfer[C]// International Conference on Computational Intelligence and Security. IEEE, 2006:1090-1095.

[48] Sun D Z, Zhong J D. Cryptanalysis of a Hash Based Mutual RFID Tag Authentication Protocol[J]. Wireless Personal Communications, 2016, 91:1-9.

[49] Yu Y, Lei Z. Research on a provable security RFID authentication protocol based on Hash function[J]. Journal of China Universities of Posts & Telecommunications, 2016, 23(2):31-37.

[50] 杨世平. 安全协议及其 BAN 逻辑分析研究[D]. 贵州大学, 2007.

[51] 冯登国, 范红. 安全协议形式化分析理论与方法研究综述[J]. 中国科学院大学学报, 2003, 20(4):389-406.

[52] 王亚弟. 密码协议形式化分析[M]. 机械工业出版社, 2006.

[53] Godor G, Giczi N, Imre S. Elliptic curve cryptography based mutual authentication protocol for low computational capacity RFID systems - performance analysis by simulations[C]// IEEE International Conference on Wireless Communications, NETWORKING and Information Security. IEEE, 2010:650-657.

[54] 高磊. 基于椭圆曲线密码的 RFID 安全协议[D]. 上海交通大学, 2007.

[55] 张星磊. 基于椭圆曲线离散对数难题的 RFID 安全协议设计与分析[D]. 上海交通大学, 2011.

[56] DarrelHankerson. 椭圆曲线密码学导论[M]. 电子工业出版社, 2005.

[57] Bernstein D J, Lange T. Faster addition and doubling on elliptic curves[C]// Advances in Crypotology, International Conference on Theory and Application of Cryptology and Information Security. Springer-Verlag, 2007:29-50.

作者简介及科研成果

作者简介：

张磊，男，1989 年生于吉林省德惠市，汉族。2014 年 6 月毕业于长春工业大学计算机科学与工程学院电子信息工程专业，现为吉林大学通信工程学院信号与信息处理专业硕士研究生，硕士期间的主要研究方向为短距离无线通信技术。

参与科研项目：

[1] 基于互联网+的汽车实时可视定位系统研发与产业化(No. 20160521021HJ)，吉林省科技厅大学生创业资金项目，2016.1-2018.12.主要参加人

发表学术论文：

[1] Yu Y, Lei Z. Research on a provable security RFID authentication protocol based on Hash function[J]. Journal of China Universities of Posts & Telecommunications, 2016, 23(2):31-37.

发明专利：

[1] 于银辉，张磊，陈倩，王达，田小建. 基于移动 RFID 系统的安全协议认证方法. (发明专利，No：201610015940.7).

[2] 于银辉，张磊，王玉星，陈登昭，田小建. 基于汽车安防系统的动态 ID 和密钥更新的 RFID 安全方法.(发明专利，No：201410754424.7).

致 谢

时间如水静静流淌，三年的研究生生涯即将结束。回首过去，收获颇丰，在 205 实验室学习和工作中，我不但学到了许多书本上的知识，而且得到了师兄、师姐以及师弟师妹们的关心和帮助，三年的研究生生活，是我人生中一段宝贵的财富。在此我想向指导、关心和帮助我的人表示衷心的感谢。

首先，我要感谢我的导师——于银辉教授，在学习上，研一初期，老师将我纳入到科研团队和项目研究中，让我学到了更多的知识，使我的科研水平有所提升。在生活中，老师不但给予我无微不至的关怀和帮助，而且教会我许多做人的道理。老师严谨的治学态度和平易近人的人格魅力，是我一生学习的榜样。本课题的研究、期刊论文和专利的发表，老师都给予我许多建议和意见，正是老师悉心地指导，我才能顺利的完成毕业论文。

感谢实验室的所有成员，尤其感谢孔繁月师妹在我撰写论文时，给予我很大的帮助，在实验室的学习和生活，我学会了承担与分享，让我感受到了一个有爱的大家庭。

感谢我的研究生同学，作为研究生班长，正是大家的信任和支持，我才能顺利的开展各项工作。全心全意为大家服务，是我的职责。

感谢我的家人，感谢他们不求回报的付出，他们的关心和支持是我前进的动力，感谢我的女朋友，是她的一路陪伴，让我的生活丰富多彩。

最后，感谢在百忙之中抽出宝贵时间评审论文的每一位专家教授，在此，致以最诚挚的感谢。