分类号\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 密级\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ＵＤＣ\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 编号\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

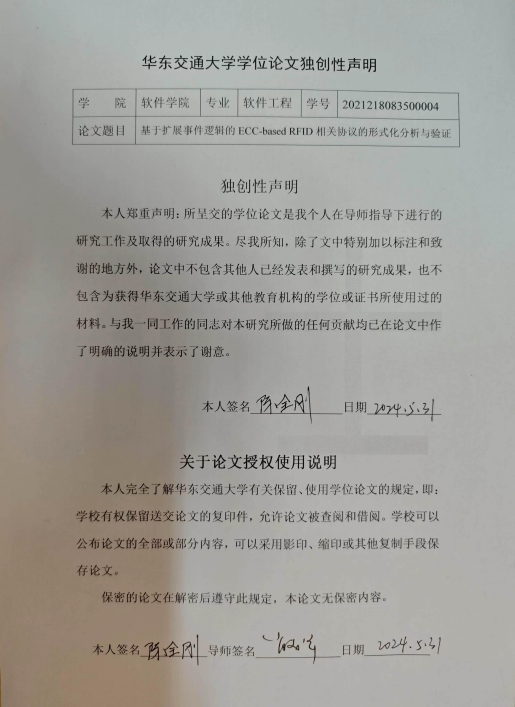
****

**硕士学位论文**

|  |  |
| --- | --- |
| **基于扩展事件逻辑的ECC-based RFID相关协议形式化分析与验证** | |
|  | |
| **学位申请人：** | **陈全刚** |
| **专业领域：** | **软件工程** |
| **校内导师：** | **肖美华 教授** |
|  |  |
|  | |
|  | |
|  | |

**答辩日期：2024.5.26**

|  |
| --- |
| **华东交通大学2024届硕士学位论文**  **书脊** |
| **基于扩展事件逻辑的ECC-based RFID相关协议形式化分析** |
| **析与验证 软件学院** |
| **陈全刚** |



**基于扩展事件逻辑的ECC-based RFID相关协议形式化分析与验证**

**摘要**

射频识别技术（RFID）是物联网（IoT）的重要组成部分，提高RFID系统的安全性是亟需解决的问题。而保障通信系统的安全性与系统所使用的安全协议息息相关，如果安全协议的安全属性没有得到严格的证明，则增加了网络通信中的风险。形式化方法是分析与验证安全协议最强有力的手段之一。事件逻辑理论（Logic of Events Theory, LoET）作为一种分布式系统安全性描述的形式化方法，提供了对安全协议基本原语的形式化规范，并通过对协议的强认证性质进行证明，进而验证协议的安全属性。

本文通过对事件逻辑理论的创新性扩展，成功将其应用于基于ECC的RFID这一类协议的形式化分析与验证中，使扩展后的事件逻辑理论适用于带有复杂加密算法协议的安全性分析。本文的主要研究内容如下：

1. 详细介绍事件逻辑基本理论，给出事件逻辑基本定义，包括基本建模理论，公理系统以及协议的形式化描述。引入扩充谓词和以及相应的推理规则，增强其在协议分析中的实用性，特别是在处理消息的新鲜性和识别发送事件的首发性方面，有助于确保协议证明过程中事件类和基本序列的一致性，同时提高了事件排序的能力并降低了协议分析的复杂度。

2. 将事件逻辑与其他形式化方法进行比较，分析事件逻辑对于其他方法的优势与不足。对事件逻辑理论进行扩展，提出三个新事件类、、并给出相应的定义。根据新的事件类，扩展因果公理，定义新的因果关系。对其他相关公理及规则进行扩展，使得扩展后的事件逻辑理论能够分析带有复杂加密算法的协议。建立机密性系统，引入归纳机密规则，扩展LoET所能证明的安全属性范畴。

3. 利用扩展后的事件逻辑理论，深入形式化分析一个ECC-based RFID双向认证协议。首先对ECC会话密钥的生成过程进行形式化抽象描述，定义协议进程和基本序列用于描述协议，对协议所需满足的强认证属性进行了严格的形式化定义，通过理论推导，证明协议在合理假设下满足双向强认证性质，表明扩展的事件逻辑理论可以证明ECC-based RFID这一类带有复杂加密算法协议的安全属性，扩展了事件逻辑理论的使用范围。

**关键词**：安全协议，形式化方法，事件逻辑理论，ECC-based RFID双向认证协议

**Formal Analysis and Verification of ECC-based RFID Correlation Protocols Based on Extended Event Logic**

**ABSTRACT**

Radio Frequency Identification Technology (RFID) is an important part of the Internet of Things (IoT), and improving the security of RFID systems is a pressing issue. And guaranteeing the security of the communication system is closely related to the security protocols used in the system, which increases the risk in network communication if the security properties of the security protocols are not strictly proved. Formal methods are one of the most powerful means of analysing and verifying security protocols. Logic of Events Theory (LoET), as a formal approach to the description of security in distributed systems, provides a formal specification of the basic primitives of security protocols and verifies the security properties of the protocols by proving the strong authentication properties of the protocols and, in turn, verifying the security properties of the protocols..

In this paper, through the innovative extension of the event logic theory, it is successfully applied to the formal analysis and verification of ECC-based RFID protocols, which makes the extended event logic theory applicable to the security analysis of protocols with complex encryption algorithms. The main research content of this paper is as follows:

1. Introduces the basic theory of event logic in detail, giving a basic definition of event logic, including basic modelling theory, axiomatic systems, and formal descriptions of protocols. Expanded predicates and and corresponding inference rules are introduced to enhance their usefulness in protocol analysis, especially in dealing with the freshness of messages and identifying the primality of sent events, which helps to ensure the consistency of event classes and basic sequences in the process of protocol proofs, and at the same time improves the ability of event ordering and reduces the complexity of protocol analysis.

2. Compare LoET with other formal methods and analyse the advantages and shortcomings of LoET for other methods. Extend the LoET, propose three new event classes *Compute*, *Retrieve*, *Generate* and give the corresponding definitions. According to the new event classes, extend the causal axioms and define new causal relations. Extend other related axioms and rules so that the extended LoET can analyse protocols with complex encryption algorithms. A confidentiality system has been established that introduces inductive confidentiality rules to extend the range of security properties that can be proved by LoET. Establishment of a confidentiality system, introduction of inductive confidentiality rules, and extension of the range of security attributes that can be proved by LoET.

3. An in-depth formal analysis of an ECC-based RFID two-way authentication protocol using the extended LoET. Firstly, the formal abstract description of the ECC session key generation process is carried out, the protocol process and basic sequence are defined for describing the protocol, and the strong authentication attributes that the protocol needs to satisfy are strictly formally defined, and through theoretical derivation, it is proved that the protocol satisfies the bidirectional strong authentication attributes under reasonable assumptions, which indicates that the extended event logic theory can prove the security attributes of the ECC-based RFID protocol with complicated It shows that the extended LoET can prove the security properties of ECC-based RFID protocols with complex encryption algorithms, which extends the scope of the LoET.

**Key Words:** Security protocol, Formal methods, Logic of events theory, ECC-based RFID two-way authentication protocol

目录

[主要符号说明 VI](#_Toc161648906)

[第一章 绪论 1](#_Toc161648907)

[1.1 研究背景及意义 1](#_Toc161648908)

[1.2 国内外研究现状 2](#_Toc161648909)

[1.2.1 ECC-based RFID协议研究现状 2](#_Toc161648910)

[1.2.2 ECC-based RFID协议形式化分析研究现状 3](#_Toc161648911)

[1.3 本文主要内容 5](#_Toc161648912)

[1.4 论文结构安排 5](#_Toc161648913)

[第二章 ECC-based RFID认证协议及形式化方法概述 7](#_Toc161648914)

[2.1 ECC-based RFID认证协议 7](#_Toc161648915)

[2.1.1 RFID系统介绍 7](#_Toc161648916)

[2.1.2 椭圆曲线密码体制 8](#_Toc161648917)

[2.1.3 ECC-based RFID认证协议的安全需求 10](#_Toc161648918)

[2.2 ECC-based RFID双向认证协议分析 11](#_Toc161648919)

[2.3 形式化方法概述 13](#_Toc161648920)

[2.3.1 模型检测 14](#_Toc161648921)

[2.3.2 模态逻辑 15](#_Toc161648922)

[2.3.3 定理证明 17](#_Toc161648923)

[2.4 本章小结 18](#_Toc161648924)

[第三章 事件逻辑理论 19](#_Toc161648925)

[3.1 基本建模理论 19](#_Toc161648926)

[3.1.1 消息自动机 19](#_Toc161648927)

[3.1.2 不可猜测的原子 20](#_Toc161648928)

[3.1.3 事件序、事件类及事件结构 20](#_Toc161648929)

[3.2 事件逻辑理论公理系统 21](#_Toc161648930)

[3.3 事件逻辑形式化描述协议 25](#_Toc161648931)

[3.3.1 线程和匹配会话 25](#_Toc161648932)

[3.3.2 基本序列和协议动作 25](#_Toc161648933)

[3.3.3 协议描述 26](#_Toc161648934)

[3.4 事件逻辑证明协议安全性流程 28](#_Toc161648935)

[3.5 本章小结 29](#_Toc161648936)

[第四章 事件逻辑理论的扩展 30](#_Toc161648937)

[4.1 事件逻辑理论与其他形式化方法的对比 30](#_Toc161648938)

[4.2 对事件类的扩展 31](#_Toc161648939)

[4.3 相关公理及规则的扩展 32](#_Toc161648940)

[4.3.1 扩充谓词及其定义 32](#_Toc161648941)

[4.3.2 相关公理的扩展 33](#_Toc161648942)

[4.4 机密性系统的建立 35](#_Toc161648943)

[4.4.1 机密性基础概念 35](#_Toc161648944)

[4.4.2 机密性核心公理及推理规则 36](#_Toc161648945)

[4.5 本章小结 39](#_Toc161648946)

[第五章 ECC-based RFID双向认证协议的形式化分析 40](#_Toc161648947)

[5.1 协议形式化分析 40](#_Toc161648948)

[5.2 ECC-based RFID双向认证协议认证性证明 43](#_Toc161648949)

[5.2.1 证明过程 43](#_Toc161648950)

[5.2.2 证明过程 45](#_Toc161648951)

[5.3 ECC-based RFID双向认证协议机密性证明 48](#_Toc161648952)

[5.4 本章小结 49](#_Toc161648953)

[第六章 总结与展望 50](#_Toc161648954)

[6.1 总结 50](#_Toc161648955)

[6.2 展望 51](#_Toc161648956)

[参考文献 52](#_Toc161648957)

[个人简介 在读期间发表学术论文 56](#_Toc161648958)

[致谢 57](#_Toc161648959)

# 主要符号说明

 协议中参与的主体

 秘密信息类

 所有消息和明文

 中的成员

 事件

 事件集合

 随机数集合

 集合中的一个随机数

 事件发生的主体，上的函数

 事件发生的主体持有的密钥

 事件为生成随机数的事件

 事件为发送类消息的事件

 事件为接收类消息的事件

 原始信息与事件有关

 逻辑关系包含

 不可测参数

 协议主体标识符

 基本序列

 事件在事件之前发生

 上局部有限的传递关系

 局部有限偏序

 逻辑独立

 弱匹配；为事件，为拥有相同信息的事件

 强匹配；且和具有因果关系

# 绪论

随着物联网（The Internet of Things，LoT）的快速发展，在互联网的基础上，通过结合射频识别技术（Radio Frequency Identification，RFID），各种信息传感器设备实现物物连接的网络，为人类提供方便舒适的生活，万物互联也不再遥不可及。但是随着RFID技术的迅速发展和应用，RFID系统安全性和隐私问题也日益突出。

## 研究背景及意义

射频识别技术是一种通过射频信号来实现无接触自动识别技术[1]，被广泛应用于物流管理、医疗保健以及工业制造等领域。一个完整的RFID系统主要由三部分组成，包括标签、阅读器和服务器。随着RFID系统的不断发展和完善，使其可以应用到越来越多的领域中，物流仓储、车辆识别与管理、贵重物品与票证的防伪、食品商品管理等领域都可以看到它的身影，也促使各行各业向着智能化和标准化进一步发展[2]。

在RFID系统中，由于标签和阅读器之间的通信通过无线信道进行传输，所以非常容易遭到非法入侵者的攻击，随着RFID的广泛应用，所面临的安全和隐私问题日益突出。学者们对RFID的隐私问题做了大量研究，基于物理方法也提出了许多方案[3]，包括Kill命令和静电屏蔽方法，这些解决方案是在牺牲标签一部分功能的基础上来实现RFID系统的安全性，虽然效果显著但同时大大增加了整个系统的成本。鉴于标签芯片的运算处理能力和存储空间极为有限[4]，传统的安全协议往往不适用于射频识别系统，这一局限性促使研究人员探索轻量级而又能保持高安全效率的RFID认证协议。针对这一需求，目前已经发展出基于不同加密算法的轻量级RFID认证协议，主要包括：按位逻辑运算、散列函数（亦称Hash函数）、现行的对称加密算法及公钥密码体制。这些方法旨在满足标签芯片对资源的低要求，同时确保认证过程的安全性和效率。尽管基于简单按位逻辑运算的RFID认证协议在运算简便性上与标签芯片的有限内存和运算能力高度匹配，但这种方法的安全性确实存在不足。这主要是因为仅依靠按位逻辑运算的安全机制，难以抵御复杂的攻击策略，如重放攻击、欺骗攻击等，这些攻击手段可能会危及数据的完整性和保密性。因此，尽管其低资源消耗在特定环境下具有明显优势，但在安全需求较高的应用场景中，这种协议可能不足以提供必要的保护。并且只使用散列函数和对称加密算法设计的RFID认证协议也被学者证明无法满足安全需求[6]。

椭圆曲线加密算法（Elliptic Curve Cryptography，ECC）作为一种高效的公钥密码体制，由于其在提供相同安全强度下所需的密钥长度远短于传统的公钥密码体制[7]，因此极其适合内存和运算能力受限的RFID系统。ECC的这一优势使其在资源受限环境中，如标签芯片，能够实现高安全性而不对系统的运行效率造成过大负担。相对于其他公钥密码体制，ECC能够在保持较低资源消耗的同时，提供相等甚至更高的安全保障，这使得ECC成为适应RFID系统安全需求的理想选择。

为确保射频识别系统的隐私与安全，形式化方法的应用显得尤为重要[8]。这些方法能够在协议运行过程中确保其安全属性，显著提高系统的安全性。形式化方法主要包括模型检测[9]、模态逻辑[10]以及定理证明[11]三种技术。相较于非形式化方法，形式化方法的优势在于其清晰的语义和准确性，它们能够无歧义地描述协议，并减少对专家经验和直觉的依赖。通过应用形式化方法，可以在设计阶段预先识别并修正潜在的安全漏洞，从而提供更为严谨和可靠的安全保障。

事件逻辑理论（Logic of Events Theory，LoET）是一种专门用于定理证明的形式化方法，它致力于描述和分析分布式系统中的协议和算法[12][13]。事件逻辑理论的基础框架由三个核心部分组成：基本建模语言、理论系统以及形式化描述系统。

（1）基本建模语言：这一部分的目的是为要分析的协议提供一种建模工具，使得协议的行为和特性可以被准确地描述和模拟。

（2）理论系统：包含了一系列的公理和推论，为协议的安全性和正确性证明提供了理论基础。这些公理和推论为分析协议提供了必要的逻辑支持。

（3）形式化描述系统：定义了协议的线程序列和匹配会话[14]，以确保协议的每一步骤都能被准确跟踪和验证。

随着技术的不断发展和研究的深入，事件逻辑理论也得到了扩展，其应用范围变得更加广泛[15][19]。这些扩展使得LoET不仅能够应对更加复杂多变的分布式系统安全需求，还增强了其在新兴技术领域中的适用性和有效性。

随着互联网的不断普及和迅速发展，信息安全问题已经成为一个各行各业都关注的重要问题，使用形式化方法对协议进行安全分析，保证通信安全，具有重要意义。

## 国内外研究现状

### ECC-based RFID协议研究现状

近几十年里，许多RFID方案被学者们提出有些并得到广泛应用，其中，基于椭圆曲线加密公钥密码机制的RFID方案受到越来越多学者的推崇。

在2006年，Tuyls和Batina[15]提出了基于椭圆加密算法（ECC）的首个RFID认证协议，即Schnorr协议。这一协议利用椭圆曲线离散对数问题作为其安全基础，有效地防御了恶意攻击者的被动攻击和假冒攻击，为RFID系统实现了双方的相互认证。尽管Schnorr协议在增强RFID系统的安全性方面取得了显著成效，但它仍存在一定的局限性，特别是容易受到追踪攻击的影响。追踪攻击可以威胁到用户的隐私安全，因为攻击者可能通过分析交互信息来追踪特定的标签，进而推断出标签持有者的行动轨迹。因此，尽管Schnorr协议在提高RFID系统的安全认证方面具有创新性，但在设计更高级的协议时，还需要考虑如何更有效地抵御追踪攻击，以全面保障用户的隐私和安全。为了解决这个问题，Batina在2007年改进了这个方案，提出Okamoto协议[21]来防止主动攻击，但是效果并不理想，此方案仍然容易遭受追踪攻击和中间人攻击。而后Lee在同一年分析了上述两个方案，发现二者都无法为标签提供匿名性，所以为提供匿名性并减少标签的工作量，提出了一种新的加密方案EC-RAC[22]。2008年Bringer等人发现Lee的协议存在跟踪攻击和假冒标签攻击的漏洞，为了抵御这两种攻击，提出了随机Schnorr协议[23]。

2009年，Martinez等人[24]基于零知识证明提出了一种ECC认证协议，但是被学者证明容易受到跟踪攻击。2011年，Godor等人[25]基于ElGamal算法提出一种新的基于椭圆曲线加密的RFID认证方案。同年，Zhang等人[26]引入随机密钥的思想，提出了基于ECDLP的RFID认证协议，但没有解决最基本的相互认证问题。随着RFID技术的发展，不同研究者提出了多种基于ECC的认证协议，以提高RFID系统的安全性和效率，这些协议各有优势和局限性。Liao等人[27]在2013年提出了一种基于ECC的RFID双向认证协议。通过引入ECC，旨在增强协议的认证能力。然而，尽管其在认证方面取得了进步，该协议在数据完整性方面仍存在不足，且遭遇了密钥安全性的挑战。具体来说，密钥一旦被泄露，便可能严重削弱系统的整体安全性，暴露于各种安全威胁之下。2016年，Alamr等研究者[28] 提出了一种新的基于ECDH（椭圆曲线Diffie-Hellman）的RFID双向认证协议。通过采用ECDH机制，该协议有效地解决了以往协议中存在的密钥泄露和跟踪攻击问题，从而在用户隐私保护和系统整体安全性方面取得了显著的提升。然而，尽管在这些方面取得了进步，该协议在设计时并未充分考虑到数据完整性的重要性。这一遗漏可能导致数据在传输过程中被篡改，而系统无法及时发现这种篡改行为。2019年，Dinarvand等人[29] 提出了一种新的基于ECC的RFID认证方案。该方案在安全性上有所提高，能够更有效地保护系统免受多种攻击。但是，该方案在密钥查找方面的效率较低，可能会影响到系统的整体性能，尤其是在需要快速处理大量请求的应用场景中。

综上所述，在最近十几年的时间里，基于ECC的RFID认证方案在不断发展中不断完善，已经能够很好地满足RFID系统所需要的隐私与安全需求。由于RFID系统是一个资源受限的系统，所以一个优秀的RFID认证方案不仅需要满足必要的安全属性，还要考虑方案的效率问题。

### ECC-based RFID协议形式化分析研究现状

基于椭圆加密算法学者们设计了大量RFID认证方案，但在实际应用过程中存在多种攻击，面对这些问题，学者们展开了对ECC-based RFID认证协议安全性分析。2014年，Liao等人[30]设计了一种ECC-based RFID认证方案，使用高效且令人信服的形式化方法证明了该协议在遭受各种攻击时的安全性。2016年，Qian等人[31]使用BAN逻辑形式化分析了一种基于ECC的RFID轻量化认证方案的安全性。

2021年，Kumar等人[32]吸取其他学者的不足设计了新的ECC-based RFID认证方案，使用AVISPA工具对协议进行仿真，结果表明协议对所有的被动和主动攻击都是安全的。同年，薛跳跳[33] 提出了一个基于椭圆曲线密码体制的RFID双向认证协议，并在这个基础上，假设阅读器和服务器之间的信道是无线的，又提出了一个基于ECC的RFID三方认证方案。随后使用ProVerif工具，运用模型检测的方法对一个基于ECC的RFID双向认证协议和一个基于ECC的RFID三方认证协议的安全属性进行了形式化分析与验证。

Gabsi等人[34]在2021年在分析之前学者研究的基础上，提出了一种基于ECC的RFID协议，并使用AVISPA对协议进行了形式化分析，提出的协议在计算性能和抵御不同攻击的强度之间做出了很好的平衡，能够抵御冒充标签、位置追踪和重放攻击，并能提供相互身份认证、机密性、匿名性和数据完整性服务的能力。

2022年，贺嘉琪等人[34] 提出了一种创新的基于Hash-ECC的RFID双向认证协议，并通过随机预言模型对其进行了分析。研究表明，该协议不仅满足了多个安全属性，还能有效抵抗多种入侵者攻击，如重放攻击、伪装攻击和跟踪攻击等。与其他一些典型的双向认证协议相比，这一新协议的显著优势在于其能够在保持高安全性的同时，显著减少计算时间和存储空间的需求。这一特点使其非常适合于资源受限的环境，如RFID系统，能够高效支持系统的多种安全需求。这表明，通过巧妙结合Hash函数和ECC，可以在提高RFID系统安全性的同时，优化系统的性能和资源利用效率，满足现代RFID系统对高效安全性的需求。

在ECC-based RFID认证方案的安全性分析研究中，学者们常采用BAN模态逻辑和一些非形式化方法。非形式化方法主要依赖于研究者的个人经验和对已知攻击手段的了解，以此对安全协议进行评估。然而，这种方法的主观性较强，缺乏严格的数学证明，因此得出的安全结论往往不够准确和可靠。BAN模态逻辑作为一种分析认证协议的逻辑工具，尽管在某些情况下能提供有用的洞察，但其理想化过程的非形式化、逻辑语义的不完整，以及对初始假设的过分依赖，限制了其在规约和描述ECC-based RFID协议所需满足的安全属性方面的应用。这些局限意味着BAN模态逻辑难以精确刻画和验证复杂的安全需求和条件，尤其是在面对高度复杂和不断演化的安全威胁时。

因此，对于ECC-based RFID认证方案的安全性分析，需要更加精确和可靠的形式化方法。这样的方法应具备严格的数学基础，能够明确定义安全属性，提供准确的安全性证明，从而更有效地评估和确保协议的安全性。通过发展和应用这些方法，可以提高安全性分析的准确性和可信度，为RFID系统的安全设计和评估提供坚实的理论支持。

窗体顶端

## 本文主要内容

本文通过对事件逻辑理论的创新性扩展，成功将其应用于基于ECC的RFID这一类协议的形式化分析与验证中，使扩展后的事件逻辑理论适用于带有复杂加密算法协议的安全性分析。本文的主要研究内容如下：

（1）详细介绍事件逻辑基本理论，给出事件逻辑基本定义，包括基本建模理论，公理系统以及协议的形式化描述。引入扩充谓词和以及相应的推理规则，增强其在协议分析中的实用性，特别是在处理消息的新鲜性和识别发送事件的首发性方面，有助于确保协议证明过程中事件类和基本序列的一致性，同时提高了事件排序的能力并降低了协议分析的复杂度。

（2）将事件逻辑与其他形式化方法进行比较，分析事件逻辑对于其他方法的优势与不足。对事件逻辑理论进行扩展，提出三个新事件类、、并给出相应的定义。根据新的事件类，扩展因果公理，定义新的因果关系。对其他相关公理及规则进行扩展，使得扩展后的事件逻辑理论能够分析带有复杂加密算法的协议。建立机密性系统，引入归纳机密规则，扩展LoET所能证明的安全属性范畴。

（3）利用扩展后的事件逻辑理论，深入形式化分析一个ECC-based RFID双向认证协议。首先对ECC会话密钥的生成过程进行形式化抽象描述，定义协议进程和基本序列用于描述协议，对协议所需满足的强认证属性进行了严格的形式化定义，通过理论推导，证明协议在合理假设下满足双向强认证性质，表明扩展的事件逻辑理论可以证明ECC-based RFID这一类带有复杂加密算法协议的安全属性，扩展了事件逻辑理论的使用范围。

## 论文结构安排

本文共分为六章，全面讨论了基于椭圆曲线密码的射频识别双向认证协议及其形式化分析，具体内容安排如下：

第一章 绪论。介绍研究背景及其重要性，概述国内外基于ECC的RFID协议发展和形式化分析的现状。重点阐述本文的主要研究内容，并对文章的结构进行说明。

第二章 ECC-based RFID认证协议及形式化方法概述。分析ECC-based RFID协议的基本框架，详细阐述协议的认证流程。同时，从模型检测、模态逻辑和定理证明三个角度介绍形式化方法。

第三章 事件逻辑理论。详细介绍事件逻辑理论的基础，包括基本建模理论、公理系统以及协议的形式化描述。重点讨论事件逻辑理论的公理系统，并展示如何利用该理论证明协议的安全性。

第四章 事件逻辑理论的扩展。对事件逻辑理论与其他形式化方法进行比较分析，指出事件逻辑在证明协议安全属性时的优势以及局限性；为增强事件逻辑的表达能力，引入、、三个 事件类并给出相应定义，并对相关的公理和规则进行扩展；为确保协议证明过程中事件类和基本序列的一致性，引入扩充谓词和以及相应的推理规则，来刻画消息的新鲜性以及发送事件的首发性，增强事件逻辑事件排序能力，降低协议分析复杂度；此外，建立机密性系统，引入归纳机密规则，扩展事件逻辑所能证明的安全属性范畴。

第五章 ECC-based RFID双向认证协议的形式化分析。基于扩展的事件逻辑对ECC-based RFID双向认证协议的认证双方进行形式化描述并对其安全属性进行证明。

第六章 总结与展望。总结本文的研究工作，并针对未来的研究方向进行展望，探讨如何进一步深化和扩展对ECC-based RFID双向认证协议及其安全性的研究。

# ECC-based RFID认证协议及形式化方法概述

随着射频识别技术的不断发展，RFID系统成为了物联网的重要组成部分[36]，轻量级的ECC-based RFID协议的安全性也愈加重要，使用传统的协议分析方法不可客观的描述协议的安全性，很容易忽略某些细微漏洞，所以要采取形式化的方法对ECC-based RFID协议进行分析。

## ECC-based RFID认证协议

ECC-based RFID协议是在RFID系统中借助椭圆曲线加密算法实现协议双方的相互认证，所以在开始分析协议前，先简单介绍一下RFID系统和椭圆曲线加密机制。

### RFID系统介绍

在当前广泛应用的RFID系统中，其架构主要包含三个关键组成部分：标签、阅读器以及后台服务器。这一系统的工作流程起始于将独特信息存储在贴附于需识别物品上的标签中。随后，阅读器与标签进行相互认证，并将收到的信息转发至后台服务器。服务器则通过复杂的计算过程验证信息的合法性。此过程确保了RFID系统在各种应用场景中的可靠性和安全性，从而实现高效的物品跟踪和管理。

RFID（射频识别）系统的工作机制相对直观，其核心由两部分组成：阅读器（读写器）和电子标签（标签）。工作原理概述如下：

1. 信号发送：阅读器通过其天线向周围环境发送特定频率的射频（RF）信号。这些信号具有一定的有效范围，即识别区域。

2. 电子标签激活：当电子标签进入阅读器的有效识别区域内，标签的天线捕获到射频信号，产生感应电流。这个感应电流为电子标签提供了必要的能量，使其激活。激活后的电子标签能够使用这股能量来开启其内部电路。

3. 信息传递：一旦被激活，电子标签通过其内置天线将存储的编码信息（如唯一的身份标识符）以调制信号的形式发送回阅读器。这个过程通常称为反向散射（backscatter）。

4. 信号接收与处理：阅读器的接收天线捕获从电子标签发回的调制信号。阅读器内部的解调和解码系统对这些信号进行处理，提取出有效信息。然后，这些信息被传送到后台服务器进行进一步的处理和分析，如存储、跟踪或管理。

RFID系统的这种工作方式使其在许多应用领域中非常有用，包括但不限于库存管理、货物跟踪、个人身份验证、无线支付系统等。其无需直接视线和能够同时识别多个标签的特点，为自动化识别和数据捕获提供了极大的便利。

电子标签的构造主要包括一个内置的微型芯片和射频天线，其中芯片用于数据存储和执行有限的计算任务。每个电子标签均配备了唯一的标识符，用以确认其身份。根据身份认证后标识符是否能够更新，电子标签被分为静态标签与动态标签两种类型。此外，电子标签还根据供电方式的不同，被细分为有源标签、无源标签和半有源标签。有源标签配备电池供电，而无源标签则通过阅读器发射的电磁波激活，半有源标签则介于两者之间，既有电池也能通过电磁波获取能量。这些分类反映了电子标签在不同应用场景下的多样性和灵活性。阅读器是连接电子标签和后台服务器的桥梁，能够与标签进行无线通信，并且自身的存储容量和计算处理能力都要比标签强。在RFID系统中，后台服务器扮演着至关重要的角色，作为系统的核心，它具备最强大的存储容量和计算处理能力。服务器内部存储了系统中所有标签和阅读器的必要信息，这些信息在认证过程中发挥着关键作用。当阅读器向服务器发送验证请求时，服务器负责对这些请求进行确认并做出相应的回复，以此完成标签和阅读器之间的相互认证。通过这种方式，后台服务器确保了RFID系统的安全性和高效运行，是整个系统正常工作的关键支撑。

### 椭圆曲线密码体制

椭圆曲线加密体制(ECC)最初是由Kobilitz[37]提出的。椭圆曲线是指在给定的维尔斯特拉斯(Weierstrass)方程



下定义的平面曲线，通常用来表示这样的曲线。其中属于域，可以是有理数域、复数域或有限域。椭圆曲线上的有限域是所有解的集合，方程表示为，其中，且。椭圆曲线有一个特殊的点，称为无穷远处的点，用表示。椭圆曲线的运算规则如下：

对于，有，；

对于椭圆曲线上的点和，其中，，且，则有：





椭圆曲线上的加法运算和乘法运算都具有几何意义，下面简单描述这两种运算：加法运算：假设在椭圆曲线上有两个不同的点P和Q，要找到这两点的和R = P + Q的几何过程是这样的：首先，画一条直线L通过点P和Q。这条直线将会与椭圆曲线相交于第三点M。然后，将点M关于x轴做对称得到点R，即为P和Q的和。特别地，如果P、Q、M三点共线，那么它们的和定义为无穷远点0，这种情况相当于椭圆曲线上的“零元素”。

乘法运算：当我们讨论P + P（即点P自身的加法）时，情形稍有不同。由于不能直接作通过P和P的直线（因为这将是一条垂直线），我们改为作椭圆曲线在点P处的切线。这条切线将会与椭圆曲线相交于另一个点，我们再将这个交点关于x轴做对称，得到的点即为2P。这便是椭圆曲线上点乘运算（或称标量乘法）的几何意义。要获得3P，我们只需将2P与P相加（即计算2P + P），重复利用上述加法运算的几何过程。

这些几何运算是椭圆曲线密码学的基础，它们的性质使得反向操作（如从R找到P和Q）变得极其困难，为ECC提供了其安全性基础。下面介绍椭圆曲线上的离散对数问题。

假设椭圆曲线在有限域上，，的阶为，是由生成的循环子群，给定，求，使得。

简单的来说，椭圆曲线对数问题就是一个求解过程：假设是椭圆曲线上一点（称为基点），为一整数，已知和，求。

椭圆曲线加密体制是基于椭圆曲线离散对数问题的困难性建立的，这一数学难题的解决时间复杂度为指数级别，超出了其他公钥加密算法所能达到的范围。这种高度的计算复杂性为ECC提供了强大的安全性，使其在相同安全级别下，能够使用比其他公钥加密体系更短的密钥长度，从而在提供高安全性的同时，减少计算资源的消耗和提高系统效率。

椭圆曲线密码体制与其他公钥加密算法如RSA加密算法相比，主要具有以下几点优势：

（1）密钥长度短：椭圆曲线密码体制使用的密钥长度相对较短，可以实现与RSA算法相当甚至更高的安全性。

（2）安全性高：椭圆曲线密码体制的安全基础在很大程度上取决于椭圆曲线上的离散对数问题的计算复杂度。与RSA算法依赖的大数分解问题相比，椭圆曲线上的离散对数问题被广泛认为更加困难，这使得ECC在相同密钥长度的条件下提供了更高的安全性。

（3）加密、解密速度快：ECC的加密及解密速度比RSA算法更快，这让ECC在移动设备和嵌入式系统中更受欢迎[38]。

（4）存储空间和带宽需求小：因为椭圆曲线密码机制的密钥长度更短，所以ECC需要的存储空间和带宽比RSA更少。

综上所述，椭圆曲线密码机制是一种高安全性、加密解密速度快、存储空间和带宽需求少的加密算法，因此，椭圆曲线密码机制在许多领域得到了广泛的应用，在RFID系统认证协议中更是如此。

### ECC-based RFID认证协议的安全需求

RFID系统中，由于电子标签和阅读器之间进行的是无线通信，所以在网络中更容易遭到入侵者的非法入侵，如图2-1。

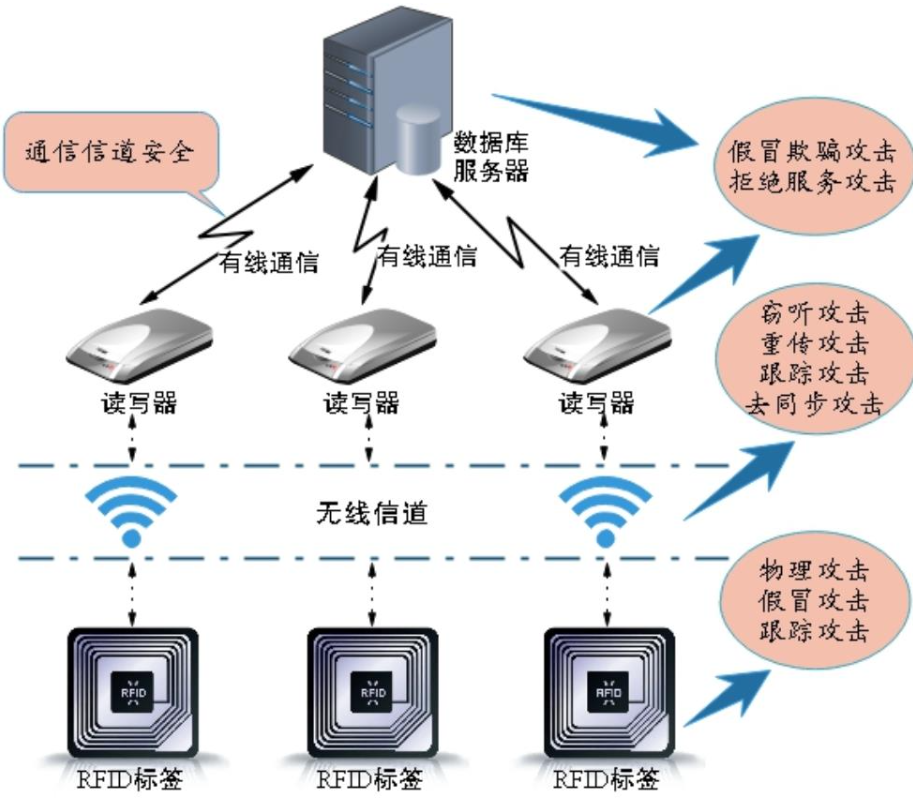


图2-1 RFID系统受到的威胁

Fig.2-1 Threats to RFID systems

因此，设计的认证协议必须满足一些安全性质，其中相互认证性是RFID协议首先要满足的安全需求。在协议认证过程中需要满足以下需求：

（1）相互认证性：旨在确保认证机制能够在多个参与方之间实现实时的双向认证。这一过程中，电子标签与后端服务器将通过相互认证机制，有效阻断未授权用户的网络访问尝试。

（2）秘密性：在电子标签系统中，标签所含的私密信息，如物品详情，须在无线通讯过程中严格保密，以避免恶意攻击者的窃取和滥用。这是通过确保每次通讯使用一次性的会话密钥来实现的，即便某次会话密钥被泄露，也不会危及到其他会话的安全性。这种做法有效地阻止了通过伪造标签对服务器进行欺骗的行为。

（3）前向安全性：即使在恶意攻击者成功获得某个标签中存储的秘密信息的情况下，该攻击者也无法利用这些信息来推断出该标签在之前通信过程中使用的敏感信息。

（4）会话密钥不可预测性：在认证交互过程中，会话密钥的生成需确保绝对的随机性，以防止任何外部实体能够事先决定或预测这些密钥。

（5）匿名性：确保单个标签在重复使用过程中对于恶意攻击者的身份不可识别，防止攻击者能够追踪到特定的标签。由于RFID系统中的标签数量众多且标签可能会被多次使用，在不采取适当保护措施的情况下，恶意攻击者通过技术手段捕获标签的固定标识符，可能会对标签的活动轨迹进行跟踪，从而侵犯用户隐私。

## ECC-based RFID双向认证协议分析

基于上述描述，本文选取一种基于ECC的射频识别安全认证协议[39]进行分析。协议主体包括服务器与标签两部分，其中后台服务器与阅读器之间的连接方式为有线信道，所以我们把这一部分的通信看作是安全的，把这两者看作一个整体，来与电子标签进行无线通信。双方使用挑战应答模式进行认证。该协议分为系统设置阶段和认证阶段。在系统初始化阶段，参数配置遵循以下步骤：首先，生成两个大素数，其中定义了有限域的规模，即有限域中元素的总数；接下来选择一条安全的椭圆曲线，其中，随后确定一个椭圆曲线上的基点，其阶数为 ；系统中的服务器和每个标签都需要存储椭圆曲线的参数集;服务器选择一个随机数作为自己的私钥，并计算相应的公钥（通过椭圆曲线上的点乘计算得出）；最后为每个标签在椭圆曲线上选择一个随机点作为自己的身份认证因子，服务器将此身份认证因子保存到自己的数据库中并把自己的公钥连同身份认证因子一起存储于标签的内存中，以完成系统设置和个体标签的初始化。本文分析的协议认证流程如图2-2所示。



图2-2 基于ECC的RFID双向认证协议认证过程

Fig. 2-2　 ECC-based RFID Two-way Authentication Protocol Authentication Process

（1）服务器生成随机数并进行标量乘运算，将发送给标签。

（2）在接收到消息后，标签生成随机数，进行标量乘计算并生成认证信息，并将发送给服务器。

（3）当服务器接收到来自标签的认证信息后，其首要任务是根据接收到的数据恢复出标签的身份认证因子；完成恢复操作后，服务器会将得到的身份认证因子与服务器本地数据库中存储的所有标签的身份认证因子进行匹配对比。如果比对过程中未找到匹配的身份认证因子，那么服务器将判断该标签为非法，随即终止与该标签的认证协议，拒绝进一步的通信或交互；反之，如果服务器成功匹配到相应的身份认证因子，这表明该标签为合法的标签，随后，服务器利用自己的私钥进行计算，并将发送给标签。

（4）在标签接收到服务器发送的认证信息后，它会执行一项关键的验证操作，即检查是否成立，这一步骤是标签确认服务器身份的重要环节，旨在确保标签与一个合法且可信的服务器进行通信。条件满足，标签便认定服务器是合法的；否则标签会立即终止与服务器的通信协议，拒绝进一步的数据交换。

在上述的ECC-based RFID认证协议交互过程中，服务器和标签先后确定双方认证的可信性，简化的交互过程如图2-3所示。



图2-3 双向认证中主要交互信息描述

Fig. 2-3 Description of Main Interactive Information in Mutual Authentication

## 形式化方法概述

随着网络技术和物联网技术的不断发展，对软件和硬件的要求也越来越高，其中计算速度的提升和体系结构的复杂化尤为显著，这些进步虽然大大推动了技术的发展，但同时也带来了安全可靠性的巨大挑战[40]。特别是在那些安全至上、极其注重信息安全的领域上，如果系统一旦违反了期望的执行步骤，不仅会损害软硬件及应用系统的可靠性和可用性，还会造成无法逆转的后果[41]。二十世纪六七十年代，由于软件危机的爆发，人们迫切需要一种安全可靠并且严谨的方法来确保软件的可靠性，如此，形式化方法应运而生。

形式化方法依托于深入的数学原理，利用精确的数学概念与逻辑推理技术来对安全协议进行细致的描述与分析。这种方法能有效揭示设计上的不一致性、模糊性或缺陷，简化协议分析的复杂性，进而促进其规范化和实用化。在当前的安全协议分析领域，形式化方法已成为一个不可或缺的工具[42]。

形式化方法的探索起源于20世纪60年代末，当时学界开始致力于安全协议的形式化模型研究，并据此推荐了标准化的协议描述语言。随着时间的推移，这些技术经历了不断的发展与完善，现已广泛应用于电路和协议设计领域，取得了显著的成就。当前，如何有效利用形式化方法提升安全协议设计与分析的可靠性，已成为该领域内的研究焦点。现在的形式化方法主要分为三类[43]，如图2-3所示，分别为模型检测、模态逻辑和定理证明。



图2-4 形式化方法分类

Fig.2-4 Classification of Formal Methods

### 模型检测

模型检测[44]是一种验证有穷状态下并发系统的自动化方法，具备自动化验证过程和验证速度快等优点，被广泛运用在安全协议的分析与验证、系统的安全性设计与验证等领域。由于模型检测考虑的是协议的有限行为，当分析的协议较为复杂时，会出现状态爆炸问题，所以该方法更适用于找到协议的漏洞，而不是验证协议的正确性。为缓解状态爆炸这一问题，在对系统进行建模时，需要定义系统的状态以及对应的状态迁移函数，为此模型检测器需要牺牲一定的空间状态来验证是否能满足安全属性，所以模型检测方法只适用于那些模型较小、状态数以及迁移数都比较小的系统。对于那些较大的系统，使用模型检测方法可能会找不到违反性质的反例，但这不意味着这个系统就是安全的，因为模型检测器很有可能没有完全遍历整个状态空间而没有找到反例的存在。尽管模型检测方法存在着种种限制，但是由于其自动化程度高而且会自动生成违反性质的反例等这些特点，它仍受到学者们推崇，广泛的使用于安全协议的形式化验证[45]。以下介绍几种常见的模型检测工具：

常见的模型检测工具有FDR（Failures Divergence Refinement），ProVerif（Protocol Verifier），Murφ，SPIN等。

FDR[46][47]，一款基于通信顺序进程（CSP）[48] 的并发语言模型检测工具，专为描绘并验证系统安全问题的规约而设计，以确保其符合预定的描述性要求。此外，FDR也被应用于审查状态机的确定性问题。由于CSP的设计初衷是为了抽象地表达通信参与者的行动模式，FDR因而特别适用于对抽象属性的检验。

ProVerif[49]是一个基于Dolev-Yao模型[50]的形式化自动分析密码协议的模型检测工具，使用应用PI演算的变体来描述协议，能够处理不同类型的密码原语以及无限数量的并行协议会话和消息空间。由此，该工具可以验证协议是否能够顺利执行以及是否能够达到预期目标。

Murφ[51]，依托于Murφ描述语言和相应的编程框架，是专门用于协议验证的高级工具。它在工业级协议分析中得到了广泛应用，特别是在处理多处理器缓存同步和内存模型的协议问题上表现卓越。Murφ的描述语言融合了传统编程语法和有限自动机的描述能力，全面覆盖了所有潜在的协议执行环境。通过Murφ编译器[52] 的作用，可以将描述语言转换为编译代码，进而生成一个非确定性的有限状态自动机，为协议验证提供了强大的支持。

SPIN[53]是被应用于追踪分布式系统设计中逻辑设计错误的分析并发系统逻辑一致性的工具，是现如今应用最为广泛、功能强大的通用模型检测器。因简洁明了和高自动化程度等优势，SPIN在验证安全协议的安全属性等方面取得了显著的成就。使用静态分析技术等新方法，将模型简化从而大幅度降低协议的状态数，缓解了模型检测器遍历系统状态空间时出现的状态爆炸问题。SPIN工具不仅是在系统设计阶段识别逻辑漏洞的有效手段，而且还被广泛应用于密码协议的分析验证中，确保这些协议能够准确实现其预定义的属性。SPIN由于其独特特点与其他模型检测工具相比更容易让人所接受，因为SPIN不要求将系统的具体执行动作输入其中，而是先对系统进行形式化的描述，集合线性时态逻辑LTL[54]（Linear Temporal Logic）对系统所要满足的性质进行形式化规约，最后再通过SPIN验证系统是否满足性质规约公式，如果最后系统不满足性质规约公式，SPIN会给出相应的反例。

图2-4所示为模型检测验证框架：



图2-5 模型检测验证框架

Fig.2-5 Model Checking Verification Framework

### 模态逻辑

模态逻辑是一种专注于知识与信念推理的形式化方法，为分析和验证安全协议提供了一种直接且高效的途径。它主要通过命题和一套推理规则来表达和推导主体对信息的知识或信念状态。命题用于描述主体对某一消息的认知，而推理规则则允许从现有的知识和信念出发，推导出新的结论。在安全协议的分析中，模态逻辑能够帮助识别和验证协议中的安全属性，如认证、保密性和完整性等。通过将协议操作映射为知识和信念的变化，研究人员可以应用模态逻辑的推理规则，从初始状态出发，逐步推导协议的执行过程，验证最终状态是否满足安全要求。这种方法不仅能够准确地捕捉到协议设计中的潜在弱点，还能够在协议设计早期阶段就识别出可能的安全问题，从而提高安全协议的整体质量和可靠性。

BAN逻辑[54]，作为模态逻辑领域内最为人所熟知的一个分支，由Burrows等研究者于1989年首次提出。以其直观简洁的特性著称，BAN逻辑能够有效地识别安全漏洞，并分析密码协议中诚实主体信仰的变化过程。这种以主体信仰变化为核心的分析方法，标志着密码协议分析领域的一大创新，也是应用于此类分析的首个形式化方法。BAN逻辑作为首个模态逻辑方法应用于安全协议的分析，使得安全协议与数学逻辑之间建立了一种联系，并通过一系列的逻辑符号语言对安全协议进行形式化推理。BAN逻辑引入了多个创新性的概念来描述和验证安全协议的执行过程，比如通过引入特定的逻辑结构来精确描述协议中的关键概念，如信任、认证和授权等。这些逻辑结构有助于清晰地表达和分析协议的安全目标和假设条件；通过合适的密钥管理机制来确认消息发送者的身份；提出由可信赖的第三方服务器生成的密钥被认为是“良好”的，即这些密钥在协议的安全性分析中可以被假设为安全可靠的；引入了时间戳概念，通过对消息附加时间戳，可以有效防止重放攻击，确保消息在传输过程中的时效性和一次性。

尽管BAN逻辑在分析和验证安全协议方面取得了显著进展，但它依然面临着一些显著的缺陷。这些缺陷主要包括其公理系统的不完善性、语义的不清晰性，以及协议理想化过程对分析者直觉的过度依赖。这些问题不仅影响了BAN逻辑在具体应用中的有效性，也限制了其使用范围，尤其是在处理复杂或新型安全协议时。但由于使用直观并且简单，分析过程简洁等特点，仍然广泛应用于各个领域，在分析安全漏洞等方面效率极具优势。针对BAN逻辑在分析特定安全协议时遇到的局限性和缺陷，学术界提出了多种改进方案，以拓宽和深化安全协议分析的理论和应用。这些改进基于BAN逻辑，发展出了GNY逻辑[56]、AT逻辑[57]、VO逻辑[58]、SVO逻辑[59]和Kailar逻辑[60]等一系列BAN类逻辑，每种都在原有基础上做出了创新和补充。运用模态逻辑方法分析安全协议安全属性的分析框架如图2-5所示。



图2-6 模态逻辑分析框架

Fig.2-6 The Analysis Framework of Modal Logic

模态逻辑在协议分析与验证中的应用步骤：

（1）协议理想化：这一步骤要求使用形式化语言对协议的交互流程进行准确描述，确保所有细节均被清晰表达。

（2）初始化假设：定义协议在理想执行条件下的基本预设假设，为后续分析建立起始点。

（3）逻辑推演：基于初始化假设，利用模态逻辑的公理和推理规则进行逻辑推演。这个过程中，通过模拟协议的执行和参与者的逻辑推理，来揭示参与者通过协议交互最终可能获得的知识或形成的信仰。

（4）安全性评估：对比逻辑推演得出的结果与协议的预期目标，分析判断是否达成预期的安全保障。

### 定理证明

定理证明方法的核心思想是将研究的目标系统的所满足的性质规约定义为一个严谨的数学逻辑命题，通过相应的公理系统及其推理规则，采用演绎推理的方法来证明命题的成立。定理证明方法通过对安全协议及其操作进行精确建模，将协议本身抽象为一套公理系统。在此基础上，协议旨在实现的安全目标被形式化为需证明的定理。因此，这些定理的验证结果直接决定了协议是否能够实现其预定的安全目标。

定理证明方法主要包括以下几种：

（1）Paulson归纳法[61]。此方法通过将安全协议表述为一系列事件迹的集合，利用定理证明器Isabelle进行归纳式证明。这种方式旨在验证协议的所有可能执行路径上是否均能满足既定的安全断言。

（2）串空间模型[62]。本理论框架采用集合论和有向图工具来形式化地表达安全协议的状态以及它们之间的交互关系。通过分析这些状态之间的偏序关系，特别是对集合内最小元素的定义与证明，该方法能够有效地识别潜在的攻击节点。

（3）协议组合逻辑（PCL）[63]。PCL是一种高度先进的形式化分析方法，它巧妙地融合了模态逻辑的语法结构，并从串空间理论中吸收了“线索”（clue）的概念，这一创新使得PCL能够有效描述和分析安全协议的并行执行过程。通过引入程序断言，PCL能够清晰地表达程序执行过程中的状态变化，这不仅增加了分析的清晰度，也提高了其准确性。

（4）事件逻辑理论。事件逻辑理论提供了一种强大的框架，专门用于在分布式系统环境下分析和验证协议及算法的安全性。它通过对安全协议中的关键原语进行精确的形式化规范，使得对协议的强认证属性进行严格证明成为可能，从而确保了协议安全属性的验证。

在验证协议正确性的方法论中，定理证明法突出以其专注于证明协议正确性而不必面对状态爆炸问题的优势，相较于模型检测方法而言。此外，相比于模态逻辑方法，定理证明法在分析安全协议时提供了更清晰的语义和一个更为完整的推理规则体系。这种方法通过建立精确的数学模型和定义明确的逻辑推理规则，使得对安全协议的分析和验证能够在一个严格的逻辑框架内进行，大大提高了安全性验证的可靠性和准确性。然而，尽管定理证明法在证明安全协议的安全属性方面具有显著优势，其证明过程大多需依赖手动执行，这一点增加了其应用的复杂度，也限制了实现完全自动化的可能性。如下图2-6，展示了定理证明方法对协议的安全属性进行形式化分析的流程。

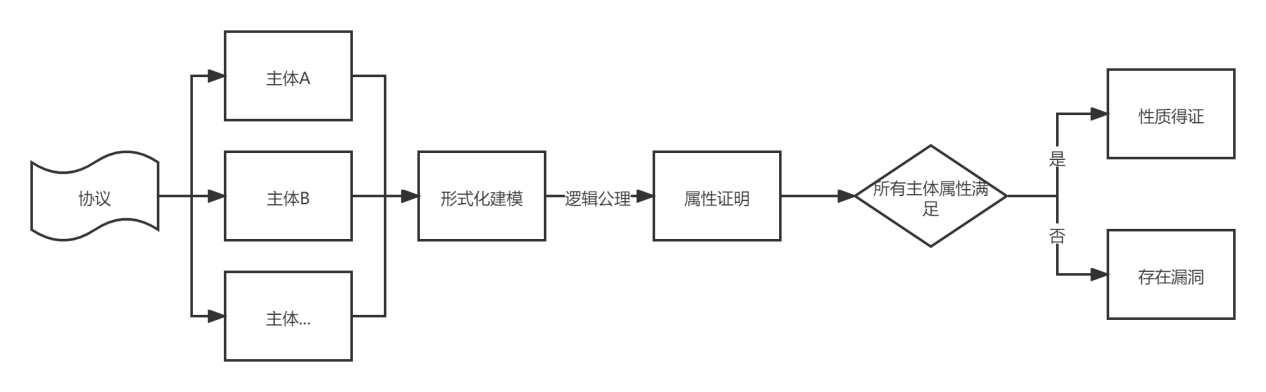


图2-7 定理证明分析流程

Fig.2-7 The Analysis Process of Theorem Proving

## 本章小结

本章对RFID系统以及椭圆曲线密码机制进行了简单介绍，选取一个ECC-based RFID协议，对协议主体之间的交互流程进行了阐述和分析，为后续证明协议的安全属性奠定了基础；还对几种不同的形式化方法进行了详细介绍，分别为模型检测、模态逻辑和定理证明。

# 事件逻辑理论

安全协议是如今网络通信的基础，提出针对安全协议的安全属性进行分析的方法是具有重大意义的。在开放且复杂的网络环境中，如果安全协议不能抵御恶意入侵者的攻击，则无法保证通信主体之间的安全性，安全协议一旦受到攻击，可能导致信息泄露、数据篡改等严重后果，给组织和个人带来巨大损失。因此，研究和开发用于评估和验证安全协议安全属性的方法具有极其重要的意义。形式化方法是分析协议安全属性的强有力方法，事件逻辑理论是一种描述分布式系统安全性的方法。2009年，肖美华教授和Mark Bickford教授首次提出将事件逻辑理论应用于安全协议的安全属性证明，这一创新性的工作为安全协议的设计和分析开辟了新的路径。使用事件逻辑对安全协议进行形式化分析，不需要对恶意攻击者的执行动作进行显示推理，只需要对协议主体间的交互动作进行推导即可。基于事件逻辑理论对协议的安全属性进行分析在如今应用的十分广泛并取得了不错的成就[64][65]。本章详细介绍事件逻辑理论，为后续扩展事件逻辑理论提供理论基础。

## 基本建模理论

### 消息自动机

消息自动机是一种模拟复杂系统通信行为的特殊类型的非确定性状态机。它主要通过执行发送和接收消息的操作，基于这些操作完成内部状态的转换或迁移。这种模型特别适用于描述和分析分布式系统或网络通信协议中的动态交互过程，因为它能够精确地捕捉到系统组件间的消息传递行为及其对系统状态的影响。在简化的类型约束下，消息自动机一般被划分为状态()、行为()和消息()三个基本类型。

 （3-1）

上述公式描述事件在消息自动机的状态迁移。将一个可能计算时状态、队列和事件交替的流，描述为，当事件是一个内部操作时，那么。当事件是一个消息接收时，那么，指需要从队列中接收的消息。

### 不可猜测的原子

事件逻辑理论中有三大原始值类型，分别为原子类型、标识符类型和布尔值类型，其中原子类型使用表示，标识符类型使用表示，通常写作大写字母。布尔值类型使用表示。

原子类型是消息的一种类型，在事件逻辑中通常用来表示挑战数、密文及密钥等不可猜测的数据，其中的成员用表示。为基本类型，没有结构且不能被生成，是不可预测的。

在对协议进行抽象建模时，首先把类型引入到了模型中，分配用来表示具有秘密性的数据成员，且由于的不可猜测性，每个成员都是相互独立的存在，因此需要一个独立性命题  来刻画的获取。

事件逻辑中关于独立性的定义为：给定一个原子，当且仅当独立性命题()为真时，类型的值与原子相互独立。

### 事件序、事件类及事件结构

一个分布式系统的运行可以由分布式计算形式化模型定义，在运行过程中能够识别信息传输的点在事件逻辑中称为事件，记作或，将与事件相关的原始信息定义为。

1. 事件序

定义事件序为，其中是事件上的函数，因果顺序是事件上一个局部有限的传递关系，即事件包含有限个前驱。在事件逻辑理论中，事件的发生地址是事件发生的主体，所以对于某些标识符，有。可以将同一主体的 事件序记为，简写为。

1. 事件类

在事件逻辑理论中，通过事件对协议进行分类描述，使用事件序语言以及事件类对协议进行构建。在协议运行过程中，存在多种事件发生，包括挑战数的生成、消息的发送与接收、签名与签名验证、消息的加密与解密这七类事件，它们的类型列表为：

 （3-2）

类类型相同，类与类类型相同，均为三元组。对于类中事件有相同的三元组类型，即。存在事件，表示事件是主体通过密钥将明文加密生成密文，主体拥有消息和密钥；存在事件，表示事件是主体通过密钥将密文解密生成明文。

1. 事件结构

为对协议进行抽象建模，需构建一个能够反应分布式系统时间性和空间性特点的模型。因此，事件逻辑理论构建了以事件为基本元素的事件结构。事件逻辑中的事件记作，本质是主体执行动作而产生的实例，例如主体执行发送动作将会产生发送事件，执行接收动作会产生接收事件。

事件语言(Event Language, EL)是扩展的语言，其中符号表示所有事件的集合，而是定义在事件集合上的一个函数，它表明了事件发生的地址，即表明了分布式系统空间性的特点，因果序表明了两个事件之间具有前后因果的关系，是定义在事件上的传递关系，表明两个事件发生的先后顺序，这表现了分布式系统时间性的特点。事件逻辑理论中，事件发生，则相应的发生地址表明了事件发生的主体。如果两个事件，发生于同一主体且具有因果关系，则可以表示为，可以简化记作为，该符号表明事件发生于事件之前，事件之间具有因果关系且都由同一主体产生。

事件结构是满足以下规则的事件语言模型。

（1）表示局部有限偏序，且每个事件包含有限个前驱。

（2）是局部事件序，即同一主体上所有事件集成员的总排序。

（3）和事件的原始信息息息相关，位置是事件的发生主体。

## 事件逻辑理论公理系统

事件逻辑是一种用于证明协议安全性的核心方法，它通过一系列公理和推理规则来分析和验证协议的安全属性。主要的六大公理及相关引理构成了事件逻辑的基础，使得安全性的证明过程既系统化又形式化。接下来将对这些公理进行简要介绍。

在事件逻辑理论中一般使用来表示那些无法被外部猜测的密钥，如对称密钥和私钥，使用标识符表示公钥。因为私钥和对称密钥不同，所以类可以表示为：

 （3-3）

事件逻辑理论的证明还需三个附加函数：

 （3-4）

其中，使用函数构建密钥之间的关系，函数为每个主体分配一个。

（1）密钥公理

密钥公理对密钥之间的关系进行定义：对称密钥只能匹配它本身，私钥只能匹配它所对应的公钥，两个不同的主体不能拥有相同的私钥，如下式所示。

 （3-5）

（2）因果公理

因果公理在事件逻辑理论中起着至关重要的作用，它通过建立事件之间的因果关系，确保了协议的逻辑正确性和安全性。其中,类似，两个公理都是关注协议行为的匹配性，即对于任何接收事件，必须存在一个先前发生的、内容相匹配的发送事件，在任何验证事件发生之前，必须存在一个对应的签名事件，且两者涉及的信息内容相同。引入了新的密钥元素，专注于解密和加密事件之间的匹配性。该公理规定，在任何解密事件发生之前，必须存在一个与之对应的加密事件，且两者涉及的信息内容和使用的密钥必须相匹配。这保证了加密信息的保密性，只有拥有正确密钥的主体才能解密并获取原始信息。公理如下式所示。

 （3-6）

（3）不相交公理

不相交公理分为两个部分，第一个不相交公理规定任意七个事件类不在其他事件类中，如下式所示。

 （3-7）

第二个不相交公理在安全协议分析中起着重要的作用，它旨在确保系统中使用的挑战数、私钥、签名以及密文保持互不相交，即它们不应使用相同的进行表示或生成。不相交公理特别强调，签名和密文之间应保持不同。签名通常是通过对明文进行哈希加密后再使用私钥签名的结果，而密文则是直接通过加密算法将明文加密得到的。尽管签名和密文都是源自相同的明文信息，但由于它们生成过程的不同，因此它们在逻辑上和物理上都应当不相同。第二个不相交公理如下式所示。

 （3-8）

（4）诚实公理

事件逻辑理论中函数对诚实主体进行断言，被标记为诚实的主体不会泄露其私钥给任何其他方。这个假设是建立在对参与协议的实体信任程度的基础上，确保只有被认定为诚实的主体才能使用其私钥进行关键的加密、解密和签名操作。公理如下式所示。

 （3-9）

（5）流关系公理

流关系是挑战数在因果序事件间的关联。类包含的七个事件类成员用来指代，当且仅当中包含，为真，具体如下式所示。

 （3-10）

流关系表示从动作流向动作，主要包含以下三种情况。第一，动作和动作发生在同一主体；第二，动作和动作分别为发送事件和接收事件，且以明文方式发送；第三，位于加密事件的明文中，且以密文的形式流向匹配的解密事件。具体流关系递归如下式所示。

 （3-11）

引理1：如果，则且。

如果第一个动作是加密，且第二个动作包含第一个动作的密文时，两个动作之间的关系写作，即。

如果在流关系的传递闭包中事件拥有，则事件可能拥有，表示为

。

引理2：如果，则。

（6）挑战数公理

挑战数公理包含三个部分，分别为，其中为流属性公理，规定挑战数与其唯一事件的关联性，如下式所示。

 （3-12）

由，根据以及引理1可得出，同理可得，因此，由此推出引理3，挑战数的唯一性。

引理3：如果且，则。

是关于签名和加密以及它们与事件相关性的重要公理。这两个公理帮助建立了签名和加密动作与特定信息之间的逻辑关系，而不是将这些安全动作直接与独立事件相关联。由这两个公理可知当一个动作包含签名或者密文的时，可以推断出拥有相同信息的签名或加密动作，具体如下式所示。

 （3-13）

## 事件逻辑形式化描述协议

### 线程和匹配会话

事件逻辑理论中，协议单个状态位上操作的有序列表称为线程，定义如下。

 （3-14）

表示线程是发生在线程之前的一个相邻线程，表示两个线程之间存在的因果关系，即。线程中的消息是线程中所有和动作的集合，具体如下所示。

 （3-15）

存在消息和，前者属于发送事件上的消息，后者属于接收事件上的消息，且二者传递的消息内容相同，则两条消息构成一个弱匹配关系，即。如果发生在之前，且二者之间有直接因果关系，则构成一个强匹配关系，即，具体如下所示。

 （3-16）

两个线程，都存在个消息事件对，如果他们对应的消息事件对都满足强匹配，则线程，构成长度为的强匹配会话，记作。如果上述消息事件对仅满足弱匹配，则满足弱匹配会话，记作。

### 基本序列和协议动作

在安全协议分析中，基本序列定义了协议动作的参数集合，其中主体通过标识符，表示。根据协议规范，一个遵守规则的主体可以同时参与协议的多个实例，即多线程操作。事件逻辑理论支持多主体同时参与同一协议，增加了协议执行的灵活性。在这一框架下，如果主体严格遵循协议，则其能够在不同的执行线程中与主体进行交互。然而，若在交互过程中遭遇连接失败或信任问题，则预定的接收动作将不会被执行，这一机制确保了协议交互的安全性和可靠性。

事件逻辑理论将基本序列形式化定义为两个位置与一个线程之间的关系，当线程是基本序列给定的位置参数时，则这个关系为真，定义如下式所示。

 （3-17）

使用协议动作来描述协议，将其定义为一个类，类中所有成员由标签和值组成，记为，其中为七种协议动作的常量字符串，对应相应的类型。类中成员组成如下式所示。

 （3-18）

如果协议动作(Protocol Action)对应事件，则有

 （3-19）

如果对应线程，且二者拥有相同的长度，即，则事件匹配满足。

### 协议描述

事件逻辑理论使用类型的基本序列关系表定义协议，协议经过形式化描述后是状态关系点上的谓词，具有类型。协议定义如下。

 （3-20）

假设主体、为诚实主体且二者都遵循协议，主体完整发起基本序列的实例，主体也全部响应基本序列的实例。如果接受消息和发送消息的内容一致，则构成合法匹配会话。消息双方完成身份认证，匹配会话过程满足强匹配，协议中基本序列对个消息进行认证，认证过程如下式所示。

 （3-21）

## 事件逻辑证明协议安全性流程



图3-1 事件逻辑证明协议认证性流程

Fig.2-6 The Logic of Events Theory Proof Protocol Authentication Process

## 本章小结

本章致力于深入介绍事件逻辑理论框架，重点关注基本建模理念、公理化体系构建以及安全协议的形式化描述等关键领域。在基本建模理论部分，我们将探索包括消息自动机、不可预测性原子元素、事件类别以及事件结构等概念的引入，利用这些基础理念对安全协议进行初步的框架搭建。接下来，公理系统部分着重介绍六项基本公理及其衍生的引理，这些构成了验证协议安全性的理论核心。在形式化定义环节，本章将对协议所需达成的身份验证属性进行详尽的形式化阐释。通过本章对事件逻辑理论的细致讲解，旨在为理论的进一步拓展和应用奠定坚实的理论基础。

# 事件逻辑理论的扩展

事件逻辑理论专注于通过对安全协议中诚实主体的交互行为进行形式化分析，以此描述协议及其安全特性。该理论的独特之处在于，它无需直接考虑恶意攻击者的行动模式，即可对协议的安全性提供深入的洞见。但是，现有的事件逻辑理论也存在着局限性，对于一些带有复杂加密算法体制的认证协议，事件逻辑理论无法做到对其进行形式化分析。随着大数据和物联网的不断发展，物联网所提供的信息交换和通信的优势愈加明显，其安全显得愈发重要。因此，需要对事件逻辑理论进行扩展，扩大其使用范围。

## 事件逻辑理论与其他形式化方法的对比

形式化方法对于提高开放环境下网络通信的安全具有重要推进作用，事件逻辑理论是形式化分析安全协议安全属性的有效手段之一。安全协议的形式化分析就是采用形式化语言的方法对协议运行的环境以及协议运行主体之间的交互动作和安全属性进行准确描述，验证协议是否能够满足预期的安全目标。

为了增强事件逻辑理论的应用广度，本研究首先通过与现有形式化方法的综合比较分析，凸显了事件逻辑理论在安全协议安全属性形式化分析方面的独特优势。此外，分析也明确指出了事件逻辑理论当前的局限性，标识出需要紧急解决以提升理论效能的关键领域。

（1）与模态逻辑对比

在采用BAN类逻辑进行安全协议的形式化分析前，必须设定一系列初始化假设，这些假设往往反映了分析者的主观预判且缺乏形式化基础。此过程中，分析的理想化阶段过分依赖于分析者的判断和经验，有时可能导致理想化处理后的协议与其原始形态之间存在显著偏差。相比之下，事件逻辑采用了基于精确数学规则的方法，通过一整套公理化的规则体系对协议施加形式化的约束，以此确保分析证明的严谨性和可靠性。

BAN逻辑在表达安全协议的信息内容和安全属性方面存在语义上的模糊性，这限制了其在精确刻画协议细节及分析结果准确性方面的能力。相反，事件逻辑理论以其精确无歧义的语义和结构清晰的特点，显著提升了安全协议证明过程的可靠性，从而增强了协议安全属性的可信度。

虽然BAN类逻辑的公理系统在数量和内容上比事件逻辑理论更为丰富，引入了多种谓词来细致区分协议主体的动作，但这两种逻辑方法都对分析者提出了较高的能力要求。尤其是在自动推理方面，两者仍存在一定的局限性，这一点在实际应用中需要得到进一步的关注和改进。

（2）与协议组合逻辑对比

协议组合逻辑和事件逻辑理论均基于一阶逻辑系统发展而来，包含了一系列用于证明安全协议的公理和规则。这两种方法有效地对安全协议中诚实主体的行为及多主体间的互动进行了精确的形式化描述，涵盖了消息操作和协议执行过程的输入输出。

尽管协议组合逻辑在描述包含数据签名操作的协议方面存在局限，事件逻辑理论通过引入因果公理解决了此类问题。它明确指出，任何验证事件之前，都必须有一个内容一致的签名事件发生，从而使事件逻辑理论能够有效分析携带数据签名的协议安全性。

此外，协议组合逻辑在描述动作先决条件方面的机制不如事件逻辑丰富，后者通过引入原子独立性规则来明确事件顺序和线程状态。虽然两种逻辑系统都规定了协议执行动作的先后顺序，但协议组合逻辑对动作顺序的定义更为严格和详尽。相对于事件逻辑，其严格性是一个优势，表明事件逻辑可以通过增加额外的谓词来补充对动作序列更精确的描述需求。

（3）与模型检测对比

模型检测方法以其能够识别安全协议潜在漏洞的能力而著称，主要通过对协议状态空间进行全面搜索，利用搜索算法寻找违反特定安全断言的路径，从而实现证伪过程。相反，事件逻辑的核心在于验证安全协议的安全属性，即通过逻辑证明过程来确认协议的安全性，而非指出具体的攻击路径。

在状态空间的处理上，模型检测方法要求协议系统模型具备有限状态空间特性，但协议主体数量的增加或运行条目的扩展往往导致状态空间迅速膨胀，形成所谓的“状态爆炸”问题。虽然通过优化算法可以在一定程度上缓解状态空间的扩张，这一挑战依旧存在。与之形成鲜明对比的是，事件逻辑理论对协议的状态空间没有具体要求，因此不受状态爆炸问题的影响。

从自动化程度来看，模型检测的一大优势在于其高度自动化的分析流程，研究人员通过使用模型检测工具对协议进行建模后，可以直接从模型检测器获得形式化验证的结果。而基于事件逻辑的安全协议分析依赖于研究者的专业知识与经验，需要手动进行分析与证明，这一过程更加依赖于人的参与。

## 对事件类的扩展

事件逻辑理论中，事件类描述的是协议中各诚实主体之间的交互动作，分别为挑战数的生成、消息的发送和接收、加密和解密事件以及签名与签名的验证，然而这七种事件类并不包含所有协议动作，如今的新兴协议中，协议参与者之间的行为更加多样化，加密机制愈发复杂，现有的事件逻辑理论不足以证明其安全属性。故针对基于ECC的RFID协议提出新的事件类、、，能够有效的对此类协议事件间的因果关系进行验证。其定义如下所示：

 （4-1）

如果存在一个事件满足，那么在事件中主体A对数据项进行椭圆曲线计算，并生成了认证消息，如果A是一个诚实主体，那么。如果存在一个事件满足，那么在事件中主体B成功对A生成的认证消息进行了还原并得到原始数据项，。如果存在一个事件，那么在事件中，主体进行了椭圆曲线标量乘计算并生成了一个公钥。

## 相关公理及规则的扩展

### 扩充谓词及其定义

在对相关的公理及规则进行扩展之前，首先引入谓词，，并分别给出对应的定义，以此来增强事件逻辑理论对事件顺序的推理能力，为后续对安全协议安全属性的形式化分析与认证提供方便。

谓词表示主体拥有原子，对于任意主体拥有原子，有以下几种情况：

（1）原子是由主体生成的；

（2）原子是由主体点乘计算生成的；

（3）原子是由主体明文接收的；

（4）原子是由主体密文接收的，且拥有解密密钥。

形式化定义如下：

 （4-2）

对任意发生在主体上的挑战数的生成事件，因为挑战数具有原子的不可猜测性，且其他诚实主体都未见过该挑战数，那么我们称挑战数在事件中是新鲜的，令，则新鲜性记为。如果在事件之后，包含原子的事件发生之前，所有的发送事件都不涉及到，则在事件中也是新鲜的，即有成立。新鲜性的形式化定义如下：

 （4-3）

对于任意发送事件，如果主体第一次发送数据是主体在事件发送消息时，其中可能是的子集，且，其他诚实主体在发送事件之前从未见过，那么事件是数据的首发事件，记作，形式化定义具体如下：

 （4-4）

因为诚实主体会严格的遵守协议规则，所以当存在诚实主体发送包含新鲜性数据子项时，那么该事件为首发事件，对谓词有以下推理规则：

 （4-5）

根据定义可知，其他诚实主体发生的任何与中的信息有关的事件均发生于之后，则有：

 （4-6）

其中，两条规则的诚实主体，不能是同一主体，即。

### 相关公理的扩展

、两个事件类引入后，需要对因果公理进行扩展。规定复原事件前序存在与它对应的计算事件，二者信息相同且椭圆曲线会话密钥相等。如下所示为复原公理的定义。

 （4-7）

引入事件类后，需要定义相关规则方便后续协议的证明。首先，主体进行标量乘计算时，生成了主体的公钥和私钥，如下所示：

 （4-8）

当主体进行标量乘计算并把产生的公钥发送，则存在一个主体接受到消息，获得了主体的公钥，并且无法通过计算得到的私钥，如下式所示：

 （4-9）

当主体存在标量乘事件，并生成，则此事件保留的新鲜度，或者在事件发生之后，包含的事件发生之前，所有发送事件都不包含，那我们认为事件保留了的新鲜度，如Rule3所示：

 （4-10）

在事件逻辑理论中，流关系公理中存在着对协议动作的描述，既然本文对事件类进行了扩展，相应的流关系公理也要进行扩展。

（4-11）

在流关系公理体系内，的定义主要聚焦于协议动作的描述，而未对传递信息的具体内容做出细致区分。在安全协议的证明实践中，若能够细化并区分协议动作中信息的具体内容，并引入额外的规则，便能更加精确地验证事件间的因果联系。基于此，对定义的扩展提出了以下新规则：

 （4-12）

在的基本定义之上，引入了信息组的拆分与合并功能，以及信息元组的概念，极大地简化了信息发送与接收的过程。此外，通过下述公式，引入了在持有特定密钥的前提下对信息执行加密与解密操作的能力，这一改进明显增强了信息处理的灵活性和可读性，使得已有的信息能够被更加有效地利用。

 （4-13）

## 机密性系统的建立

认证性和机密性构成了安全协议设计的两大核心属性。特别地，机密性强调协议内部数据的保密性，确保敏感信息不会被非授权主体获取。例如，在安全协议中生成并加密新的挑战数后发送时，该挑战数理应保持机密，因为只有持有相应解密密钥的授权主体能够访问该数据。在实际协议交互中，参与主体通常会接收加密消息，并发送出经过另一密钥加密的消息片段。鉴于协议的异步执行特性及潜在的不诚实参与者，确保即便在多步操作后，加密消息仍然对攻击者不可见，显得尤为关键。本节在弱化了完美密码假设的前提下，通过引入归纳机密规则，扩展LoET所能证明的安全属性范畴。

### 机密性基础概念

第一步引入谓词，假设消息中存在机密信息，则消息中出现的每一个机密信息都受集合中的密钥保护，即，且的类型为，不以事件类的形式引入。

引入谓词后，接着引入两个类型同样为的相关概念与。前者表示为主体在线程上发送的机密信息都是安全的，并由集合中的密钥保护；后者表示为在协议中所有发送事件中的机密信息都是安全的，且受集合中的密钥保护。

通过引入以上新概念，可以得到如下公理。

 （4-14）

是指如果存在某个消息使为假，并且存在消息使得为真，那么可以得到消息和是两个不同的消息；是指如果存在一个消息集合使得为真，则可以得到两个消息子集都为真，即和都为真，且这两个公式具有等价性，互为充分必要条件，可以相互推导；和类似，表示如果存在一个消息由加密事件或者计算事件所加密，并使为真，则可以推出为真且；表示如果消息由一个标量乘事件所加密，使得为真，则可以得到。

### 机密性核心公理及推理规则

在进行安全协议的机密性验证过程中，确保所有生成机密信息以及访问对应密钥的关键事件仅在诚实主体的控制之下进行是至关重要的。这是因为，如果这些包含敏感操作的事件被不诚实的主体执行，机密信息及密钥的泄露将成为不可避免的后果，这种泄露对于数据的整体机密性将造成重大且不可逆的影响。因此，从设计之初，就需要确保安全协议具备足够的机制来预防这类风险，保障机密数据的安全性。所以假设事件主体是诚实的，引入新的诚实规则，定义如下式所示。

 （4-15）

在安全协议的分析中，和分别代表密钥集和机密信息的诚实性规则，这两条规则构成了分析的基础。其核心假设是，所有关于生成机密信息和访问密钥的关键事件，必须是由诚实的主体执行的。这意味着，只有被认定为信任的实体才被允许生成新的机密信息或访问现有的密钥，以此确保整个系统的安全性。综合这两个规则的应用，可以形成以下统一的表述：

 （4-16）

安全协议执行过程中涉及消息的发送、接收及各类操作，因此，引入先行项成为确保执行过程中机密性的关键。先行项的应用旨在验证通过安全网络接收到的消息保持其安全性。具体来说，代表在协议中，如果某主体的所有发送事件均在密钥集的子集保护下并共享相同的安全属性，则无论该主体经历何种事件，其所有后续的发送事件中的机密消息均保持安全。该逻辑可通过下述公式表示：

 （4-17）

指的是假设协议中某主体发起的所有发送事件均由密钥集合的一个子集所保护，并且这些事件共享相似的安全特性。根据此公理，当该协议主体通过接收事件接收到消息后，消息内部包含的每个机密元素必须都由密钥集中的密钥加以保护。

 （4-18）

设定在安全协议的环境下，若存在一个主体，其所有通过发送事件传递的消息均为安全，则即便该主体执行了发送事件以外的其他任何事件，其在发送事件中传递的消息安全性依然得到保持。此公理强调了消息安全性在协议操作中的持续性，确保信息保护机制在协议的各种操作下仍然有效。

 （4-19）

定义了在安全协议环境中，如果某主体在其发送事件中的所有消息均已确保为安全，并且在该主体执行一个发送事件，从而发送出消息后，能够继续保证消息中包含的每个机密信息均受到密钥集的一个子集的保护，那么就可以得出一个结论：该主体发起的包括此次在内的所有后续发送事件中传递的消息同样保持安全。这一公理强调了安全消息在连续发送事件中保护的持久性，确立了一个保护机制，以维护信息在传递过程中的机密性。

 （4-20）

在安全协议分析中，主体的基本序列排序依据该主体上事件的时间分区来定义。因此，如果一个基本序列包含接收事件，该事件仅位于序列的开头部分。这一定义及排序机制关键于证明从安全网络中接收到的消息的安全性。一旦接收消息的安全性得到证明，便可以进一步利用至来验证发送出的消息同样保持安全性。

初始时，谓词被选定用以表征消息的机密性。在成功证明接收和发送事件中消息的安全性之后，引入新的规则来进行协议整体机密性的进一步推理和分析变得必要。据此，我们提出以下公理作为基础，以支持对协议整体机密性的推理分析：

 （4-21）

阐述了在保护机密信息和密钥集的安全网络环境下，能够接触到非安全消息的仅可能是信息的生成者或是密钥集中密钥的持有者。此处，谓词用以标明信息的机密性状态。

基于该公理，进一步可以推导出两项规则，具体如下：

 （4-22）

这条规则指出，如果协议中的所有发送事件都通过密钥集中的一个子集保护，并且这些发送事件共享相同的安全属性，那么当协议中的某个主体执行接收事件并成功接收到消息时，可以确信消息中所有的机密信息也都受到了密钥集中某个子集的保护。这意味着机密信息在传输过程中保持了其机密性，不会被未经授权的第三方获取。

与类似，但是将关注点从发送事件转移到了接收事件。这条规则说明，如果协议中的接收事件能保证接收到的消息中的机密信息受到密钥集中一个子集的保护，则协议能确保信息的安全性。这种情形通常适用于协议中需要验证接收到的消息是否为安全传输的场景。

这两条规则共同强调了在安全协议设计中，确保机密信息在传输过程中通过适当的密钥进行保护的重要性。通过应用这些规则，设计者可以评估和验证安全协议是否能有效地保护机密信息，防止信息在传输过程中被泄露或篡改，从而确保通信双方的数据交换既安全又可靠。如下式所示。

 （4-23）

## 本章小结

目前物联网发展迅猛，所提供的信息交换和通信的优势愈加明显，其安全显得愈发重要。为了对新兴协议进行安全属性的分析，需要对事件逻辑理论进行补充和完善，扩大其使用范围。

本章首先将事件逻辑理论与其他形式化方法进行对比，突出事件逻辑理论在形式化分析安全协议安全属性上存在的优势，分析事件逻辑理论中存在的不足，然后对事件逻辑理论进行扩展。首先对事件类进行扩展，添加三种新的协议动作，分别为、、；根据新扩展的事件类对相关公理和规则进行扩展，并引入谓词，增强事件逻辑理论对事件顺序的推理能力，为后续对安全协议安全属性的形式化分析与认证提供方便。并且在弱化了完美密码假设的前提下，通过引入归纳机密规则，扩展LoET所能证明的安全属性范畴。

# ECC-based RFID双向认证协议的形式化分析

在ECC-based RFID双向认证协议中，参与主体被明确定义为认证方和被认证方。这里，后台服务器承担认证方的角色，而电子标签则是被认证方。为了有效避免碰撞攻击的风险，协议设计首先对被认证方即电子标签的身份进行验证，随后才验证认证方服务器的身份真实性。本章将采用扩展的事件逻辑理论对该ECC基于的RFID双向认证协议进行形式化分析，旨在证实其安全性。

## 协议形式化分析

LoET是基于进程演算的形式化方法，用于分析和验证安全协议。该方法的核心步骤包括定义协议中各个角色的进程，并对基本序列中的会话消息进行匹配分析。通过比较主体之间发送和接收的消息内容是否一致，以及评估这些动作的时序关系，LoET能够有效地揭示协议的操作逻辑和潜在的安全缺陷。进一步地，LoET利用定理来明确协议需要满足的强认证属性，这些定理反映了协议设计的安全目标和预期行为。

在研究基于ECC的RFID双向认证协议前，面临一个关键的挑战： LoET的基本建模理论并没有直接提供适用于形式化描述ECC功能的工具。因此，为了使ECC的特定功能能够在LoET框架下进行有效分析，首要步骤是对ECC实现的功能进行抽象化处理。这一抽象化过程旨在简化ECC的复杂性，将其安全性原理转化为可通过LoET分析的形式。如图5-1所示，为实现ECC在RFID双向认证协议中安全机制的关键。



图5-1 ECC实现原理

Fig.5-1 ECC implementation principle

ECC-based RFID协议安全性的实现主要是通过两个步骤实现。其中第一个步骤，响应者即后台服务器完成了对标签的身份认证因子的编码，得到如下公式。

 （5-1）

第二个步骤，发起者即标签通过解码还原出身份认证因子并与自身的身份认证因子进行比较，完成了对服务器的认证，得到如下公式。

 （5-2）

通过对ECC功能的抽象化处理，我们可以利用事件逻辑理论来对具体的ECC-based RFID双向认证协议进行详细描述。这一过程首先涉及定义两个关键进程：Initiator（认证服务器）和Responder（标签主体），它们分别代表协议交互的两方。在协议交互过程中，Initiator和Responder通过一系列的交互步骤实现认证，这些步骤被抽象化为基本序列，对于Initiator来说，其基本序列可表示为；而对于Responder则为。这些基本序列包含了双方进行交互所需执行的具体动作和消息传递，有效地描述了双向认证过程的每一个关键步骤，基于事件逻辑的协议描述如图5-2所示。



图5-2 双向认证中交互信息的描述

Fig.5-2 Description of Interactive Information in Mutual Authentication

通过事件逻辑理论来定义协议需要满足的身份认证性质，验证基于ECC-based RFID双向认证协议的认证性，首先需要协议的基础序列进行排序。定义基于ECC-based RFID协议为。



图5-3 双向认证协议基本序列

Fig.5-3 Basic Sequence of Mutual Authentication Protocol

从对上述协议基本序列的分析中可以看出，为了满足协议中的强认证性， Initiator必须与Responder进行两次消息发送与接收动作的交互。这意味着，存在长度为2的匹配会话，即两个步骤的通信序列，确保了双方能够有效地进行身份验证和确认。该性质刻画为。

 （5-3）

相应的Responder需满足的强认证性为。由此得出，在协议的安全性证明中，需要满足的强身份认证性质为：

 （5-4）

## ECC-based RFID双向认证协议认证性证明

### 证明过程

第一步先对进行证明，假设诚实主体（后面分别使用，指代），和共享公钥和标签认证信息，由于诚实主体双方都遵循ECC-based RFID双向认证协议规则，所以、的参与协议运行的任意线程都是SP的基本序列实例。令是基本序列的一个实例，则存在事件序，由于的主体为，那么对于事件的主体也为，则对于类型参数，的事件序列实例为：

 （5-5）

由计算公理和诚实公理公理可知，对于复原事件，协议中的某个线程中必定存在计算事件，且使成立。由于遵循基于ECC的RFID双向认证协议，所以事件一定为双向认证协议基本序列中的实例成员。在协议所有基本序列中包含计算动作的有。由于是以当前发生的事件为基准，所以对一切未发生的事件不纳入考虑范围之内，所以排除。假设为序列线程中的事件，那么对于类型，在主体上存在事件组成的事件序列为：

 （5-6）

通过上式，发现可以满足下式：

 （5-7）

则可知有，并且由于，则有：

 （5-8）

可得出：

 （5-9）

根据以上证明结果，可以得到：

 （5-10）

即和构成两个完整的事件，此时可以得到一个长度为2的弱匹配会话。

接着分析它们是否为强匹配会话，即分析会话事件是否满足时间事件序。在已经规定主体的情况下，根据的定义，可以得到：

 （5-11）

由此可以证明是在事件中第一次发送的。

 （5-12）

由可知，包含的所有操作都必须在事件之后发生，包括事件。因此，根据LoET中的诚实公理，可以得到事件顺序。同理，可分析出。

所以，通过以上分析可得知主体认证线程在主体存在与之强匹配会话，即得证。

### 证明过程

下一步对进行证明，令是基本序列的一个实例，定义为线程的事件，基本序列中事件发生主体为被认证方主体，则对于一些类型参数有：

 （5-13）

由解密公理和诚实公理公理可知，存在与解密事件匹配的加密事件，且满足。由于诚实主体遵循ECC-based RFID双向认证协议，所以事件一定是该双向认证协议基本序列中的实例成员。在协议所有基本序列中包含加密动作的是。假设为中的事件，那么对于类型的，则线程中存在组成的事件序列如下：

 （5-14）

通过上式，发现可以满足：

 （5-15）

并且由于，根据公理，则有：

 （5-16）

通过上式可以得到，并可以得到以下公式：

 （5-17）

得出一个匹配会话：。

又因为线程中存在复原事件，根据和公理，存在满足：，因此需要进行新一轮的协议交互分析。若事件存在，那么必定为基于ECC的RFID双向认证协议基本序列中的某一个实例成员。假设为协议实例的计算事件，其中包含计算动作的有，与上节分析类似，对于未发生事件将其排除在外，也就得出中存在一个基本序列包含事件。

假设是线程在上的实例计算事件，对于，主体发生事件，则：

 （5-18）

从上述对事件的描述可以发现满足：

 （5-19）

通过以上公式可得出线程实例中计算事件与线程复原事件满足匹配，则：

 （5-20）

由此可以得到：

 （5-21）

根据以上证明结果，可以得到：

 （5-22）

对于诚实主体的任意线程，诚实主体存在一个消息数为2的线程与之形成弱匹配会话。下一步证明它们是否为强匹配会话，即证明。在已经规定主体的情况下，根据的定义，可以得到：

 （5-23）

然后证明是在事件中第一次发送的。

 （5-24）

由可知，包含的所有操作都必须在事件之后发生，包括事件。因此，根据事件逻辑理论中的诚实公理，可以得到事件顺序。同理，可以分析得出。

综上所述，可知主体任意线程，在主体中存在两个交互完整的强匹配会话，即得证。最终ECC-based RFID双向认证协议满足双向强认证性，表示为得到完整性证明。因此，通过详细的分析和验证，可以确定在协议的执行过程中，消息重放攻击的风险被有效排除，从而确保了协议安全性的充分证明。

## ECC-based RFID双向认证协议机密性证明

由ECC-based RFID双向认证协议的基本序列可知，在中主体还没有执行发送事件发送消息之前，主体与主体都遵循诚实公理，那么在协议中挑战数都是两个主体之间的机密信息，要想证明挑战数的机密性，那么则需要证明以下式子能够成立：

 （5-25）

在对序列中发送事件之前的基本序列进行详尽分析后，可以归纳得到以下数学公式：

 （5-26）

上式的成立是因为从协议发起者主体的角度出发，主体生成了挑战数，并且使用椭圆曲线加密发送出去。而且，发送的消息为保持信息在传递过程中的一致性遵循特定格式发送，如果其中信息进行了更改，则无法确定通信双方的身份。

 （5-27）

由于在协议分析的初始阶段设定了特定的支撑条件，我们可以确定公式也成立。这意味着，在线程中的发送事件执行之前，主体尚未执行该发送事件，且两个主体均遵循诚实公理。因此，中考虑的状态是主体还未发送最终消息的情景。一旦发送信息后，主体便能确定主体的身份。

 （5-28）

上式表明，如果在协议的执行过程中，一个诚实的主体完成了最终步骤的发送事件，那么可以推断，在此之前，该主体要么生成了一个挑战数，要么接收到了包含挑战数的信息。

 （5-29）

上式表明，某一主体的信息经过加密后被发送，那么我们可以确信，该主体既是加密事件的执行者，也是发送事件的执行者。

在ECC-based RFID协议的执行过程中，由于指定的密钥集为主体和主体的密钥，所以可以使得公式成立。并且，由于主体生成了挑战数，那么公式也成立。所以能够表明协议基本序列中发送的消息是安全的，假设上述四个公式成立，则成立于基本序列的开始，对于所有的基本序列，结合机密性证明推理可得到：

 （5-30）

则挑战数的机密性得证。

## 本章小结

在本章中，通过扩展的事件逻辑理论，对ECC-based RFID双向认证协议进行了深入的形式化验证，证明了该协议的认证性和机密性。首先，将ECC的功能进行了抽象和形式化的描述，确保其能够适应事件逻辑框架进行分析。随后，通过精细地分析协议双方的交互过程，详尽地阐述了认证流程，并定义了协议执行的基本序列，从而实现对该ECC基于的RFID双向认证协议形式化建模。通过这一过程，确定了需要验证的关键认证属性，目的是证明认证协议的安全性。

经过严格的分析和验证，最终结果表明，基于ECC的RFID双向认证协议确实满足了强认证属性。这意味着，在所有基础假设被满足的前提下，该协议被证明为安全的，并且能够有效抵御重放攻击等潜在威胁。这一发现为该类认证协议的应用提供了强有力的安全保障，证明了其在保护信息交换安全中的有效性。

# 总结与展望

至此，本文有关的形式化分析研究结束，本章总结以上研究工作，并展望未来的研究方向。

## 总结

射频识别技术（RFID）是物联网（LoT）的重要组成部分，提高RFID系统的安全性是亟需解决的问题。而保障通信系统的安全性与系统所使用的安全协议息息相关，如果安全协议的安全属性没有得到严格的证明，则增加了网络通信中的风险。形式化方法是分析与验证安全协议最强有力的手段之一。事件逻辑理论（LoET）作为一种分布式系统安全性描述的形式化方法，提供了对安全协议基本原语的形式化规范，并通过对协议的强认证性质进行证明，进而验证协议的安全属性。

本文通过对事件逻辑理论的创新性扩展，成功将其应用于基于ECC的RFID这一类协议的形式化分析与验证中，使扩展后的事件逻辑理论适用于带有复杂加密算法协议的安全性分析。本文的主要研究内容如下：

（1）详细介绍事件逻辑基本理论，给出事件逻辑基本定义，包括基本建模理论，公理系统以及协议的形式化描述。引入扩充谓词和以及相应的推理规则，增强其在协议分析中的实用性，特别是在处理消息的新鲜性和识别发送事件的首发性方面，有助于确保协议证明过程中事件类和基本序列的一致性，同时提高了事件排序的能力并降低了协议分析的复杂度。

（2）将事件逻辑与其他形式化方法进行比较，分析事件逻辑对于其他方法的优势与不足。对事件逻辑理论进行扩展，提出三个新事件类、、并给出相应的定义。根据新的事件类，扩展因果公理，定义新的因果关系。对其他相关公理及规则进行扩展，使得扩展后的事件逻辑理论能够分析带有复杂加密算法的协议。建立机密性系统，引入归纳机密规则，扩展LoET所能证明的安全属性范畴。

（3）利用扩展后的事件逻辑理论，深入形式化分析一个ECC-based RFID双向认证协议。首先对ECC会话密钥的生成过程进行形式化抽象描述，定义协议进程和基本序列用于描述协议，对协议所需满足的强认证属性进行了严格的形式化定义，通过理论推导，证明协议在合理假设下满足双向强认证性质，表明扩展的事件逻辑理论可以证明ECC-based RFID这一类带有复杂加密算法协议的安全属性，扩展了事件逻辑理论的使用范围。

## 展望

形式化方法作为安全协议研究的关键路径，已经由国内外的专家学者通过深入研究取得了显著成就。本文通过对事件逻辑理论的扩展，对ECC-based RFID双向认证协议的安全性进行了详尽分析，尽管取得了一定的进展，但仍有若干领域需要进一步探索和完善。未来的研究可能会聚焦于以下几个方向：

（1）尽管扩展后的事件逻辑理论已经能够处理基于ECC的RFID协议，但面对包含更复杂加密机制的协议时，其适用性还待提高。未来的工作应致力于将这一理论应用到更广泛的密码协议分析中。

（2）目前，事件逻辑理论在安全协议的分析和证明过程中依赖于研究人员的手动操作，这限制了分析的自动化程度和效率。因此，开发一个能够实现安全协议自动化证明的验证系统，将是提高效率的重要方向。

（3）虽然目前的理论框架主要集中于验证安全协议主体的身份认证性，但安全属性的范畴远不止于此。因此，对事件逻辑理论的进一步扩充和完善，以包括更多安全属性的分析，是未来研究的重要内容。

# 参考文献

1. Han Shen et al. Efficient RFID Authentication Using Elliptic Curve Cryptography for the Internet of Things[J]. Wireless Personal Communications, 2017, 96(4): 5253-5266.
2. Al-Fuqaha A, Guizani M, Mohammadi M, et al. Internet of Things: A Survey on Enabling Technologies, Protocols and Applications[J]. IEEE Communications Surveys & Tutorials, 2015, 17(4): Fourthquarter 2015.
3. 甘勇,许允倩,贺蕾等.RFID系统的安全及隐私综述[J].网络安全技术与应用,2015(12):69-71.
4. 宁焕生.RFID重大工程与国家物联网[M].机械工业出版社:201008.240.
5. 葛云峰.基于RFID的轻量级安全认证协议的文献综述[J].网络安全技术与应用,2020(08):19-22.
6. Burmester M, De Medeiros B, Motta R. Robust, anonymous RFID authentication with constant key-lookup[C]//Proceedings of the 2008 ACM symposium on Information, computer and communications security. 2008: 283-291.
7. Menezes A J, Van Oorschot P C, Vanstone S A. Handbook of applied cryptography[M]. CRC press, 2018.
8. Sidhu D P, Leung T K. Formal methods for protocol testing: a detailed study[J]. IEEE Transactions on Software Engineering, 1989, 15(4): P.413-426.
9. Maggi P, Sisto R. Using SPIN to Verify Security Properties of Cryptographic Protocols[M]// Model Checking Software. Springer Berlin Heidelberg, 2002.
10. Chagrov A, Zakharyaschev M. Modal Logic[J]. Philosophical Review, 1997, 109(2):286-289.
11. F. Javier Thayer Fábrega. Strand spaces: proving security protocols correct[J]. Journal of Computer Security, 1999, 7(2-3):191-230.
12. Bickford M, Constable R L. A logic of events. Cornell University, 2003.
13. Xiao M, Bickford M. Logic of Events for Proving Security Properties of Protocols[C]// International Conference on Web Information Systems & Mining. IEEE Computer Society, 2009.
14. Meihua X, Chenglin M, Chunyan D , et al.A Novel Approach to Automatic Security Protocol Analysis Based on Authentication Event Logic[J].Chinese Journal of Electronics,2015,24(01):187-192.
15. 钟小妹, 肖美华, 杨科, 罗运先. 基于事件逻辑的PUFs认证协议形式化分析[J/OL]. 华中科技大学学报(自然科学版): 1-8[2023-02-26]. DOI: 10.13245/j.hust.240209.
16. 肖美华, 李娅楠, 宋佳雯, 王西忠, 李伟, 钟小妹. 基于事件逻辑的WMN客户端与LTCA认证协议安全性分析[J]. 计算机研究与发展, 2019, 56(06): 1275-1289.
17. Zhong X, Xiao M, Zhang T, et al. Proving mutual authentication property of rcia protocol in rfid based on logic of events[J]. Chinese Journal of Electronics, 2022, 31(1): 79-88.
18. Xiao, M.; Chen, Q.; Li, Z.; Chen, Y.; Xu, R. Formal Security Analysis of ECC-Based RFID in Logic of Events Theory. Electronics 2023, 12, 3286.https://doi.org/10.3390/electronics12153286
19. Xiao, M.; Chen, Y.; Li, Z.; Chen, Q.; Xu, R. Proving Mutual Authentication Property of Industrial Internet of Things Multi-Factor Authentication Protocol Based on Logic of Events. Electronics 2024, 13, 177. https://doi.org/10.3390/electronics13010177
20. Tuyls P, Batina L. RFID-tags for anti-counterfeiting[C]//Topics in Cryptology–CT-RSA 2006: The Cryptographers’ Track at the RSA Conference 2006, San Jose, CA, USA, February 13-17, 2005. Proceedings. Springer Berlin Heidelberg, 2006: 115-131.
21. BATINA L, GUAJARDO J, KERINS T, et al. Public-Key Cryptography for RFID-Tags[C]//Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (Per Com W’07). 2007: 217-222.
22. 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. 2008.
23. BRINGER J, CHABANNE H, ICART T. Cryptanalysis of EC-RAC, a RFID Identification Protocol[C]//FRANKLIN M K, HUI L C K, WONG D S. Cryptology and Network Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008: 149-161.
24. MARTÍNEZ S, VALLS M, ROIG C, et al. A Secure Elliptic Curve-Based RFID Protocol[J]. Journal of Computer Science & Technology, 2009(02): 131-140.
25. GÓDOR G, IMRE S. Elliptic curve cryptography based authentication protocol for low-cost RFID tags[C]//IEEE International Conference on Rfid-technologies & Applications. 2011.
26. Zhang X, Li L, Wu Y, et al. An ECDLP-based randomized key RFID authentication protocol[C]//2011 international conference on network computing and information security. IEEE, 2011, 2: 146-149.
27. Liao Y P, Hsiao C M. A secure ECC-based RFID authentication scheme using hybrid protocols[C]//Advances in Intelligent Systems and Applications-Volume 2: Proceedings of the International Computer Symposium ICS 2012 Held at Hualien, Taiwan, December 12–14, 2012. Springer Berlin Heidelberg, 2013: 1-13.
28. Alamr A A, Kausar F, Kim J S. Secure mutual authentication protocol for RFID based on elliptic curve cryptography[C]//2016 International Conference on Platform Technology and Service (PlatCon). IEEE, 2016: 1-7.
29. Dinarvand N, Barati H. An efficient and secure RFID authentication protocol using elliptic curve cryptography[J]. Wireless Networks, 2019, 25(1): 415-428.
30. Liao Y P, Hsiao C M. A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol[J]. Ad hoc networks, 2014, 18: 133-146.
31. Qian Q, Jia Y L, Zhang R. A Lightweight RFID Security Protocol Based on Elliptic Curve Crytography[J]. Int. J. Netw. Secur., 2016, 18(2): 354-361.
32. Kumar S, Banka H, Kaushik B, et al. A review and analysis of secure and lightweight ECC‐based RFID authentication protocol for Internet of Vehicles[J]. Transactions on Emerging Telecommunications Technologies, 2021, 32(11): e4354.
33. 薛跳跳.基于ECC的RFID认证协议的形式化安全分析[D].西安电子科技大学,2021.DOI: 10.27389/d.cnki.gxadu.2021.003599.
34. Gabsi S, Kortli Y, Beroulle V, et al. Novel ECC-based RFID mutual authentication protocol for emerging IoT applications[J]. IEEE access, 2021, 9: 130895-130913.
35. 贺嘉琦, 彭长根, 付章杰等.面向RFID的轻量级双向认证协议[J].计算机工程与应用,2023,59(18):268-277.
36. ATZORI L, IERA A, MORABITO G. The Internet of Things: A Survey[J]. Computer Networks, 2010: 2787-2805.
37. Koblitz N. Elliptic Curve Cryptosystems[J]. Mathematics of Computation, 1987, 48(177): 203-209.
38. 张利华,沈友进.基于ECC和指纹USBKey的身份认证协议[J].华东交通大学学报,2014,31(02):95-98. DOI:10.16749/j.cnki.jecjtu.2014.02.018.
39. 魏国珩,秦艳琳,张焕国.基于ECC的轻量级射频识别安全认证协议[J].华中科技大学学报(自然科学版),2018,46(01):49-52.
40. 王戟, 詹乃军, 冯新宇, et al. 形式化方法概貌[J]. 软件学报, 2019, 30(01):36-64.
41. Li, Yahui, et al. A Survey on Network Verification and Testing with Formal Methods: Approaches and Challenges[C]// IEEE Communications Surveys & Tutorials, 2018.
42. 刘欣倩.基于事件逻辑的可证明网络安全协议形式化分析[D].华东交通大学,2016.
43. 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 研 究 生 院 学报,2003(04):389-406.
44. Handbook of model checking[M]. Cham: Springer, 2018.
45. 肖美华,周浩洋,朱志亮,等.基于模型检测的区块链智能合约公平性形式化验证[J].华东交通大学学报,2021,38(03):52-60.DOI:10.16749/j.cnki.jecjtu.20210706.009.
46. Gibson-Robinson T, Broadfoot G, Carvalho G, et al. FDR: from theory to industrial application[J]. Concurrency, Security, and Puzzles: Essays Dedicated to Andrew William Roscoe on the Occasion of His 60th Birthday, 2017: 65-87.
47. Gibson-Robinson T, Armstrong P, Boulgakov A, et al. FDR3: a parallel refinement checker for CSP[J]. International Journal on Software Tools for Technology Transfer, 2016, 18: 149-167.
48. Hoare C A R. Communicating sequential processes[J]. Communications of the ACM, 1978, 21(8): 666-677.
49. BURROWS M, ABADI M, NEEDHAM R. A Logic of Authentication[J]. ACM Trans. Comput. Syst., New York, NY, USA: Association for Computing Machinery, 1990, 8(1): 18-36.
50. Dolev D, Yao A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2):198-208.
51. Dill D L. The Murϕ verification system[C]//Computer Aided Verification: 8th International Conference, CAV'96 New Brunswick, NJ, USA, July 31–August 3, 1996 Proceedings 8. Springer Berlin Heidelberg, 1996: 390-393.
52. Mitchell J C, Mitchell M, Stern U. Automated analysis of cryptographic protocols using mur/spl phi[C]//Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097). IEEE, 1997: 141-151.
53. Holzmann G J. The model checker SPIN[J]. IEEE Transactions on software engineering, 1997, 23(5): 279-295.
54. 杨科,肖美华,钟小妹,占东明.时序逻辑及其表达能力综述[J].华东交通大学学报,2023,40(02):57-70. DOI: 10.16749/j.cnki.jecjtu.20230330.015.
55. Burrows M, Abadi M, Needham R M. A logic of authentication[J]. Acm Transactions on Computer Systems, 1989, 23(5):1-13.
56. Gong L, Needham R, Yahalom R. Reasoning about belief in cryptographic protocols[C]// Research in Security and Privacy, 1990. Proceedings. 1990 IEEE Computer Society Symposium on. IEEE, 1990.
57. Abadi M, Tuttle M R. A semantics for a logic of authentication[C]//Proceedings of the tenth annual ACM symposium on Principles of distributed computing. 1991: 201-216.
58. Van Oorschot P. Extending cryptographic logics of belief to key agreement protocols[C]Proceedings of the 1st ACM Conference on Computer and Communications Security. ACM, 1993: 232-243.
59. Syverson P F, Van Oorschot P C. On unifying some cryptographic protocol logics[C]//Proceedings of 1994 IEEE Computer Society Symposium on Research in Security and Privacy. IEEE, 1994: 14-28.
60. Kailar R. Reasoning about accountability in protocols for electronic commerce[C]//Proceedings 1995 IEEE Symposium on Security and Privacy. IEEE, 1995: 236-250.
61. Paulson L C. The inductive approach to verifying cryptographic protocols[J]. Journal of computer security, 1998, 6(1-2): 85-128.
62. Thayer Fanrega F J, Herzog J C, Guttman J D.Strand space: why is a security protocol correct[C]// Proceedings of the1998 IEEE Symposium on Security and Privacy.Piscataway: IEEE, 1998:160-171.
63. Datta A, Derek A, Mitchell J C, et al. Protocol composition logic (PCL)[J]. Electronic Notes in Theoretical Computer Science, 2007, 172: 311-358.
64. Song J, Xiao M, Zhang T, et al. Proving authentication property of PUF-based mutual authentication protocol based on logic of events[J]. Soft Computing, 2022, 26(2): 841-852.
65. Song J, Xiao M, Yang K, et al. LoET-E: A refined theory for proving security properties of cryptographic protocols[J]. IEEE Access, 2019, 7: 59871-59883.

# 个人简介 在读期间发表学术论文

**个人简历：**

**陈全刚**，男，1999年2月生。

2021年7月毕业于山东理工大学计算机科学与技术学院软件工程专业，获学士学位。

2021年9月入华东交通大学读硕士研究生。

**论文：**

1. Xiao, M.; **Chen, Q.**; Li, Z.; Chen, Y.; Xu, R. Formal Security Analysis of ECC-Based RFID in Logic of Events Theory. Electronics 2023, 12, 3286. https://doi.org/10.3390/electronics12153286
2. Xiao, M.; Chen, Y.; Li, Z.; **Chen, Q.**; Xu, R. Proving Mutual Authentication Property of Industrial Internet of Things Multi-Factor Authentication Protocol Based on Logic of Events. Electronics 2024, 13, 177. https://doi.org/10.3390/electronics13010177

**其他成果：**

[1] 软件开发信息化管理系统V1.0，软件著作权

[2] 网络协议参数配置系统V1.0，软件著作权

**参与项目：**

[1] 基于事件逻辑理论的安全协议实施安全性形式化分析与验证，国家自然科学基金(62362033)

[2] 基于事件逻辑的云计算环境下数据完整性验证模型及协议研究，国家自然科学基金(61962020)

[3] 基于事件逻辑理论的安全协议实施安全性形式化分析若干关键技术研究, 江西省“双千”人才项目(JXSQ2023201009)

# 致谢

光阴似箭，日月如梭，转瞬之间，三年研究生生涯即将结束。回忆在校园度过的每个日夜，感慨良多，收获丰厚。三年的读研生活，有成功的喜悦、有精彩的故事、也有失败、挫折的痛苦，无论如何，这将促使我继续前行。在此感谢读研期间老师对我的谆谆教诲，家人默默无闻的支持以及师兄弟之间的互相帮助。

首先，我要感谢我的导师肖美华教授，在肖老师的悉心栽培和指导下，才有了今天的我。在学习上，他教会我如何做科研、撰写论文、做演讲，增强我的学习能力；在生活上，他更加关心我们的日常生活，也会让我们多运动锻炼身体，同时注重对我们的道德品行上的教育，注重德智体全面发展；当我在生活和研究中遇到困惑时，他会化身为慈爱的长者，耐心地指导我、帮助我。肖老师高尚的人格、宽广的胸怀使我受益终生。他不仅教会了我专业知识和科研技能，更教会了我人生的学问和做人的道理。

感谢父母和家人们。你们呵护我的成长，无私奉献、对我毫无保留的支持，鼓励我追求更高的学术理想。

感谢305、307实验室的各位师兄师姐以及师弟师妹们，在实验室里的生活有了你们的帮助和支持，使得我在研究生阶段能够过得充实并且丰富多彩，也希望我们在未来的日子里能更上一层楼！

最后，向参加论文评审、答辩以及提出宝贵意见的各位老师、专家们表示衷心的感谢，愿您们工作顺利、幸福安康！