基于PQ-ECIES的蔬菜物联网区块链防伪追溯系统

齐培杨[1,2], 孙传恒[2], 谭昌伟[3], 王 俊[4], 罗 娜[2], 邢 斌[2*]

(1. 上海海洋大学信息学院, 上海 201306,中国; 2. 国家农业信息化工程技术研究中心,北京 100097,中国;
3. 扬州大学农学院,江苏扬州 225009,中国; 4. 江苏立卓信息技术有限公司,江苏常州 213000,中国)

摘 要: [**目的/意义**]蔬菜供应链具有生产主体类别多、产品品种多、流通环节复杂等特点,针对传统追溯过程中数据采集准确率低、追溯标签易伪造、数据易篡改、供应链信息断链等问题,通过分析蔬菜生产、加工、储运、销售等流程,利用蓝牙、区块链、物联网等手段,创建数据可信共享、全链溯源区块链平台。[**方法**]集成气象站、农残检测仪、标签打印机等物联网设备,通过硬件标识与企业主体绑定机制建立设备-主体可信映射;融合椭圆曲线综合加密方案与后量子密码中的Kyber算法,研发抗量子混合加密方案,实现物联网数据量子安全加密,阻断伪造篡改行为。在此基础上研发基于物联网和区块链的蔬菜防伪追溯系统并进行实验测试,对信息采集准确率、数据上链、数据查询进行了测试分析。[**结果和讨论**]实验结果表明,物联网方式能够提高数据录入的准确率,数据上传至蔬菜防伪溯源区块链系统时延为2 879 ms,查询数据时延为122 ms。蔬菜供应链后量子增强型椭圆曲线综合加密方案对128 B明文的加密与解密时间总开销为10~30 ms,相比于传统加密方法RSA非对称加密的50~80 ms表现出较高效率,相较于对称加密的高级加密标准时间开销大,但抗量子安全性高。[**结论**]系统的数据上链和数据查询效率较高,可以满足系统的应用需求,能够有效解决传统追溯存在的漏填或错填追溯信息、追溯数据造假等问题,实现蔬菜的可信溯源。

关键词: 物联网;区块链;蔬菜溯源系统;防伪追溯;后量子加密;供应链

中图分类号: S126;TP311 **文献标识码:** A **文章编号:** SA202507019

引用格式:齐培杨, 孙传恒, 谭昌伟, 王俊, 罗娜, 邢斌. 基于PQ-ECIES的蔬菜物联网区块链防伪追溯系统[J]. 智慧农业(中英文), 2026, 8(2): 237-250. DOI: 10.12133/j.smartag.SA202507019

QI Peiyang, SUN Chuanheng, TAN Changwei, WANG Jun, LUO Na, XING Bin. Vegetable IoT Blockchain Anti Counterfeiting Traceability System Based on PQ-ECIES[J]. Smart Agriculture, 2026, 8(2): 237-250. DOI: 10.12133/j.smartag.SA202507019 (in Chinese with English abstract)

0 引 言

蔬菜作为人们生活中必不可缺少的食物,是人类食谱中的重要组成部分[1]。随着人民生活水平的提高,对蔬菜的品质和质量安全要求也不断提升[2]。然而,蔬菜生产销售过程中违规用药、过量施药和不严格执行农药安全间隔期等现象屡禁不止,导致蔬菜质量安全问题不断发生[3]。蔬菜质量安全涉及生产、加工、物流、销售主体、政府监管部门和消费者[4],因此,需要建立能够覆盖全供应链流程且数据真实可信的追溯系统来保障蔬菜的质量安全[5,6]。

20世纪90年代国外率先开始了农产品追溯领域的研究,中国针对农产品追溯系统的研究始于2002年,林建材[7]开展了烟台苹果质量安全监管和追溯系统的研究和应用。随着信息技术的不断发展,溯源系统在农产品质量安全管理上的应用也逐渐深入,形成了企业主导、政府主导、第三方主导等多种农产品追溯模式。在现有技术中,首先是中心化数据库系统,如基于条码电子秤的追溯系统,张继恩[8]基于商品条码建立了食品冷链物流追溯系统,这种系统依赖人工录入,存在数据孤岛和篡改风险。其次是区块链基础模型,如熊盼和黄小燕[9]通过区块链节点授权保护方法构建果业供应链信息保护模型,解决了水果供应链追溯过程中隐

收稿日期:2025-07-11
基金项目:江苏省科技计划(重点研发计划现代农业)项目(BE2023315)
作者简介:齐培杨,硕士研究生,研究方向为农业信息化技术研究。E-mail:2556382216@qq.com
*通信作者:邢 斌,硕士,副研究员,研究方向为农业信息化技术研究。E-mail:xingb@nercita.org.cn

私数据泄露问题；张净等[10]针对农产品追溯系统研究融合区块链多链架构与星际文件系统（Inter-Planetary File System, IPFS）存储技术，结合椭圆曲线加密（Elliptic Curve Cryptography, ECC）算法构建支持隐私保护的多链分布式追溯系统，该方法通过分布式账本解决篡改问题。追溯系统在实际应用过程中需要重点解决数据采集准确度低[11]、人为干预操作失误与自动化设备伪造风险并存等问题[12]。在追溯信息隐私与透明方面，需要协调全流程知情权与企业商业秘密保护的冲突[13-15]。当前蔬菜追溯系统普遍依赖ECC/RSA（Rivest-Shamir-Adleman）等传统加密算法，而量子计算的发展如Shor算法可在多项式时间内破解像离散对数或者大数分解等数学基础问题[16, 17]，从而使隐私信息有被攻击破解的风险。

针对上述问题，提出基于物联网与区块链协同的蔬菜防伪追溯系统，以蔬菜全供应链为对象，集成气象站、视频监控设备、虫情灯、农残检测仪、农事采集App、蔬菜信息条码打印机、物流检测设备、仓储检测设备，以及智能电子秤等9类物联网设备，结合Hyperledger Fabric联盟链平台设计系统，实现从生产到销售的全环节可信溯源，并基于四大环节中的物联网设备设计溯源ID，确保物联网设备信息与各批货物紧密关联。将生产商、加工商、储运商、销售商各环节和物联网设备通过数字加字母映射的形式进行编码，确保每批次蔬菜溯源码的唯一性。核心创新在于优化椭圆曲线集成加密方案（Elliptic Curve Integrated Encryption Scheme, ECIES）算法在蔬菜溯源场景的应用，通过密钥派生简化曲线优选，将加解密时延压缩至10 ms内来解决效率与安全问题，并且引入美国国家标准与技术研究院（National Institute of Standards and Technology, NIST）标准算法中的模块误差学习（Model Learning with Error, MLWE）算法CRYSTALS-Kyber，有效抵御量子计算对传统ECC的威胁，如Shor算法破解椭圆曲线离散对数问题，并且通过双共享密钥机制椭圆曲线密钥加Kyber封装密钥实现双重安全保障，以此来解决后量子密码安全问题。

1 蔬菜供应链物联网架构

1.1 技术简介

1.1.1 物联网技术

物联网是通过信息传感设备，按照约定的协议，将任何物体与网络相连接，物体通过信息传播媒介进行信息交换和通信，实现智能化识别、定位、跟踪、监管等功能[18]。物联网技术在蔬菜生产监测、质量检测、产后处理与追溯等方面提供了技术支撑[19, 20]，大大降低信息采集的成本[21, 22]。通过分析蔬菜供应链各环节所需采集和溯源的信息，结合供应链各环节主体信息化管理和蔬菜质量安全需求，确定所需要的物联网设备、采集方式、采集数据和用途。

1.1.2 区块链技术

区块链技术是一种分布式账本架构，其核心在于数据的去中心化存储、不可篡改性和透明性。这一技术通过数据加密和共识机制确保数据安全，同时智能合约的引入为自动化交易提供了可能。区块链可以划分为公有链、私有链和联盟链三种类型，在这三种类型中，联盟链更适合作为蔬菜供应链溯源的技术背景[23]。郭浩[24]阐述了太原市农产品供应链追溯系统，涵盖大数据、物联网、云平台与二维码等关键技术，然而无法保证数据不被篡改。因此使用区块链系统保证数据完整性和安全性，通过区块链本身的不可篡改性保证数据从采集到上链存储的整个流程中不被篡改。

1.1.3 隐私加密技术

隐私加密是通过技术手段将敏感信息转化为密文，防止未经授权的访问或泄露。常见方法包括对称加密，如对称加密的高级加密标准（Advanced Encryption Standard, AES）和非对称加密，如RSA，广泛应用于数据传输、设备存储等领域，是保障个人隐私与数据安全的核心技术。孙传恒等[25]提出了一个面向果蔬全供应链的区块链多链模型，使用的加密算法是ECC，然而该算法在抵御量子攻击时显得较为脆弱，因此通过ECIES中引入Kyber提供的后量子安全层抵御未来量子计算攻击，同时保证高效密钥管理，通过后量子增强型椭圆曲线集成加密方案（Post-Quantum Enhanced ECIES, PQ-ECIES）的双共享密钥机制，各方仅需维护一对长期ECC密钥，Kyber的密钥封装机制（Key Encapsulation Mechanism, KEM）简化会话密钥分发，在复杂的多企业供应链环境中，简化密钥的生成、分发、存储和更新流程，降低管理负担和安全风险。

1.2 设备总体架构

应用物联网技术搭建蔬菜追溯系统的硬件架构，将农药残留检测仪、条码标签打印设备、视频监控、虫情灯、环境信息采集和产后物联网设备等

与网络相连接，通过信息交换和通信，实现追溯信息的设备识别、信息采集与关联。蔬菜追溯物联网设备架构如图1所示。

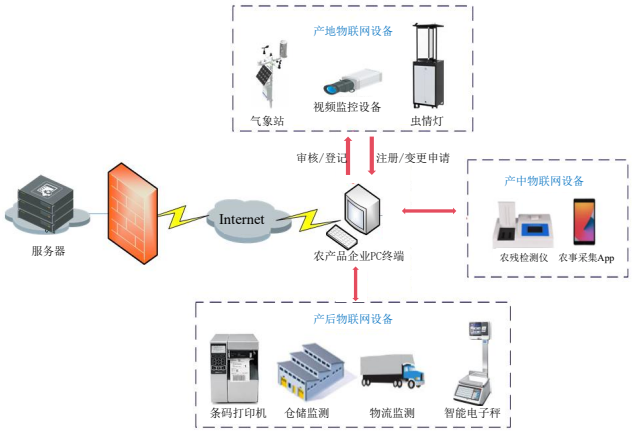


图1　追溯全流程的物联网设备架构

Fig. 1　The architecture of IoT devices throughout the entire tracing process

1.3　设备绑定与准入验证机制

钱建平等[26]改进了蔬菜追溯系统，通过自动获取快速检测设备如农残检测仪的实时数据，避免手工录入误差与篡改风险，实现了检测信息与生产批次的精准关联，但是无法保证数据源认证与防伪。本研究设计物联网设备绑定和准入验证机制，防止非授权设备或非认证企业冒用合法身份上传伪造的追溯数据。

蔬菜供应链企业将所要应用在追溯系统中的硬件设备进行线上注册，提交设备ID、设备名称、类型、版本号、设备序列号，企业地理区域范围等数据，平台监管用户对企业提交信息的真实性、完整性、准确性进行审核，审核成功后将设备信息进行登记，绑定设备与企业信息。注册成功后从该设备所采集到的数据将被认定为绑定企业上传。如果设备与企业的信息发生变化，则供应链企业可提出变更申请，并按照上述流程进行绑定。

针对农残检测仪、追溯标签打印机等与农产品质量安全相关的重要设备，设计了设备验证准入机制，主要流程如下：第一步研发设备验证移动App，将设备内置蓝牙通信模块，通过移动App与蓝牙建立连接。连接成功后，进行第二步开发App自动定位功能模块，确定设备的地理位置。第三步为验证位置，应用蓝牙通信距离短的特点，如果能进行数据交互则认为设备与App属于同一地理位置。第四步为接入许可和数据传输，如果设备地理位置、ID与企业设备登记时的注册信息一致则认定为合法设备，可以应用该设备，进行设备接口调用，数据采集和传输，否则将无法进行数据交互，通过上述方法能够避免设备被非法企业盗用。

1.4　数据处理与上链流程

物联网设备如气象站、视频监控设备、虫情灯等会持续产生大量数据。这些数据中可能包含格式错误、不一致或重复的信息，需要进行处理以保证数据的质量。

在设备布置妥当并且绑定设备后，当用户应用物联网设备采集供应链各环节追溯数据时，将设备ID与蔬菜批次相关联，记录设备对所关联批次蔬菜的处理数据。物联网设备数据通过有线网络、Wi-Fi、4G等方式上传。服务器端采用socket通信、多线程监听、异步数据处理方式，对设备进行状态监测、数据感知。将数据上传至服务器进行解析和处理，根据设备ID、地理位置、绑定信息对设备进行合法性认证，认证成功后将处理后的数据进行上链存储。具体流程如图2所示。

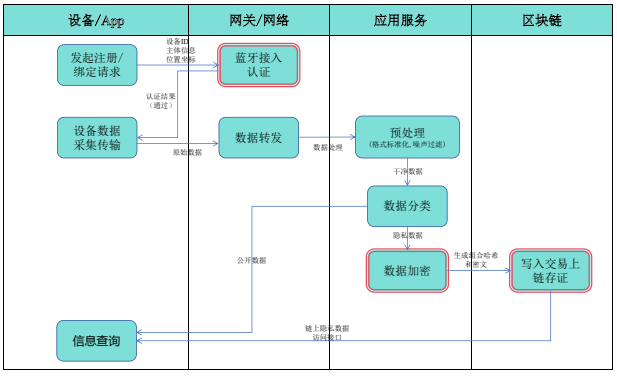


图2　设备验证准入到上链的数据处理流程

Fig. 2　Data processing workflow for device verification and admission to the blockchain

2　关键模型与方法设计

2.1　数据隐私性分析

物联网通过传感器实时监测环境条件和物流状态，确保蔬菜从田间到餐桌的全过程可追溯，通过位置定位、App权限控制可实现异地设备无法上传信息，非供应链认证企业无权上传信息，从而提升蔬菜供应链中物联网设备数据采集的真实性。在蔬菜溯源防伪区块链中，四情物联设备、农残检测仪、农事采集App、条码打印机、仓储检测设备、物流检测设备、智能电子秤设备在上传数据过程中

将数据分为公开信息和隐私信息。公开信息包括产品信息、检测结果、物流状态等，而加密的隐私信息包括用户身份、内部追溯信息和企业商业秘密，通过区块链技术得到严格保护，确保数据安全和隐私权益[27,28]。在蔬菜溯源防伪区块链中，消费者可以清晰查询蔬菜从生产、加工、运输、销售等环节信息，增强信息透明度，提升蔬菜产品信任度。隐私信息经过数据加密上传至区块链网络中，确保数据敏感性。监管机构和相关蔬菜供应链组织节点通过加密授权可以获得相关隐私数据的明文，消费者无法获取隐私信息明文，从而提高蔬菜供应链运行效率。物联网设备上传区块链信息如表1所示。

表 1 蔬菜产中与产后物联网设备采集信息

Table 1 Information collection via IoT devices during and post-vegetable production

供应链阶段	物联网设备	公开信息	隐私信息
产中	四情物联设备	蔬菜货物溯源ID、土壤湿度、气候数据、虫害发生情况	农户的具体位置、个人联系方式、四情物联设备ID
	农残检测仪	蔬菜货物溯源ID、检测时间、检测结果	生产者的身份信息、具体的种植地点、农残检测值、农残检测仪识别ID
	农事采集App	蔬菜货物溯源ID、作物生长周期、施肥、灌溉的时间	农户的操作记录、个人农事安排、农事采集设备ID
产后	条码打印机	蔬菜货物溯源ID、产品的追溯码、生产日期	生产批次、生产者信息、条码打印机设备ID
	仓储检测	蔬菜货物溯源ID、仓储公司、仓库温湿度、产品存储量	仓库位置、管理人员信息、仓储传感器设备ID
	物流检测	蔬菜货物溯源ID、运输路线、货物状态、运输公司信息	司机信息、运输公司内部数据、物流传感器设备ID
	智能电子秤	蔬菜货物溯源ID、称重数据、计量时间	交易双方的信息、价格谈判数据、智能电子秤设备ID

2.2 蔬菜供应链隐私数据加密方法

当前主流蔬菜追溯系统，如孙传恒等[29]的牡蛎供应链溯源方法，其数据安全保障普遍依赖于传统的非对称加密算法，如RSA、基础ECC或对称加密如AES。这些方案在特定场景下存在一些显著挑战，RSA算法在处理物联网设备高频产生的小数据包时，其较大的计算开销和较长的密钥导致加解密延迟较高，难以满足如农残检测结果实时上链、物流状态快速更新等蔬菜流通环节对实时性的要求。更关键的是，基于大整数分解RSA或椭圆曲线离散对数ECC的传统非对称算法，面临着量子计算如Shor算法的潜在威胁[30,31]。一旦实用化量子计算机出现，现有系统的长期数据机密性将面临严峻挑战。因此，亟须一种针对蔬菜溯源场景优化的加密方案，它需要高效率适应物联网设备和实时业务；加强安全性以抵御当前和未来的计算威胁，特别是量子计算；支持非对称特性以实现安全的密钥分发和身份认证；易于集成到去中心化的区块链架构中。

将后量子密码算法基于代数格的密码kyber（Cryptographic Suite for Algebraic Lattices kyber, CRYSTALS-Kyber）与ECIES结合，构建抗量子攻击的混合加密方案[32]。基于ECC非对称加密、Kyber后量子加密、对称加密和密钥派生算法，采用PQ-ECIES实现蔬菜供应链隐私数据防伪功能。ECIES及PQ-ECIES在蔬菜供应链区块链中的核心优势如下：采用“ECC密钥协商+对称加密”混合模式，加解密速度快约10 ms，适合资源受限的IoT设备和高频数据上链；相同安全强度下，ECC密钥远短于RSA，节省存储与带宽，适合农业物联网环境；密文自包含，可直接作为交易上链，接收方用私钥即可解密，无需额外交互；结合Kyber后量子算法，抵御未来量子攻击，保障溯源数据长期机密；双密钥机制（ECC+ Kyber KEM），各方只需维护ECC密钥，会话密钥动态分发，适合多方协作；虽引入抗量子能力，总耗时仍远低于RSA，略高于AES，整体性能满足实际业务需求。

蔬菜供应链隐私数据访问者提出隐私数据访问请求，数据拥有者通过数据访问者公钥确认身份并决定使用数据拥有者公钥加密对称密钥，将加密对称密钥和加密密文封装。蔬菜供应链隐私数据访问者通过解封装获得加密密文和加密的对称密钥，通过自身私钥解密，获得蔬菜供应链隐私数据的对称密钥，通过对称密钥解密蔬菜供应链物联网设备采集隐私数据。PQ-ECIES加密与解密流程如图3和图4所示，具体伪代码演示由表2和表3所示。

本研究使用的PQ-ECIES混合加密基于secp256k1椭圆曲线公钥加密体系和Kyber-512后量子加密算法，其中secp256k1椭圆曲线公钥加密计

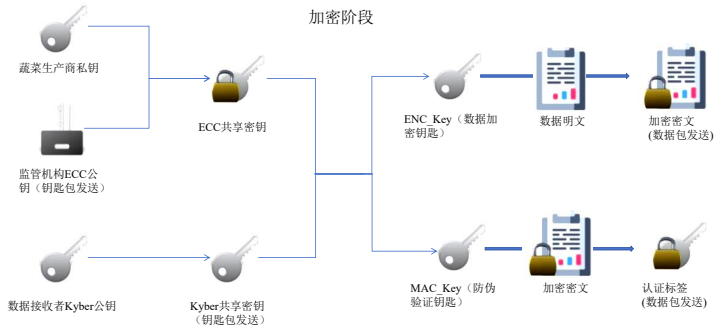


图 3　PQ-ECIES 加密

Fig. 3　PQ-ECIES encryption

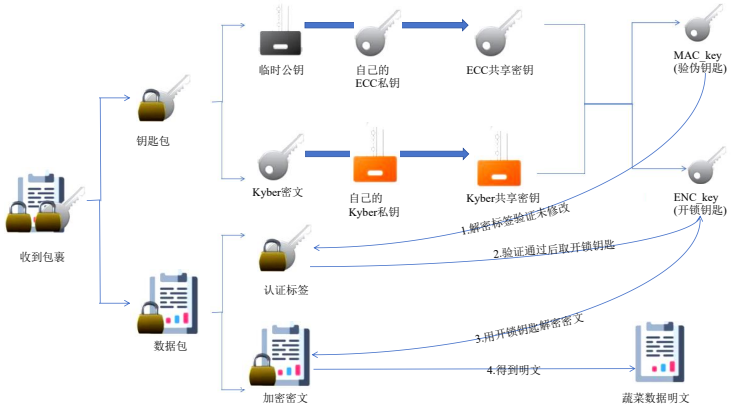


图 4　PQ-ECIES 解密

Fig. 4　PQ-ECIES decryption

表 2　PQ-ECIES 加密步骤伪代码

Table 2　Pseudocode for the encryption steps of PQ-ECIES

Algorithm 1：加密步骤算法
Input：PrivacyData，(ReceiverPublicKey，ReceiverKyberPublicKey)　//隐私数据，数据接收者双重公钥
Output：Complete ciphertext　　//完整密文
1：/*步骤 1：生成发件人的临时密钥*/
2：SenderTemporaryPrivateKey ← Random()　　// 生成临时随机私钥
3：SenderTemporaryPublicKey ← SenderTemporaryPrivateKey × G　// 计算椭圆曲线公钥
4：SenderTemporaryKyberPublicKey ← Kyber.KeyGen()　　// 生成 kyber 临时公钥
5：/* 步骤 2：计算共享密钥 */
6：EllipticCurveSharedSecret ← SenderTemporaryPrivateKey × ReceiverPublicKey // 椭圆曲线共享密钥
7：(KyberCiphertext，KyberSharedSecret) ← Kyber.Encapsulation(ReceiverKyberPublicKey) // Kyber 共享密钥
8：/*步骤 3：派生联合密钥 */
9：CombinedSecret ← SHA3-256(EllipticCurveSharedSecret // KyberSharedSecret) // 合并共享密钥并哈希
10：EncryptionKey ← KDF(CombinedSecret，"ENC")　　// 密钥派生函数(Key Derivation Function，KDF())，AES-GCM 是 高级加密标准(AES)的一种工作模式，全称是 Galois/Counter Mode
11：MessageAuthenticationKey ← KDF(CombinedSecret，"MAC") //派生消息认证码(Message Authentication Code，MAC)认证密钥
12：/* 步骤 4：加密隐私数据 */
13：Ciphertext ← AES-GCM-Encrypt(EncryptionKey，PrivacyData) // 使用 AES-GCM 加密数据
14：AuthenticationTag ← HMAC-SHA256(MessageAuthenticationKey，Ciphertext) //生成完整性认证标签，基于散列的消息认证码-安全哈希算法(Hash-based Message Authentication Code-Secure Hash Algorithm，HMAC-SHA)
15：/*　步骤 5：封装完整密文 */
16：CompleteCiphertext ← SenderTemporaryPublicKey // SenderTemporaryKyberPublicKey //
17：KyberCiphertext // Ciphertext // AuthenticationTag　　// 拼接完整密文作为最终输出

表3 PQ-ECIES解密步骤伪代码

Table 3 Pseudocode for the decryption steps of PQ-ECIES

Algorithm 2：解密步骤算法

```
Input：CompleteCiphertext，（ReceiverPrivateKey，ReceiverKyberPrivateKey）      //完整密文，数据接收者双重私钥
Output：Decryptedprivacydata          // 隐私数据
1：/* 步骤 1：解析密文结构 */
2：[SenderTemporaryPublicKey，SenderTemporaryKyberPublicKey，
3：KyberCiphertext，Ciphertext，AuthenticationTag] ← CompleteCiphertext // 拆分完整密文
4：/* 步骤 2：计算共享密钥 */
5：EllipticCurveSharedSecret ← ReceiverPrivateKey × SenderTemporaryPublicKey // ECC 椭圆曲线共享密钥
6：KyberSharedSecret ← Kyber.Decapsulation（KyberCiphertext，ReceiverKyberPrivateKey）// Kyber 共享密钥
7：/* 步骤 3：重建联合密钥 */
8：CombinedSecret ← SHA3-256（EllipticCurveSharedSecret ∥ KyberSharedSecret）// 合并共享密钥并哈希
9：EncryptionKey ← KDF（CombinedSecret，"ENC"）       // 重建 AES-GCM 解密密钥
10：MessageAuthenticationKey ← KDF（CombinedSecret，"MAC"）// 重建 MAC 认证密钥
11：/* 步骤 4：验证完整性 */
12：CalculatedTag ← HMAC-SHA256（MessageAuthenticationKey，Ciphertext）// 计算认证标签
13：if CalculatedTag ≠ AuthenticationTag then
14：Reject the ciphertext                    // 验证失败，拒绝解密，数据已被篡改
15：end if
16：/* 步骤 5：解密隐私数据 */
17：DecryptedPrivacyData ← AES-GCM-Decrypt（EncryptionKey，Ciphertext）// 还原原始隐私数据
```

算如公式（1）所示。

$$y^2=x^3+7 \quad (1)$$

式中：x和y分别为坐标系内椭圆曲线上的点坐标的横纵坐标值。

PQ-ECIES基于secp256k1椭圆曲线与Kyber-512算法，其设计遵循以下科学原则，首先是双密钥封装机制KEM与混合加密，采用“KEM+DEM”的混合结构。利用ECC密钥协商与Kyber密钥封装并行生成两个独立的共享密钥EllipticCurve-SharedSecret和KyberSharedSecret。随后，通过cryptographic hash函数SHA3-256将二者混合派生出一个高强度的联合主密钥CombinedSecret。此设计确保了最终会话密钥的安全性同时依赖于ECC和Kyber两个数学难题，即使其中一个在未来被破解，整体系统依然安全。

其次是实现密钥派生与功能分离，使用密钥派生函数KDF并附加不同标签如“ENC”和“MAC”，从同一主密钥CombinedSecret中安全地派生出用于数据加密的对称密钥EncryptionKey和用于消息认证的密钥MessageAuthenticationKey。这实现了密钥的细分和隔离，符合cryptographic best practices。

最后是保证机密性与完整性统一，使用高效的对称加密算法如AES-GCM，在加密数据的同时生成认证标签，确保了传输过程中数据的机密性和完整性，能有效防止密文被篡改。

本研究提出的抗量子混合加密方案（PQ-Hybrid-ECIES），融合椭圆曲线密码学与后量子密码算法Kyber，在保障数据安全性的同时实现了三个改进：首先是抗量子攻击保障，通过Kyber算法抵御量子计算威胁，符合NIST L3安全标准；其次是密钥管理优化，双密码体制下各参与方仅需维护一对公私钥，大幅简化密钥分发与存储流程；最后平衡了效率与安全，在以ARM Cortex-M4为微处理器内核的物联网设备实测中，完整加密延迟11.3 ms，满足蔬菜流通实时性需求。

2.3 蔬菜供应链防伪溯源模型

蔬菜防伪追溯系统整体架构设计主要分为以下几个关键层次：物联网可信感知层、数据处理层、区块链分布式信任层、PQ-ECIES量子安全层、智能合约逻辑层、应用层、安全与隐私保护机制、管理与决策支持层。物联网可信感知层（IoT Trusted Perception Layer），不仅指硬件设备传感器、检测仪，更涵盖“设备-主体-数据”三元绑定体系与动态验证机制蓝牙定位与ID认证，确保数据采集源头可信，从物理世界阻断伪造与篡改。关键在于将设备身份与企业主体、地理空间强关联，形成防伪第一道防线。在蔬菜生产、加工、储运、销售等环节部署各类物联网设备，负责实时监测和收集关键

信息，为追溯系统提供原始数据支撑。数据处理层将收集到的原始数据经过预处理以确保数据质量。选择具有模块化、可插拔的架构，支持不同组件的灵活部署，以及强大的隐私保护机制。

PQ-ECIES量子安全层（PQ-ECIES Quantum-Safe Layer），不仅是加密算法，更是“动态双盾防护体系”，ECC高效密钥协商满足实时性，Kyber抗量子封装应对量子算法威胁，提供终身级数据机密性，并通过非对称特性实现细粒度访问控制监管可解密，消费者不可见。其关键在于双重密钥机制，使企业仅需维护1对长期ECC密钥，大幅简化管理。

区块链分布式信任层（Blockchain Distributed Trust Layer），形成“不可篡改账本”，实现“流程确权+分级透明”。通过Fabric通道与智能合约，约束各环节企业仅能写入权限内数据，如加工商无权修改生产数据。公开数据检测结果、物流状态全网可查；隐私数据企业机密、位置经PQ-ECIES加密后上链，哈希存证公开数据，降低存储压力+防篡改，建立跨企业协作信任基座，解决信息孤岛，实现数据全程可审计。

智能合约逻辑层（Smart Contract Logic Layer），作为业务规则与信任规则的执行引擎，自动触发数据分类（公开/隐私）、数据上链、PQ-ECIES加密/解密验证、权限校验如QueryPrivacyData（）仅授权节点可调用，每个合约都包含了详细的业务逻辑，将人工流程编码为可信代码，降低人为干预风险，提升系统的自动化与合规性，以确保数据的准确性和安全性。

应用层提供用户界面和访问接口，使消费者、监管机构等能够查询和验证蔬菜的溯源信息。应用层还负责与区块链平台交互，调用智能合约，实现数据的查询和展示。此外，还采用了数据访问权限机制，确保只有授权用户才能访问敏感信息。监管机构和供应链组织节点可以通过区块链网络获取相关隐私数据的明文，而消费者无法获取隐私信息明文。这提高了蔬菜供应链运行效率，提升了监管质量。

在蔬菜防伪区块链网络中，供应链的所有数据来源都通过相对应的物联网采集设备进行数据采集[33]，采集后的蔬菜数据通过相对应的逻辑智能合约进行数据分类，将关键溯源数据进行区块链上链存储，从源头开始确保蔬菜防伪溯源数据的真实有效性。根据蔬菜供应链环节分为蔬菜生产企业、蔬菜加工企业、运输企业、仓储企业、销售企业，所有供应链中的参与方均拥有一对ECC公私钥，以作为确定各个供应链参与方身份的有效标识，以及供应链各企业间隐私数据的安全访问，蔬菜防伪溯源系统模型如图5所示。

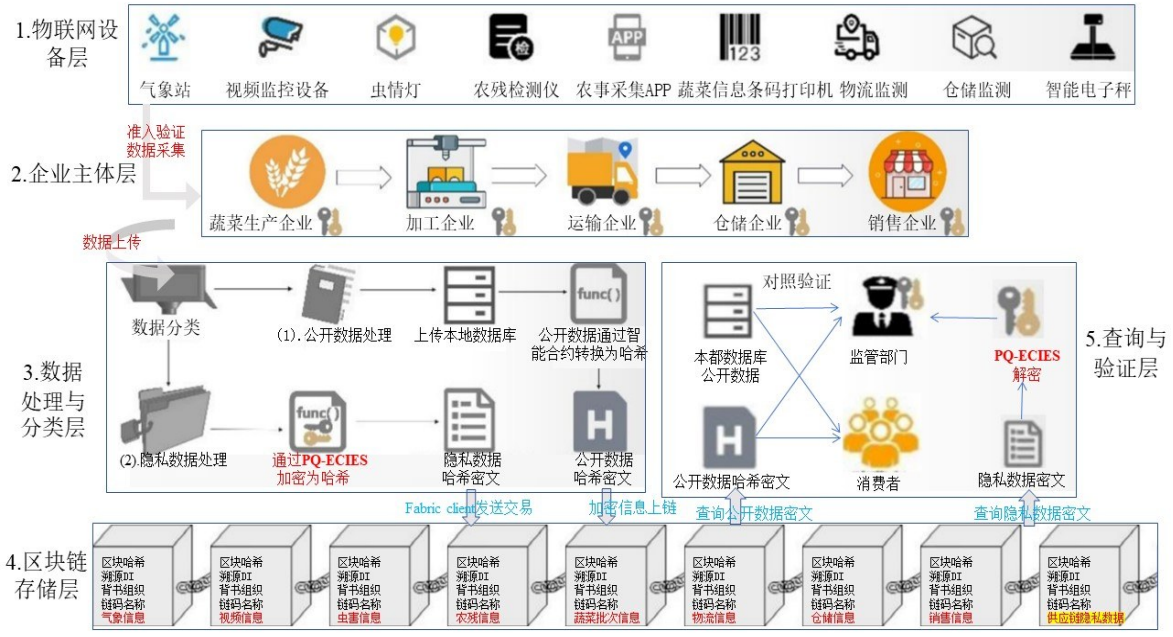


图5　蔬菜防伪溯源系统模型

Fig. 5　Vegetable anti-counterfeiting traceability system model

供应链中所有终端环节都配备相应的物联网设备，在对应供应链的终端进行数据的收集工作。同时，供应链中每个参与方都拥有ECC公私钥对，实时收集成功的数据经过分类后得到隐私数据和公开数据两种数据类型。

基于Hyperledger Fabric区块链平台构建蔬菜供应链溯源系统，将供应链划分为生产商、加工商、储运商和经销商四大环节，并设立包含监管机构的7个联盟组织。通过非对称密钥实现企业身份验证公钥上链，设置分级数据权限写入记账权限与隐私读取限制。种植环节利用物联网设备实时监测土壤墒情、苗情、虫情、灾情等关键数据，结合农事采集App和检测仪器将生产信息上链；加工商通过区块链获取原料溯源信息并关联加工批次。各节点通过共识机制实现数据确权与全网存证，确保供应链数据不可篡改。

各环节蔬菜供应链信息上传区块链前将通过数据分类实现了数据细粒度管理，隐私数据经过PQ-ECIES加密后生成对应密文，在区块链网络中仅存储隐私数据的密文，需要对隐私数据进行查询，须通过对应密钥解密之后才可以得到对应隐私数据内容；公开数据首先存入对应参与方的数据库中，同时将公开数据进行哈希转换，并将转换后的哈希值存入区块链网络中，在降低区块链网络存储压力的同时，利用哈希值转换不可逆性的特点，确保蔬菜消费者，以及相关用户能够得到真实可信的溯源数据。

区块链不是独立的系统，而是作为“分布式信任与不可篡改”的核心模块嵌入蔬菜防伪溯源系统的中间层，承担数据确权、存证、共享和访问控制的职能。平台采用Fabric SDK（Go语言）调用智能合约，内置Fabric Client，负责向区块链网络发送交易请求。

首先是底层数据来源，IoT设备采集数据后，通过数据处理层进行合法性校验与分类。其次是上链环节，处理后的数据分为公开数据和隐私数据，公开数据直接上链存证，隐私数据在PQ-ECIES量子安全层完成加密后再上链。最后是链上执行，与Peer节点交互，执行共识，完成数据上链，以及监听链码事件例如“数据写入成功”等。区块链通过智能合约完成业务逻辑，例如数据写入UploadProductionData（）、UploadStorageData（），权限校验QueryPrivacyData（）仅授权机构可调用，数据完整性验证哈希校验，防止篡改等。最后由应用层访问，消费者、监管机构、企业通过智能合约接口进行查询，链上公开数据全网可查，隐私数据需密钥解密。

区块链的模型定位是在系统架构中，位于数据处理层与应用层之间，与PQ-ECIES加密模块协同，构建“可信分布式账本+隐私保护”的双保险机制。嵌入区块链后，系统流程发生了两大变化，首先由集中式转为分布式，传统数据库存储转变为联盟链结构，每个企业节点维护账本副本，消除数据孤岛。其次实现业务逻辑智能化，人工审核或中心化平台逻辑由智能合约替代，实现“自动验真、防伪校验、权限验证”。

嵌入区块链技术对本研究的三个核心概念（可信性、隐私性、协同性）有深刻影响：

1）对“可信性”的影响。在传统问题中，中心化存储可被篡改，消费者和监管机构无法验证数据真实性。区块链的不可篡改性和多节点共识机制，使每一条数据具备可验证的真实性，形成全链溯源信任闭环，提高消费者信任和监管效率。

2）对“隐私性”的影响。公开上链会泄露企业商业机密，完全隐藏又无法实现透明。区块链通过智能合约结合PQ-ECIES，实现分级可见+权限控制：消费者仅查看公开数据（检测结果、物流状态）监管机构通过密钥授权查看隐私数据（产地位置、批次信息），这平衡了“透明度”和“隐私保护”之间的矛盾。

3）对“协同性”的影响。跨企业数据协作依赖第三方平台，存在数据孤岛和信任风险。区块链引入联盟链+Fabric通道技术，实现跨企业的数据隔离与选择性共享，提升供应链协作效率，并保证参与方数据安全。

本模型关注蔬菜供应链当前的较大问题，提供可参考方案。首先是源头防伪成本高，本研究提出物联网设备绑定机制，通过蓝牙动态验证如图2所示，替代高成本物理防伪标签，降低企业设备管理成本。其次是跨企业数据协作难，提出区块链分级透明架构，通过Fabric通道实现数据隔离与选择性共享如加工商仅见生产商公开数据，打破信息壁垒，提升供应链协同效率，传统中心化平台接入时间一般为周级，本系统接入时间为分钟级。接着是隐私与监管冲突，提出PQ-ECIES细粒度控制，消费者可查公开溯源信息哈希保障真实，监管机构可通过密钥解密全量数据，平衡商业保密与政府监督。最后是未来安全投资风险，提出后量子平滑升

级，PQ-ECIES兼容NIST标准，企业无需重构系统即可抵御量子威胁，保护相关信息安全。

3　系统实现与测试分析

3.1 运行环境

Hyperledger Fabric因其模块化、可插拔的架构和对隐私保护的支持而被选为本研究的区块链平台。相比于其他联盟链框架，如Ethereum的Quorum或R3 Corda，Fabric提供了更好的隐私保护机制，通过通道（channels）功能实现数据隔离，这对于蔬菜防伪追溯场景中保护供应链各方的敏感信息至关重要。基于Hyperledger Fabric 1.4.4搭建区块链网络，使用Raft共识机制决定该区块链网络的排序节点，设置7个联盟组织作为企业，分别为Org1（生产商组织）、Org2（加工商组织）、Org3（运输组织）、Org4（仓储组织）、Org5（销售商组织）、Org6（消费者溯源组织）和Org7（监管部门），每个组织部门创建了两个节点peer0和peer1作为实例完成相关部门的具体工作，共14个节点在链上存储蔬菜溯源数据，采用状态数据库CouchDB存储所有上链数据，通过key-value键值检索状态数据库查询相应数据。使用的虚拟机系统版本为Ubuntu 16.04 LTS。性能测试将链码通过balance-transfer接口进行封装，使用接口测试工具Postman进行测试。硬件配置为：4 GB内存、8核处理器、50 GB硬盘。使用的区块链的共识机制为Raft，出块时间为2 s，区块最大交易数量为99，区块最大容量为99 MB，每条交易最大占存储空间为512 KB。在主机配置为4.60 GHz、i5-12400F CPU、32 GB RAM、系统为Windows 10下进行实验，实验架构如图6所示。

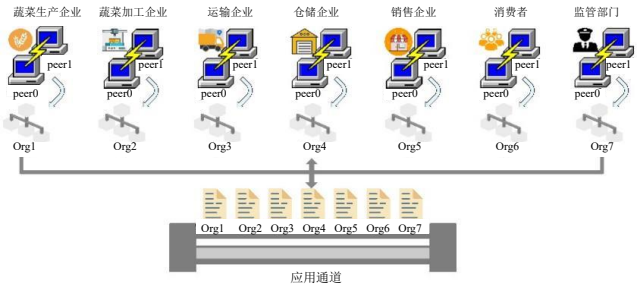


图6　蔬菜防伪溯源Fabric网络结构

Fig. 6　Fabric network structure for vegetable anti-counterfeiting traceability

在fabric中，智能合约被称为链码，赋予整个区块链网络更高级的逻辑控制，在蔬菜防伪溯源区块链网络中，通过智能合约实现所有的业务逻辑和交易记账，链码设计如表4所示。

表4　数据上链、加密、查询相关链码设计

Table 4　Design of chaincode for data uploading, encryption, and query

链码功能	方法名称	描述	输入	输出
物联网数据上链	UploadProductionData( )	将生产数据写入区块链	生产数据	True/False
	UploadProcessData( )	将加工数据写入区块链	加工数据	True/False
	UploadStorageData( )	将储运数据写入区块链	储运数据	True/False
	UploadSaleData( )	将销售数据写入区块链	销售数据	True/False
PQ-ECIES加密验证	GenerateKey( )	生成非对称密钥	组织节点信息	公私钥对
	PublicKeyEncryption( )	公钥加密	供应链隐私数据	True/False
	PrivateKeyVerification( )	私钥验证	PQ-ECIES加密后数据	True/False
数据查询	QueryPublicData( )	查询公开数据	公开数据ID	对应公开数据
	QueryPrivacyData( )	查询隐私数据	隐私数据ID	对应隐私数据

将蔬菜供应链各环节的溯源信息写入区块链均由智能合约实现。以产前物联网设备上传区块链数据为示例，具体算法见表5中的Algorithm 3。

3.2 信息采集准确性测试

追溯系统根据设备注册、验证流程，将物联网设备集成至追溯系统中，进行统一管理，整合了7类9种物联网设备，配置管理与数据如图7所示。

以农残检测数据录入场景为例，对物联网方式与人工方式的数据采集录入时效、准确率进行了测试。分别对1 000，2 000，5 000个农残样本进行检测，通过物联网设备接入、单人人工录入、双人人工录入三种方式进行数据采集，数据采集统计结果如图8所示。测试结果表明，随着数据量的增大，在录入时效方面物联网设备接入方式明显高于人工录入。在录入准确率方面，受人员注意力、样本数量、录入时间等因素的影响，采用物联网方式的数据录入准确率高于单人录入和双人录入方式。因

表5 溯源信息上链智能合约算法

Table 5 Traceability information on chain smart contract algorithm

Algorithm 3：溯源信息上链智能合约算法

Input：上传蔬菜货物溯源ID、土壤湿度、气候数据、虫害发生情况等产前物联网数据信息

Output：True/False

1：function UploadProductionData( ) //区块链中的产前物联网设备对应peer节点发起invoke上链请求

2：if len(args) then //判断请求中的数组长度是否符合规定长度标准

3：return shim.Error //数组长度不符合标准，上链失败，返回具体错误原因

4： end if

5：uploadData ← preconditioning//将参数填入数据结构中

6：m ← json.M arshal(uploadData)//将对象序列化成数组存储

7：err ← stub.P utState(uploadData.ID，m)//根据ID，创建索引

8：err ← stub.P utState(uploadData.Name，m)//根据Name，创建索引

9：if err then //判断上链请求是否成功

10：return shim.Error //上链失败，返回具体错误原因

11：end if

12：end function

此，采用物联网设备接入方式能够在大幅提升录入效率的基础上，节省人工成本，提高信息采集的准确率。

3.3 追溯数据链上性能分析

追溯链上的性能分析包括数据上链和数据查询两个部分的性能分析，数据上链性能测试结果如图9a所示，蔬菜溯源数据的平均上链时延为2 879 ms，能够满足蔬菜供应链全环节溯源数据的系统应用需求；数据查询性能测试结果如图9b所示，蔬菜溯源数据的平均查询时间为122 ms，能够满足相关溯源用户快速查询蔬菜供应链中各环节溯源信息的需求；由以下测试结果可以得出，该蔬菜防伪溯源区块链的数据上链和数据查询效率较高。

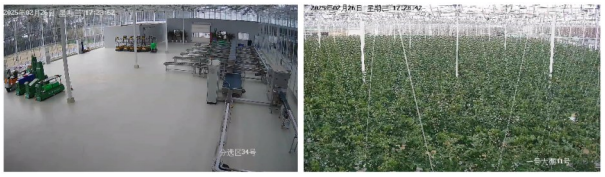
3.4 蔬菜供应链PQ-ECIES性能测试

本节性能测试旨在验证第2.2节提出的PQ-ECIES混合加密方案在蔬菜供应链防伪溯源实际场景中的可行性、效率与安全性优势。传统追溯系统依赖的ECC/RSA算法面临量子计算如Shor算法的严峻威胁，而对称加密如AES虽高效，但密钥分发管理复杂且不提供非对称特性所需的源认证和细粒度访问控制。PQ-ECIES的设计目标正是为了解决这些矛盾，在保障抗量子安全性的同时，满足物联网设备资源受限、高频数据上链的实时性需求，并通过非对称特性支持安全的密钥分发和权限控制。测试结果将直接评估PQ-ECIES是否达成这些设计目标，并量化其在蔬菜溯源场景下的实际效能。提出的蔬菜供应链防伪溯源PQ-ECIES加密算法与高级加密标准算法、非对称加密RSA算法的加密与解密环节进行测试对比，实验结果取算法运行50次的平均值，为了清晰地展示结果，将三个指标融合在一张柱状图进行展示，结果如图10所示。分别测试3种方法的密钥生成时间、加密时间和解密时间。

a. 环境监测物联网设备展示

b. 视频监控物联网设备展示

c. 实时环境监测界面

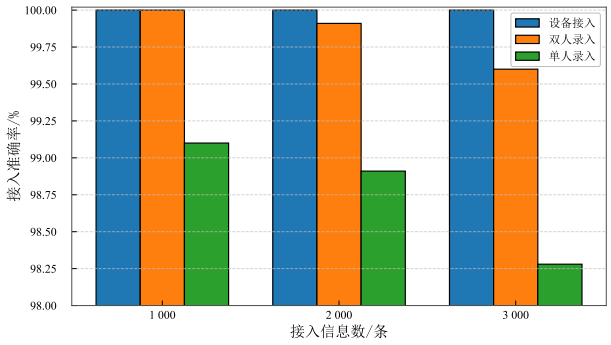


d. 实时视频监控界面

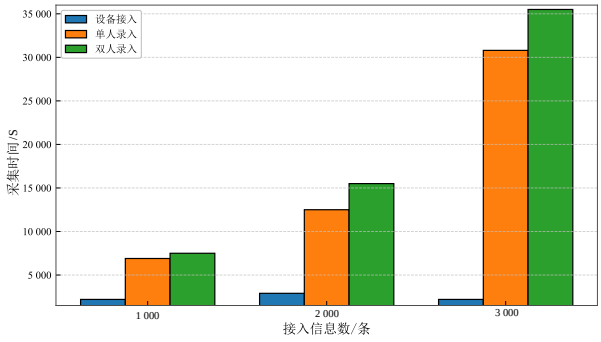
图7 基于区块链的物联网系统

Fig. 7 IoT system based on blockchain

在128 B明文大小的情况下明文加密与解密环



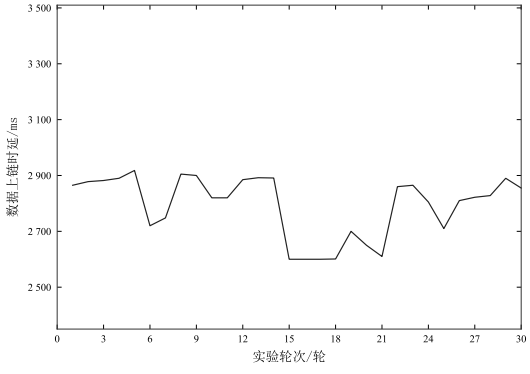
a. 不同方式数据接入准确率



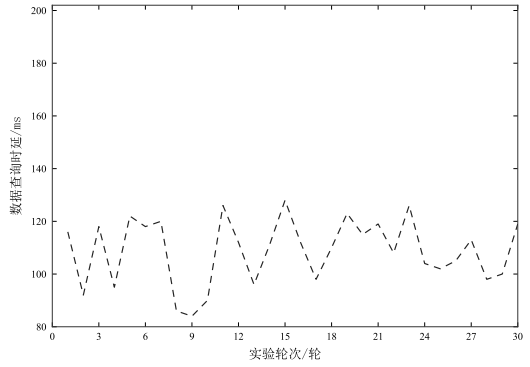
b. 不同方式数据采集时间

图8　不同方式录入数据准确率对比

Fig. 8　Accuracy comparison of data inputted through different methods



a. 数据上链平均时延



b. 数据查询平均时延

图9　区块链平台数据上链与查询性能测试

Fig. 9　Blockchain platform data on chain and query performance testing

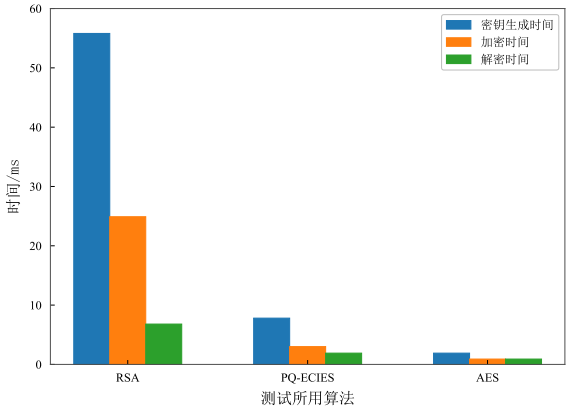


图10　隐私保护三种加密方法性能对比

Fig. 10　Performance comparison of three encryption methods for privacy protection

节所消耗总时长中RSA算法最长，约为50～80 ms，PQ-ECIES总时长约为30 ms，AES所需时长最短，在10 ms以内。本研究提出的PQ-ECIES加密算法总时长小于RSA算法是因为kyber基于格密码（Lattice-Based Cryptography），使用高效的多项式运算和结构化数学问题，易于硬件加速和并行计算，而ECC虽然同样是非对称加密算法，但在相同安全强度下使用的密钥更短，运算更快、占用资源更少，解决了高频小数据包如农残检测结果、物流状态实时上链的挑战，使安全加密能适配田间物联网设备农残检测仪、传感器和流通环节智能秤的计算能力与时效要求。而传统RSA依赖于大整数模幂运算，计算复杂度高、难以并行，且随着密钥增长性能急剧下降。

AES算法是一种对称加密算法，加密和解密使用相同的密钥，运算更简单、效率更高，所以与RSA相比时间开销还是有较明显的差距，但差距也基本在20 ms以内，通过微小效率折损换取了AES无法提供的非对称密钥分发、可验证数据源身份、细粒度访问控制及抗量子安全性，在蔬菜供应链场景中实现了安全与效率的最优平衡，实验与现场数据均表明其性能损失完全处于业务可容忍范围。

为验证PQ-ECIES的抗量子能力，采用NIST官方后量子密码评估库 Liboqs 版本0.8.0模拟量子攻击环境。测试选取Shor算法针对ECC与Grover算法针对AES作为攻击模型，对比传统ECIES与PQ-ECIES的破解难度得出表6。

传统算法在量子攻击时具有脆弱性，ECC-secp256k1/AES-256等常见加密算法数小时被破解，印证量子威胁担忧，若长期使用，一旦未来量子计算机实用化，历史与当前隐私数据包括位置、批

表6 常见隐私保护算法与PQ-ECIES对比测试

Table 6 Comparative testing of common privacy protection algorithms and PQ-ECIES

测试项	攻击算法	目标算法	量子比特需求/个	模拟破解时间	破解概率/%
ECC密钥恢复（secp256k1）	Shor算法	传统ECC	4 096	2.1小时	98.7
AES-256密钥搜索	Grover算法	传统AES	1 024	6.3小时	95.2
Kyber-768密钥恢复	格基攻击	PQ-ECIES	>1 000 000	>30年	<0.1

次、价格等机密性信息将被窃，摧毁系统可信根基。而PQ-ECIES算法具有强韧性，在NIST的评估轮次中，所有参与团队对Kyber的cryptanalysis（密码分析）均未取得突破性进展。评估团队的报告明确指出，针对Kyber-768的最佳已知攻击（使用BKZ算法）的核心SVP（最短向量问题）难度需要超过2^{140}次操作，即使未来的量子计算机也很难破解。集成的Kyber算法展现极强抗量子攻击能力，能有效抵御Shor算法等威胁。这确保了上链敏感隐私信息未来数十年的长期机密性，是传统方案无法比拟的核心安全优势，为产业提供了应对未来密码挑战的解决方案。

4 结 论

本研究通过分析蔬菜追溯过程中物联网设备需求，确定了以环境监测、农残检测、标签打印机等物联网设备为信息采集终端，搭建了追溯系统的硬件框架。建立了物联网设备数据接入与验证机制，能够有效防止因人为原因导致的数据误入、数据篡改，以及非认证设备进行非法信息采集和传输的情况发生，保证了追溯数据的真实性与准确性。

通过搭建蔬菜供应链防伪溯源区块链系统实现去中心化的数据管理，降低存储过程中的数据易篡改风险，设计基于蔬菜供应链的PQ-ECIES防伪隐私数据加密方法，有效保护蔬菜供应链中各环节物联网设备的隐私信息。PQ-ECIES通过Kyber算法实现IND-CCA2安全级别，结合ECC的短期安全性，形成双重防护壁垒。即使未来量子计算机突破ECC，Kyber仍可保障数据机密性。

通过实验分别测试物联设备信息采集的准确性、数据上传区块链和查询时的时间开销、蔬菜供应链ECIES隐私保护方法的性能。测试结果表明提出的蔬菜防伪物联网设备信息采集准确性高，ECIES隐私保护方法性能良好，系统性能满足蔬菜供应链溯源的需求，为蔬菜供应链场景下区块链防伪溯源提供借鉴与参考。

利益冲突声明：本研究不存在研究者以及与公开研究成果有关的利益冲突。

参考文献：

[1] 孙传恒, 朱文颖, 邢斌, 等. 中国农产品质量安全可追溯体系发展历程与展望[J]. 农业工程学报, 2025, 41(12): 1-14.
SUN C H, ZHU W Y, XING B, et al. Development history and prospects of agricultural product quality and safety traceability system in China[J]. Transactions of the Chinese Society of Agricultural Engineering, 2025, 41(12): 1-14.

[2] VU N, GHADGE A, BOURLAKIS M. The impact of Blockchain adoption on supply chain performance: Evidence from food industry[J]. International Journal of Production Research, 2025, 63 (14): 5402-5427.

[3] ZHANG Y T, SHANG J. Green technology investment and channel selection in sustainable food supply chain based on blockchain technology[J]. Frontiers in Sustainable Food Systems, 2025, 9: 1638313.

[4] LIU Z, YANG T C, HU B, et al. The application of blockchain technology in fresh food supply chains: A game-theoretical analysis under carbon cap-and-trade policy and consumer dual preferences[J]. Systems, 2025, 13(9): 737.

[5] BOUCHBOUT Y, BENRAZEK A E, MOLNÁR B, et al. Internet of Things and blockchain adoption in food supply chain: A survey [J]. IoT, 2025, 6(3): 51.

[6] KANDASAMY J, ETHIRAJAN M, AGRAWAL T K, et al. A new blockchain and IoT based architecture of food safety system for confectionery supply chain in Industry 4.0 era[J]. Applied Food Research, 2025, 5(2): 101340.

[7] 林建材. 烟台苹果质量安全监管和追溯系统研究与应用[R]. 烟台: 烟台市农业技术推广中心, 2002-12-11.
LIN J C. Research and application of Yantai apple quality safety supervision and traceability system[R]. Yantai: Yantai Agricultural Technology Extension Center, 2002-12-11.

[8] 张继恩. 商品条码在食品冷链物流中的应用[J]. 现代食品, 2025, 31(3): 120-123.
ZHANG J E. Application of commodity bar code in food cold chain logistics[J]. Modern Food, 2025, 31(3): 120-123.

[9] 熊盼, 黄小燕. 区块链技术在果业供应链中的应用研究[J]. 贵州农机化, 2025(2): 32-36.

[10] 张净, 唐恒睿, 刘晓梅. 基于区块链及IPFS的农产品多链追溯系统研究[J]. 中国农机化学报, 2024, 45(7): 127-134.
ZHANG J, TANG H R, LIU X M. Research on multi-chain traceability system of agricultural products based on blockchain and IPFS[J]. Journal of Chinese Agricultural Mechanization, 2024, 45 (7): 127-134.

[11] MEHANNAOUI R, MOUSS K N, AKSA K, et al. A holochain-based IoT-enabled agri-food traceability system: Application in the recombined milk supply chain[J]. International Journal of information Technology, [2025-07-09]. https://doi. org/10.1007/s41870-024-02396-7.

[12] 沈诗琦, 王婧. 基于区块链技术的农产品供应链研究[J]. 物流科技, 2025, 48(6): 99-102.
SHEN S Q, WANG J. Research on the agricultural supply chain based on blockchain technology[J]. Logistics Sci-Tech, 2025, 48 (6): 99-102.

[13] MASTILOVIĆ J, KUKOLJ D, KEVREŠAN Ž, et al. Emerging perspectives of blockchains in food supply chain traceability based on patent analysis[J]. Foods, 2023, 12(5): 1036.

[14] 陈醇, 张重阳, 冯国富. 基于区块链的水产养殖数据存储与溯源模型研究[J]. 渔业现代化, 2025, 52(3): 108-116.
CHEN C, ZHANG C Y, FENG G F. Research on blockchain-based data storage and traceability model for aquaculture[J]. Fishery Modernization, 2025, 52(3): 108-116.

[15] 李瑶, 栾洲栋, 王昊东, 等. 区块链技术在果品供应溯源系统中

的创新应用[J]. 果农之友, 2025(6): 150-152.
LI Y, LUAN Z D, WANG H D, et al. Innovative application of blockchain technology in fruit supply traceability system[J]. Fruit growers' Friend, 2025(6): 150-152.
[16] OJETUNDE B, KURIHARA T, YANO K, et al. A practical implementation of post-quantum cryptography for secure wireless communication[J]. Network, 2025, 5(2): 20.
[17] IAVICH M, KUCHUKHIDZE T. Investigating CRYSTALS-kyber vulnerabilities: Attack analysis and mitigation[J]. Cryptography, 2024, 8(2): 15.
[18] 巫宇, 刘明光, 费奕霖, 等. 基于区块链与大数据技术的预制菜质量安全溯源系统[J]. 智慧农业导刊, 2025, 5(7): 17-20.
WU Y, LIU M G, FEI Y L, et al. Quality and safety traceability system for prefabricated vegetables based on blockchain and big data technologies[J]. Journal of Smart Agriculture, 2025, 5(7): 17-20.
[19] 谢茂南. 物联网技术在农产品质量监测与溯源中的应用研究[J]. 农机使用与维修, 2023(12): 55-57.
XIE M N. Research on the application of Internet of Things technology in agricultural product quality monitoring and traceability [J]. Agricultural Machinery Using & Maintenance, 2023(12): 55-57.
[20] 张洪奇, 张艳, 张晨, 等. 设施智慧农场大数据平台开发与应用[J]. 山东农业大学学报(自然科学版), 2024, 55(3): 295-303, 475.
ZHANG H Q, ZHANG Y, ZHANG C, et al. Development and application of big data platform for facility intelligent farm[J]. Journal of Shandong Agricultural University (Natural Science Edition), 2024, 55(3): 295-303, 475.
[21] 洪轲, 梅娟. 基于农产品溯源的电子商务平台设计与实现[J]. 电脑知识与技术, 2025, 21(1): 48-50.
HONG K, MEI J. Design and implementation of E-commerce platform based on traceability of agricultural products[J]. Computer Knowledge and Technology, 2025, 21(1): 48-50.
[22] 沈倩. 基于区块链技术的农产品冷链物流追溯系统解决方案[J]. 物流工程与管理, 2024, 46(5): 60-63, 103.
SHEN Q. A solution for agricultural product cold chain logistics traceability system based on blockchain technology[J]. Logistics Engineering and Management, 2024, 46(5): 60-63, 103.
[23] 李倩, 王建平, 吕莹莹, 等. 基于区块链和物联网的优质果品溯源平台关键技术及应用[J]. 河南科技学院学报(自然科学版), 2025, 53(3): 54-69.
LI Q, WANG J P, LV Y Y, et al. Key technologies and applications of a high-quality fruit traceability platform based on blockchain and the Internet of Things[J]. Journal of Henan Institute of Science and Technology (Natural Science Edition), 2025, 53(3): 54-69.
[24] 郭浩. 太原市农产品供应链追溯系统推广策略研究[D]. 大连: 大连海洋大学, 2024.
GUO H. Research on promotion strategies for the Taiyuan agricultural product supply Chain traceability system[D]. Dalian: Dalian Ocean University, 2024.
[25] 孙传恒, 万宇平, 罗娜, 等. 面向追溯主体的果蔬全供应链区块链多链模型研究[J]. 农业机械学报, 2023, 54(4): 416-427.
SUN C H, WAN Y P, LUO N, et al. Blockchain multi-chain model of fruit and vegetable supply chain for traceability subjects[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(4): 416-427.
[26] 钱建平, 张保岩, 邢斌, 等. 集成实时快速检测信息的蔬菜追溯系统改进与应用[J]. 农业工程学报, 2015, 31(4): 306-311.
QIAN J P, ZHANG B Y, XING B, et al. Improvement and application of vegetable traceability system with integrated real-time rapid detection of information[J]. Transactions of the Chinese society of Agricultural Engineering, 2015, 31(4): 306-311.
[27] 姜锦婷. 基于区块链技术对农产品冷链物流系统的优化: 以徐州市为例[J]. 物流工程与管理, 2023, 45(11): 93-95, 119.
JIANG J T. Optimization of agricultural products cold chain logistics system based on blockchain technology: Taking Xuzhou as an example[J]. Logistics Engineering and Management, 2023, 45(11): 93-95, 119.
[28] 高琪娟, 蒋道臻, 乐阳, 等. 基于Fisco-Bcos联盟链技术的农产品溯源系统设计与实现研究[J]. 安徽农业大学学报, 2024, 51(3): 530-536.
GAO Q J, JIANG D Z, LE Y, et al. Research on the design and implementation of an agricultural product traceability system based on Fisco-Bcos consortium blockchain technology[J]. Journal of Anhui Agricultural University, 2024, 51(3): 530-536.
[29] 孙传恒, 张军, 罗娜, 等. 牡蛎供应链生物风险因子溯源隐私数据加密共享方法研究[J]. 农业机械学报, 2025, 56(5): 577-588.
SUN C H, ZHANG J, LUO N, et al. Research on method of encrypted sharing of privacy data for tracing biological risk factors in oyster supply chain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2025, 56(5): 577-588.
[30] 杨国涛, 曹冲, 韩涛, 等. 物联网中基于混合加密的密码安全认证方法[J]. 集成电路与嵌入式系统, 2024, 24(4): 23-29.
YANG G T, CAO C, HAN T, et al. Password security authentication method based on hybrid encryption in the Internet of Things [J]. Integrated Circuits and Embedded Systems, 2024, 24(4): 23-29.
[31] 米瑞琪, 江浩东, 张振峰. 基于Kyber公钥加密的高效认证密钥交换协议[J/OL]. 软件学报 . (2025-06-11)[2025-06-30]. https://link.cnki.net/doi/10.13328/j.cnki.jos.007393.
MI R Q, JIANG H D, ZHANG Z F. Efficient authenticated key exchange protocol based on kyber public-key encryption[J/OL]. Journal of Software. (2025-06-11)[2025-06-30]. https://link.cnki.net/doi/10.13328/j.cnki.jos.007393.
[32] 林自然, 程池, 陈鹏, 等. 一种针对Kyber的并行检错密钥恢复方案[J]. 密码学报(中英文), 2025, 12(2): 429-442.
LIN Z R, CHENG C, CHEN P, et al. Parallel error-checking key recovery scheme for kyber[J]. Journal of Cryptologic Research, 2025, 12(2): 429-442.
[33] EHSAN M A, ALAYED W, REHMAN A U, et al. Post-quantum KEMs for IoT: A study of kyber and NTRU[J]. Symmetry, 2025, 17(6): 881.

Vegetable IoT Blockchain Anti Counterfeiting Traceability System Based on PQ-ECIES

QI Peiyang[1,2], SUN Chuanheng[2], TAN Changwei[3], WANG Jun[4], LUO Na[2], XING Bin[2*]

（1. *School of Information*, *Shanghai Ocean University*, *Shanghai* 201306, *China*; 2. *National Engineering Research Center for Information Technology in Agriculture*, *Beijing* 100097, *China*; 3. *Agricultural College*, *Yangzhou University*, *Yangzhou* 225009, *China*; 4. *Jiangsu Legeous Information Technology Co.* , *Ltd*, *Changzhou* 213000, *China*）

Abstract: [Objective] The vegetable supply chain is characterized by multiple production entities, diverse product varieties, and complex circulation processes, which often result in low data accuracy, label forgery, data tampering, and difficulties in cross-enterprise

collaboration in traditional traceability systems. Furthermore, the rapid development of quantum computing poses significant threats to existing cryptographic foundations by enabling efficient factorization or discrete logarithm attacks. This study aimed to design and implement a vegetable supply chain anti-counterfeiting and traceability system that integrates the Internet of Things (IoT), blockchain technology, and a post-quantum enhanced elliptic curve integrated encryption scheme (PQ-ECIES). The system seeks to enhance the trustworthiness, privacy protection, and collaborative efficiency of supply chain data management, while maintaining practical performance for IoT devices and high-frequency data uploading scenarios. **[Methods]** The proposed system was constructed on an IoT framework incorporating nine categories of devices. A registration and admission mechanism was developed to establish a trusted mapping between "device–enterprise–data", effectively preventing unauthorized entities from uploading forged data. At the data layer, collected information was divided into public and private categories: Public data were uploaded directly to the blockchain, while private data were encrypted using PQ-ECIES before being stored on-chain. Smart contracts automated processes such as data classification, permission verification, and encrypted data querying, thus reducing human intervention and ensuring compliance. PQ-ECIES was designed by combining elliptic curve cryptography (ECC) and the Kyber algorithm from lattice-based post-quantum cryptography. A dual-key mechanism was employed to generate session keys, where an ECC-derived shared secret was combined with a Kyber-derived shared secret through SHA3-256 hashing, followed by key derivation for encryption and authentication. This design provided resilience against Shor's algorithm and other quantum attacks while maintaining efficiency compatible with IoT devices. The blockchain system was implemented using Hyperledger Fabric 1.4.4, with seven organizational nodes and the Raft consensus mechanism. Performance testing included evaluations of data collection accuracy, on-chain latency, query latency, and encryption performance across RSA, advanced encryption standard (AES), and PQ-ECIES. **[Results and Discussions]** The IoT-based data collection achieved significantly higher accuracy than manual input, particularly in large-scale sample scenarios such as pesticide residue testing. The average latency for data uploading to the blockchain was 2 879 ms, while data query latency averaged 122 ms, both of which met the practical requirements of vegetable supply chain applications. In cryptographic performance testing, PQ-ECIES achieved encryption and decryption of 128 B plaintext in approximately 10—30 ms, outperforming RSA (50—80 ms) and only slightly slower than AES (<10 ms). This result indicates that PQ-ECIES achieved an optimal trade-off between efficiency and security, offering asymmetric encryption benefits such as key distribution and identity verification, along with strong post-quantum resistance. Simulation under quantum attack models confirmed that traditional ECC and AES could be compromised within hours using Shor's and Grover's algorithms, whereas PQ-ECIES maintained resilience due to the lattice-based hardness assumptions of Kyber. From a system-level perspective, three major contributions were identified. First, trustworthiness was enhanced by binding IoT devices to enterprises through Bluetooth-based verification and blockchain's immutable ledger, ensuring data authenticity at the source. Second, privacy protection was achieved by adopting graded visibility: Consumers accessed only public data such as testing results and logistics status, while regulators could decrypt private information (e.g., production location and batch details) via authorized keys, balancing transparency with confidentiality. Third, collaboration across enterprises was improved through the consortium blockchain structure and Fabric channel mechanisms, which eliminated information silos and enabled selective data sharing in real time, reducing inter-organizational access time from weeks to minutes. Experimental validation confirmed that IoT-based collection significantly improved accuracy, blockchain integration achieved acceptable on-chain and query latency, and PQ-ECIES outperformed RSA while offering post-quantum resistance not available in AES. **[Conclusions]** This study proposed and implemented a vegetable supply chain traceability system that integrates IoT, blockchain, and PQ-ECIES. By deploying nine categories of IoT devices, establishing trusted device-enterprise mappings, and incorporating blockchain's decentralized and tamper-proof ledger, the system ensured reliable data collection and storage. The integration of PQ-ECIES provided dual cryptographic protection, balancing efficiency with long-term quantum security. Beyond technical performance, the system enhanced trust, privacy, and collaboration across the vegetable supply chain, effectively addressing common issues of data forgery, tampering, and cross-enterprise coordination.Overall, the proposed framework demonstrates high potential for real-world deployment in agricultural supply chains, offering a secure, efficient, and future-proof solution to ensure authenticity, reliability, and transparency in vegetable traceability. The study also provides a reference model for extending post-quantum blockchain-based traceability to other agri-food sectors facing similar challenges.

Keywords: Internet of Things; blockchain; vegetable traceability system; anti-counterfeiting traceability; Post Quantum encryption; supply chain

Foundation items: Jiangsu Provincial Science and Technology Program (Key R&D Program for Modern Agriculture) Project (BE2023315)

First author: QI Peiyang, E-mail: 2556382216@qq.com

***Corresponding author:** XING Bin, E-mail: xingb@nercita.org.cn