•聚焦国家重点研发计划•

DOI:10.12454/j.jsuese.202400954

本刊网刊

分布式无证书网络身份系统的关键技术研究构想和成果展望

张小松[1,2],曹　晟[1*],陆天波[3],杨　坤[4,5],桂　勋[1],谢国涛[6],牛伟纳[1]

(1.电子科技大学 计算机科学与工程学院(网络空间安全学院),四川 成都 611731;2.电子科技大学(深圳)高等研究院, 广东 深圳 518110;
3.北京邮电大学 计算机学院(国家示范性软件学院),北京 100876;4.浙江大学 区块链与数据安全全国重点实验室,浙江 杭州 310007;
5.浙江大学 网络空间安全学院,浙江 杭州 310007;6.中讯邮电咨询设计院有限公司,北京 100080)

摘　要:随着万物互联的持续演进与深化,工业互联网、能源互联网、车联网等数字业务规模不断扩大。同时,各类软硬件设备与系统逐渐呈现智能化和复杂化,中心化身份认证方法面临的性能问题和安全威胁日益突出,适用于分布式无证书网络身份认证的技术和平台缺失。为有效应对分布式网络身份认证的严峻挑战,研究分布式无证书身份认证基础理论体系和应用模式,包括认证架构、密钥管理、硬件增强、并行执行、集成应用等。本研究针对分布式无证书网络身份认证的3个科学问题:密钥系统安全高效管理、海量接入硬件加速认证、智能合约并行优化运行;围绕5大课题研究方向:高性能无证书的网络身份认证技术与架构、无证书的分布式密钥管理、高并行分布式终端接入硬件增强、多层级并行化智能合约虚拟机、分布式大规模物联网身份认证应用与验证;重点突破10类关键技术:高性能分布式身份标识与共识技术,无证书身份认证协议族与网络架构技术,基于智能合约的无证书密钥自动化管理技术,可持续抗攻击的分布式密钥生成、分发及回收技术,内生安全的高性能硬件层级构建技术,异构终端跨域安全接入一体化硬件加速技术,智能合约并行化协处理架构技术,智能合约虚拟机优化调度技术,轻量无证书公钥标识框架技术,基于国密的物联网标识身份管理技术;研发5种主要系统/工具:设备数字身份全流程管理系统、密钥全生命周期管理系统、硬件增强的高性能终端并发接入系统、基于国产芯片的智能合约协处理器系统、大规模分布式数字身份系统应用检测评估工具。面向能源物联网、车联网等典型工业互联网业务的分布式无证书环境下网络身份认证场景,构建具备基于国密和物联网标识认证的终端设备可信身份、安全接入、安全管控等功能的分布式大规模物联网身份认证应用平台。建立分布式无证书环境下网络身份标识、共识、集成、应用全过程的关键技术体系。研究成果从数字身份安全层面保障国家数字经济高质量安全发展,支撑中国网络空间安全与治理重大战略实施,有效鉴别对中国关键信息基础设施的访问与入侵,对于提升国家网络安全和信息化有重要意义。

关键词:网络空间安全;区块链;无证书;密钥管理;硬件增强;并行处理;身份认证

中图分类号:TP302.1;TP309.7　　**文献标志码:**A　　**文章编号:**2096-3246(2025)03-0001-10

随着全球科技发展及产业升级,海量智能设备已互联互通。2024年全球具备网络连接功能的物联网设备达到110亿台,同比增长20%。当前海量物联网设备身份认证与管理问题面临前所未有的挑战,构建分布式、高性能网络身份认证系统成为各方共识。当前,中心化身份认证方法,已无法满足认证架构难设计、密钥管理难高效、接入过程难加速、合约执行难并行等需求。

在网络安全领域,安全与效率是贯穿其中的核心矛盾:增强安全性通常意味着更高的计算开销或更复杂的协议设计,而提高效率往往需要牺牲部分安全性。因此,如何在分布式身份认证中平衡这两者,是当前研究的核心问题。具体而言,当前分布式无证书网络身份认证面临以下技术挑战:首先,在海量设备并发认证的需求下,现有的分布式认证方法在满足认证效率的同时安全性较低,易导致认证过程中的隐私

收稿日期:2024 – 11 – 16　　**修回日期:**2025 – 03 – 12　　**网络出版日期:**2025 – 04 – 25

基金项目:国家重点研发计划项目(2023YFB3105900);深圳市杰出人才培养经费资助项目;四川省科技计划项目(2023ZHJY0006)

作者简介:张小松(1968—),男,教授,博士. 研究方向:网络安全. E-mail: johnsonzxs@uestc.edu.cn

* **通信作者:**曹　晟,研究员, E-mail: caosheng@uestc.edu.cn

泄露或中间人攻击。其次，密钥管理方面，现有的密钥生成、分发和更新机制依赖于可信第三方，难以在分布式环境下实现密钥的全生命周期安全管理，尤其是在跨域场景下，密钥的可信协商与动态更新问题尤为突出。第三，硬件增强方面，随着物联网设备的异构性增加，现有的硬件加速技术难以满足大规模终端并发接入的需求，尤其是在受限节点和终端的动态跨域计算中，硬件加速的效率和安全性亟待提升。最后，智能合约的并行执行问题也制约了分布式身份认证系统的扩展性，现有的智能合约虚拟机架构多为串行执行，难以支持大规模身份认证场景下的高效并行处理。

为解决上述挑战，亟需在分布式无证书的身份认证与架构、无证书的分布式密钥管理、高并行分布式终端接入硬件增强、多层级并行化智能合约虚拟机、分布式大规模物联网身份认证应用平台集成验证等方面进行攻关，研制基于国产芯片的分布式大规模物联网身份认证应用平台。

在高性能无证书网络身份认证架构方面，现有方法缺乏针对分布式无证书网络身份的高效安全认证与管理。其中：针对分布式数字身份，现有工作主要聚焦于身份信息的中心化管理与应用，分布式数字身份的可信验证和异常行为可信追踪能力欠缺[1–4]；针对物联网终端跨域认证，现有工作主要集中于密钥派生的跨域认证方案，存在可扩展性差和认证效率低的问题[5–8]；针对共识机制，现有工作主要集中于抽象网络结构的共识算法优化，无法提供精准时标和位置信息的轻量级抗攻击共识机制[9–12]。因此，研究高性能分布式身份标识与共识、跨域分层的身份认证交互模型、多重身份动态组合及信任映射、可编程自适应协议族，实现多场景下高性能、高安全的身份认证是重要趋势。

在无证书分布式密钥管理方面，现有方法难以实现可持续抗攻击的无证书密钥安全高效管理。其中：针对密钥全生命周期管理，现有方法主要依赖于可信第三方，难以保证分布式环境下海量设备密钥的安全性和可扩展性[13–15]；针对抗攻击的密钥生成，现有方法主要使用中心化的生成方式，难以应对密钥生成过程中的单点故障问题[16–18]；针对跨域可靠密钥分发，现有方法主要集中在通信各方之间秘密协商，缺少基于智能合约的自动化高效分发能力[19–21]；针对海量设备密钥更新与回收，现有方法主要集中在分层组密钥结构化设计，难以实现跨域密钥高效更新与回收[22–24]。因此，研究密钥的智能化管理、去中心化生成、可靠分发和高效回收技术是未来的重要趋势。

在大规模终端接入的硬件增强方面，现有方法缺乏对海量异构终端的高效硬件加速技术。其中：针对高性能硬件层级构建，现有工作主要聚焦于多核处理器结构设计，缺乏跨层级的软硬服统筹优化[25–27]；针对主节点认证加速，现有工作主要集中于对密码算法引擎的高性能设计，缺乏对认证协议全流程的系统性优化及动态环境下的资源调度机制[28–30]；针对异构终端的可信密态安全加固，现有工作主要聚焦于平台内安全算法的效率提升，缺乏在不同平台和设备之间实现密态安全加固的研究[31–33]；针对国产芯片加速的加密通信，现有工作主要应用集成的国产密码卡，缺乏对国产芯片加速的支持与优化[34–36]。因此，研究大规模异构终端接入的软硬件环境安全可靠构建、受限节点与终端的动态跨域计算硬件加速，是物联网终端接入中硬件环境发展的新趋势。

在智能合约虚拟机运行加速方面，现有研究缺少针对多层级并行智能合约虚拟机架构与技术。其中：针对虚拟机架构，现有研究集中在基于栈的架构设计，缺乏支持矢量指令集和矢量算子的自主可控架构，难以支撑高性能矢量化并行化智能合约虚拟机构建[37–39]；针对智能合约编译优化和目标代码生成，现有研究集中在目标代码直接生成，缺乏中间代码优化和自定义矢量算子嵌入，难以提升智能合约目标代码的执行效率[40–42]；针对智能合约虚拟机调度，现有研究集中在虚拟机安全增强调度，缺乏提升虚拟机运行效率的调度算法、细粒度内存管理和重用机制研究，难以支撑批量智能合约的高效执行[43–45]。因此，研究支持矢量指令集和矢量算子的多层级并行虚拟机架构、中间代码优化、优化调度和高效内存管理是智能合约虚拟机研究的重要趋势。

综上可知，以往国内外相关机构和学者在身份认证的架构设计、密钥管理等方面进行了大量研究，并取得了长足进步。但在认证性能及安全接入方面仍存在诸多问题，突出表现在密钥系统安全高效管理、海量接入的硬件加速认证、智能合约并行优化运行等方面。相较于国内外已有研究，本研究针对 3 大关键科学问题，提出 5 大课题研究方向，突破 10 类关键技术，研发分布式大规模物联网身份认证应用平台，构建分布式可信身份认证体系。在分布式无证书的身份认证框架、可持续抗攻击的分布式密钥管理、硬件增强的海量异构终端一体化协同加速认证、支持国产硬件加速的多层级并行智能合约虚拟机协处理技术等 4 大方面具备创新性。

1 研究内容

1.1 拟解决的关键科学问题

面向分布式无证书网络身份系统的现状，针对分

布式无证书网络身份认证中认证架构难设计、密钥管理难高效、接入过程难加速、合约执行难并行的需求，亟需解决3大科学问题：

1）关键科学问题1，密钥系统安全高效管理问题。解决密钥的可信协商与动态更新、全生命周期自动化高效管理难题，支撑海量设备跨域密钥持续安全。

2）关键科学问题2，海量接入的硬件加速认证问题。解决大规模异构终端接入的软硬件环境安全可靠构建、受限节点与终端的动态跨域计算硬件加速等难题，支撑大规模异构终端身份认证的一体化硬件增强。

3）关键科学问题3，智能合约并行优化运行问题。解决智能合约并行执行、目标代码优化生成、指令调度优化和内存重用等难题，支撑智能合约高效执行。

1.2　主要研究内容

以3个科学问题为引领，突破10类关键技术问题为核心，沿着高性能无证书的网络身份认证技术与架构、无证书的分布式密钥管理、高并行分布式终端接入硬件增强、多层级并行化智能合约虚拟机、分布式大规模物联网身份认证应用与验证5个课题研究方向开展针对性的重点研究，研发设备数字身份全流程管理、密钥全生命周期管理、硬件增强的高性能终端并发接入、基于国产芯片的智能合约协处理器、大规模分布式数字身份系统应用检测评估5种主要系统/工具，构建基于国产芯片的分布式大规模物联网身份认证示范应用平台。科学问题与课题之间的关系如图1所示。

图1　科学问题、研究内容与课题设置

Fig .1　Scientific questions, research content and topics setting

1）课题1，高性能无证书的网络身份认证技术与架构。

针对分布式环境下数字身份难以高效安全认证的挑战，解决海量数字身份认证中分布式身份标识、数据细粒度动态分配等难题。在分布式身份标识与共识方面，考虑面向精确时标和位置信息的时空增强轻量级抗攻击共识；在无证书身份认证协议族与网络架构方面，引入可编程自适应协议族、多重身份动态组合及信任映射等因素。提出分布式跨域的在线/离线身份可信验证、匿名身份可信验证等方法，实现分布式环境下数字身份的安全、高效认证，研制设备数字身份全流程管理系统。

2）课题2，无证书的分布式密钥管理。

针对海量异构物联网终端环境中密钥易受破坏或泄漏、密钥分发与更新效率低等挑战，解决无证书分布式密钥高效管理、抗攻击的多方密钥可信协商等难题。在分布式密钥生成方面，考虑基于可验证秘密共享技术的无证书异步分布式密钥生成方法；在认证密钥协商方面，引入无证书的轻量级跨域认证密钥协商协议。提出基于智能合约的自动化密钥管理、基于门限密码学的密钥生成等技术，实现密钥安全生成、跨域可靠分发及轻量级更新与回收，研制密钥全生命周期管理系统。

3）课题3，高并行分布式终端接入硬件增强。

针对海量异构终端身份认证过程中软硬件不协调、设计冗余、并行化程度弱、安全性差等挑战，解决异构终端安全接入软硬件一体化设计、高并行多层级硬件加速架构设计等难题。在异构终端安全接入软硬件一体化设计中，采用协议分层加速的设计范式，将认证协议中计算复杂度高的核心算法（如哈希函数、椭圆曲线点乘运算等）从协议中解耦，通过定制化的硬件加速器实现快速运算。认证协议中涉及的复杂密码运算通过调用硬件加速器预留的接口完成计算，以提升终端接入时的身份认证效率。在高并发的多层级硬件加速架构方面，充分利用物联网主节点服务器的计算资源，通过分布式并行计算和基于指令集优化的国密算法，实现对海量异构终端的并发实时接入，研制硬件增强的高性能终端并发接入系统。

4）课题4，多层级并行化智能合约虚拟机。

针对现有智能合约虚拟机串行执行、执行效率低、内存利用率低等挑战，解决基于国产芯片的多层级并行智能合约虚拟机架构、智能合约中间代码优化等难题。在智能合约虚拟机架构中，引入面向身份认证的矢量指令集和矢量算子，为椭圆曲线运算中的大数加、减、乘等特殊基础运算符，设计高效的矢量指令集，并将矢量指令集融入智能合约编译器；将身份认证关键函数（签名算法，验签算法）设计出矢量算子，并将矢量算子嵌入到智能合约虚拟机，最终实现空间占据小、可高效运行的身份认证智能合约及其虚拟机。在智能合约虚拟机优化调度方面，采用多虚拟机线程管理、最短指令距离调度等方法，最终实现基于国产芯片的高性能多层级并行智能合约虚拟机协处理系统，研制基于国产芯片的智能合约协处理器系统。

5）课题5，分布式大规模物联网身份认证应用与验证。

针对工业互联网设备海量异构、应用场景复杂等挑战，解决分布式大规模场景网络连接状况复杂、在线身份预置需求明确、实体与身份映射维护困难等难题。在应对不同工业互联网应用场景的复杂性方面，构建轻量无证书公钥标识框架，设计标准化统一适配架构和接口规范；在分布式物联网身份认证系统服务模块间协同方面，设计基于AI自动编排的安全协议处理方法。提出通用网络引导与分布式无证书融合，实现分布式大规模物联网身份认证在车联网、能源、工业互联网等行业的应用落地，研制大规模分布式数字身份系统应用检测评估工具。

2 研究方法和技术路线

为解决分布式环境下海量物联网终端身份认证中存在的关键问题，按照需求分析—体系设计—技术突破—系统研发—验证示范的研究思路，突破数字身份分布式标识、无证书身份认证网络模型与可编程自适应协议族，建立支撑与验证其他课题方法的理论基础；开展针对性的关键技术研究，实现无证书的分布式密钥管理、高并行分布式终端接入硬件增强、多层级并行化智能合约虚拟机；提出支撑技术集成与验证评估的技术框架与测试平台，在理论与技术成果基础上进一步验证、反馈和完善，从而形成无证书环境下基于国产芯片的分布式大规模物联网身份认证应用平台，总体研究思路如图2所示。

1）关键技术1，高性能分布式身份标识与共识。

针对身份共识性能瓶颈问题，提出数字身份分布式标识、时空信息增强的抗攻击共识等方法，突破可控匿名身份可信验证、异常行为可信追踪、新型轻量级共识机制等技术，以支撑高性能、高安全分布式身份认证。

2）关键技术2，无证书身份认证协议族与网络架构。

针对传统证书管理复杂问题，提出分层分级的无证书身份认证网络模型，突破可编程自适应协议族、多重身份动态组合及信任映射、跨域分层的身份认证交互模型构建等技术，以支撑海量数字身份认证。

3）关键技术3，基于智能合约的无证书密钥自动化管理。

针对密钥系统安全高效管理问题，提出基于智能合约的无证书密钥管理、密钥泄露关联分析方法，突破双线性映射/格的分布式密钥生成、组间匿名数据传输等技术，以支撑密钥全生命周期管理。

4）关键技术4，可持续抗攻击的分布式密钥生成、分发及更新。

针对密钥更新易受攻击问题，提出可持续抗攻击的多方密钥协商等方法，突破非交互零知识证明的数据匿名传输、基于格的安全密钥预分配、可证安全密钥动态更新与回收等技术，以支撑密钥安全生成、跨域可靠分发、轻量级更新与回收。

5）关键技术5，内生安全的高性能硬件层级构建。

针对海量接入的硬件加速认证问题，提出纵深防御的高性能硬件架构设计方法，突破物联网节点软硬服一体化加速、高算力哈希引擎、异构终端通用型密态安全加固、国产芯片高效加密通信等技术，以支撑高性能物联网认证架构构建。

6）关键技术6，异构终端跨域安全接入一体化硬件加速。

针对海量异构设备接入困难的问题，提出物联网

节点、终端、链路三位一体的协同优化加速方法，突破面向国密算法的高性能密码卡研发、受限计算资源设备国密算法轻量化等技术，以支撑海量异构终端环境下高效身份认证计算。

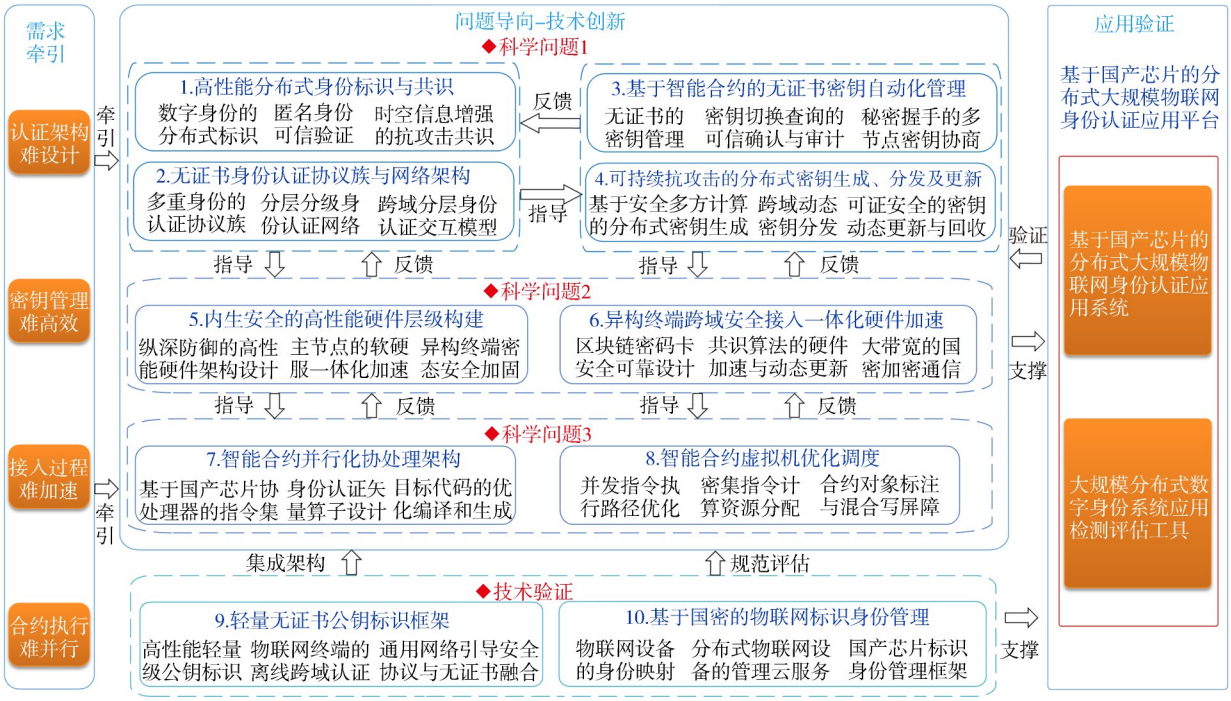

图2　总体研究思路

Fig. 2　General research ideas

7）关键技术7，智能合约并行化协处理架构。

针对智能合约并行优化运行问题，提出身份认证加速的智能合约协处理方法，突破矢量指令集和身份认证矢量算子设计、目标代码优化编译和生成等技术，以支撑大批量智能合约的并行加速。

8）关键技术8，智能合约虚拟机优化调度。

针对虚拟机调度开销大问题，提出智能合约虚拟机并发指令执行路径优化、内存高效管理与重用方法，突破最短指令调度、合约对象标注与混合写屏障等技术，以支撑内存受限环境下跳转开销小和执行效率高的智能合约虚拟机。

9）关键技术9，轻量无证书公钥标识框架。

针对跨域认证成本高问题，提出基于国密的高性能轻量公钥标识模型，突破物联网终端离线跨域认证、通用网络引导（GBA）安全协议与无证书融合等技术，以支撑安全高效的跨域物联网身份认证。

10）关键技术10，基于国密的物联网标识身份管理。

针对物联网身份验证难问题，提出国产芯片标识身份管理与应用框架，突破设备芯片指纹与密码融合信任根、基于AI自动编排的分布式无证书高效融合等技术，以支撑分布式无证书网络身份系统与平台的研制。

3　主要创新与成果展望

围绕分布式无证书网络身份系统的关键技术研究及示范中的关键科学问题和技术难题，开展联合攻关，创新点主要体现在以下4个方面。

1）分布式无证书的身份认证框架的创新，为分布式环境下海量异构物联网终端和节点安全可靠接入的身份认证提供理论与技术支撑。

围绕分布式环境下无证书的身份认证，针对分布式网络的去中心化、身份匿名、访问控制、可信管理、可信执行等特征，在已有的“互联网环境下抗深度追踪的信息传输平台研制与应用”等成果基础上，提出分布式跨域的在线/离线身份可信验证、基于零信任的细粒度动态访问控制、大规模多级递阶的身份认证网络架构设计、可编程身份认证协议族等方法，突破数字身份标识可信管理、访问控制权限安全可控无证书的跨域身份认证协同管理、动态多级信任域划分、分布式信任联盟构建、轻量级跨域身份协同管理、多重身份的动态信任映射、多层级分布式认证协商、信任分散的门限身份认证、认证协议的自动化选择及牵引、认证协议的智能化迁移及切换等关键技术，解决分布式身份认证过程中身份认证效率低、受网络攻击风险大、扩展性差、鲁棒性低、无法满足海量终端及节

点安全可靠接入等技术难点，保障海量异构设备的可信认证。

2）可持续抗攻击的分布式密钥管理的创新，为分布式无证书网络身份认证中密钥自动化管理提供理论和技术支撑。

围绕分布式无证书网络身份认证中密钥全生命周期自动化管理，针对密钥管理可信第三方依赖、使用场景复杂多变、分发路径不可控等特征，按照研究思路，在已有“基于信誉的物联网区块链共识协议”“一种证书存储节点选择方法及网络节点”“网络终端加密流量智能检测与威胁分析系统”等成果基础上，提出基于智能合约的自动化密钥管理、密钥泄漏关联分析、可验证的跨域密钥分发与回收、前向安全的密钥更新等方法，突破基于安全多方计算的分布式密钥生成、基于非交互零知识证明的安全数据匿名传输、基于椭圆曲线和格的安全密钥预分配、基于滑动窗口的量子密钥分发、基于动态分割抗私钥泄露的单向密钥演化、基于秘密共享的分布式密钥一致性检查等关键技术。解决异步网络环境下分布式随机数生成、可验证的跨域动态密钥管理等核心问题，构建一套高效、安全、自主可控的密钥全生命周期管理体系，为大规模分布式物联网身份认证提供理论支撑和技术保障。

3）硬件增强的海量异构终端一体化协同加速认证的创新，为大规模异构终端身份认证的一体化硬件增强提供技术支撑。

围绕大规模物联网身份认证的硬件增强，针对海量异构终端身份认证的软硬件不协调、设计冗余、并行化程度弱、安全性差等特征，按照研究思路，在已有异构终端身份认证硬件架构模型及“物联网系统数据安全关键技术及应用”“网络系统的分布式感知与协同控制基础理论与方法”等成果基础上，提出高并行高安全的多层级硬件架构、异构终端安全接入一体化设计、纵深防御硬件平台微架构设计、高性能数据平面加速等方法，突破物联网密码卡安全可靠设计、认证算法硬件加速、密码算法引擎轻量化、内生安全的硬件层级架构搭建。

4）支持国产硬件加速的多层级并行智能合约虚拟机协处理技术的创新，为分布式无证书网络身份认证中多层级并行智能合约虚拟机提供理论和技术支撑。

围绕适用于海量异构物联网节点身份认证的高性能智能合约虚拟机技术，针对现有智能合约虚拟机串行执行、执行效率低、内存消耗大等特征，按照研究思路，在已有“基于国产芯片的智能合约虚拟机V1.0”“一适用于形式化验证的智能合约编译方法”等成果基础上，提出多层级并行智能合约虚拟机架构、智能合约中间代码优化、智能合约虚拟机优化调度、智能合约虚拟机内存高效管理机制等方法，突破多层级并行的智能合约虚拟机协处理器、智能合约中间代码矢量化和并行化发掘、智能合约虚拟机最短指令距离调度、智能合约虚拟机细粒度内存管理和重用等关键技术，解决批量身份认证智能合约并发执行导致的系统性能瓶颈等核心问题。

本研究的最终目标是构建分布式大规模物联网身份认证应用平台，如图3所示。基于高性能无证书的网络身份认证技术与架构，在密钥管理、硬件增强、并行处理3大关键技术体系进行突破。前期，面向典型工业互联网业务，在国家级工业、能源、车联网、“双碳”等分布式网络身份认证场景，构建数字身份安全标识与共识、密钥安全管理、高并行终端接入硬件增强、多层级智能合约虚拟机的分布式大规模物联网身份认证应用与验证平台，开展技术集成验证与试点示范应用。未来，将依托完善的基于国产芯片的分布式大规模物联网身份认证应用平台，面向各行业的企事业单位，开展平台产品的应用推广与分布式身份认证技术服务，可直接、间接支撑各类互联网业务的年交易额达数十亿元。

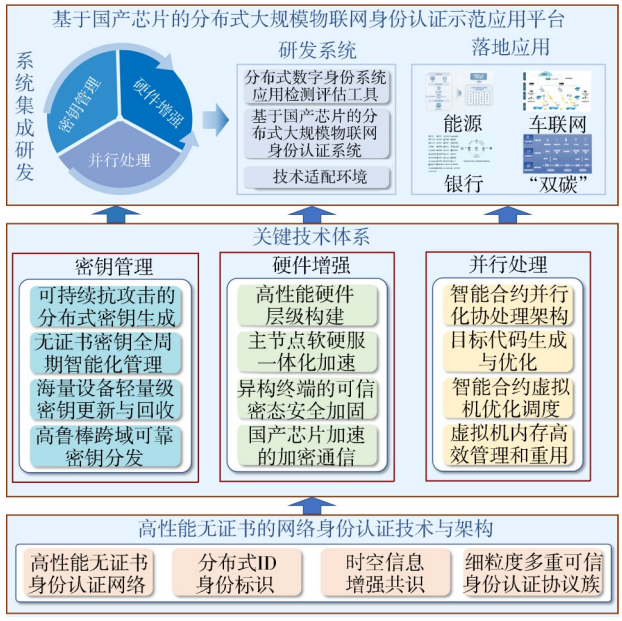

图3 分布式大规模物联网身份认证应用平台架构图

Fig. 3 Architecture diagram of distributed large-scale IoT identity authentication application platform

4 结 论

基于网络安全及互联网健康发展国家重大战略需求，面向分布式无证书网络身份认证的现状和需

求，提出认证架构设计—密钥高效管理—接入过程加速—合约并行执行—落地示范应用的研究体系框架，系统研究分布式无证书网络身份系统的关键技术。针对3大关键科学问题，提出5大课题研究方向，突破10类关键技术，具有4大创新点。

研究成果解决了分布式无证书环境下网络身份认证中认证架构难设计、密钥管理难高效、接入过程难加速、合约执行难并行的难点需求，能够实现分布式无证书环境下数据细粒度按需分配、匿名身份异常可验证；满足用户对分布式无证书环境下的身份认证的安全需求，避免隐私安全问题；实现分布式无证书环境下密钥安全生成、跨域可靠分发；实现内生安全的高性能硬件层级构建；满足海量终端环境下的高性能动态协同计算；为分布式无证书下数字身份认证提供基础理论模型、技术方法与验证平台，满足分布式无证书网络身份的安全与高效认证；对分布式无证书环境下网络身份认证等方面的科学研究、技术研发和产业推广应用具有十分重要的意义和价值。

本研究重点实现分布式无证书环境下数字身份安全标识与共识、密钥安全管理、高并行终端接入硬件增强、多层级智能合约虚拟机、大规模物联网身份认证应用与验证等全流程身份认证的理论基础与应用示范，为各类分布式无证书场景中网络身份认证提供标识与共识、密钥管理、硬件增强、并行化处理的基础架构与关键技术，并应用于工业、能源、车联网、“双碳”等典型物联网场景的网络身份认证，顺应分布式身份认证的技术和应用发展的趋势，规避中心化管理引发的风险，从数字身份安全层面保障国家数字经济高质量安全发展，支撑中国网络空间安全与治理重大战略实施。

参考文献：

[1] Jing Yue, You Xiaoyu, Bi Danyang, et al. The decentralized identity and its application for industrial Internet[C]//Proceedings of the 2021 3rd International Academic Exchange Conference on Science and Technology Innovation (IAECST). Guangzhou: IEEE, 2021: 671–674.

[2] Liu Yizhong, Zhao Boyu, Zhao Zedan, et al. SS–DID: A secure and scalable Web3 decentralized identity utilizing multilayer sharding blockchain[J]. IEEE Internet of Things Journal, 2024, 11(15): 25694–25705.

[3] Feng Libo, Lin Junyu, Qiu Fei, et al. SDAC–BBPP: A secure dynamic access control scheme with blockchain-based privacy protection for IIoT[J]. IEEE Transactions on Network and Service Management, 2024, 21(3): 3179–3193.

[4] Jarosz M, Wrona K, Zieliński Z. Distributed ledger-based authentication and authorization of IoT devices in federated environments[J]. Electronics, 2024, 13(19): 3932.

[5] Dallel O, Ben Ayed S, Tahar J B H. Blockchain-based authorization mechanism for educational social Internet of Things[J]. IEEE Access, 2024, 12: 42888–42907.

[6] Wang Fengqun, Cui Jie, Zhang Qingyang, et al. Blockchain-based secure cross-domain data sharing for edge-assisted industrial Internet of Things[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 3892–3905.

[7] Luo Deyu, Zhang Youchi, Sun Gang, et al. An efficient consensus algorithm for blockchain-based cross-domain authentication in bandwidth-constrained wide-area IoT networks[J]. IEEE Internet of Things Journal, 2024, 11(19): 31917–31931.

[8] Duan Xinrui, Guo Yajun, Guo Yimin. Design of anonymous authentication scheme for vehicle fog services using blockchain[J]. Wireless Networks, 2024, 30(1): 193–207.

[9] Yu Haifeng, Nikolic I, Hou Ruomu, et al. OHIE: Blockchain scaling made simple[C]//Proceedings of the 2020 IEEE Symposium on Security and Privacy(SP). San Francisco: IEEE, 2020: 90–105.

[10] Spiegelman A, Giridharan N, Sonnino A, et al. Bullshark: DAG BFT protocols made practical[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2022: 2705 – 2718.

[11] Sompolinsky Y, Wyborski S, Zohar A. PHANTOM GHOSTDAG: A scalable generalization of nakamoto consensus: September 2, 2021[C]//Proceedings of the 3rd ACM Conference on Advances in Financial Technologies. New York: ACM, 2021: 57–70.

[12] Decouchant J, Kozhaya D, Rahli V, et al. DAMYSUS: Streamlined BFT consensus leveraging trusted components[C]//Proceedings of the Seventeenth European Conference on Computer Systems. New York: ACM, 2022: 1–16.

[13] Rana S, Parast F K, Kelly B, et al. A comprehensive survey of cryptography key management systems[J]. Journal of Information Security and Applications, 2023, 78: 103607.

[14] Latif M A, Ahmad M B, Khan M K. A review on key management and lightweight cryptography for IoT[C]//Proceedings of the 2020 Global Conference on Wireless and Optical Technologies(GCWOT). Malaga: IEEE, 2020: 1–7.

[15] Tanveer M, Khan A U, Kumar N, et al. RAMP–IoD: A robust authenticated key management protocol for the Internet of drones[J]. IEEE Internet of Things Journal, 2022, 9(2): 1339–1353.

[16] Pan Yanjun, Xu Ziqi, Li Ming, et al. Man-in-the-middle attack resistant secret key generation via channel randomization[C]//Proceedings of the Twenty-Second Interna-

tional Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing.New York:ACM,2021:231–240.

[17] Mamandi V,Ardalani N,Ghalamkari B.A new attack resistant encryption method based on hybrid chaotic-quantum key distribution(CQKD)[J].Quantum Information Processing,2024,23(7):265.

[18] Mitra S, Das S, Kule M. Prevention of the man-in-the-middle attack on diffie–Hellman key exchange algorithm: A review[M]//Proceedings of International Conference on Frontiers in Computing and Systems. Singapore: Springer Singapore,2020:625–635.

[19] Jackson J, Perumal R. An algebraic attack on the key exchange protocol based upon a modified tropical structure [J].Information and Computation,2025,303:105259.

[20] Xia Yuxin, Zhang Jie, Man K L, et al. Handover authenticated key exchange for multi-access edge computing[J]. Journal of Network and Computer Applications,2025,234: 104071.

[21] Li Sensen,Zhang Tikui,Yu Bin,et al.A provably secure and practical PUF-based end-to-end mutual authentication and key exchange protocol for IoT[J]. IEEE Sensors Journal, 2021,21(4):5487–5501.

[22] Ravi P,Bhasin S,Roy S S,et al.On exploiting message leakage in (few) NIST PQC candidates for practical message recovery attacks[J].IEEE Transactions on Information Forensics and Security,2021,17:684–699.

[23] Castryck W, Decru T. An efficient key recovery attack on SIDH[M]//Advances in Cryptology—EUROCRYPT 2023. Cham:Springer Nature Switzerland,2023:423–447.

[24] Guo Qian, Johansson T, Nilsson A. A key-recovery timing attack on post-quantum primitives using the Fujisaki–Okamoto transformation and its application on FrodoKEM [M]//Advances in Cryptology—CRYPTO 2020.Cham: Springer International Publishing,2020:359–386.

[25] Al–Sudany S M, Asl–Araji A S, Saeed B M. FPGA-based multi-core mips processor design[J]. Iraqi Journal of Computers,Communications, Control and Systems Engineering, 2021,21(2):16–35.

[26] Li Wanwu, Liu Lin, Zhang Jixian, et al. Multi-core parallel architecture design and experiment for deep learning model training[J].Multimedia Tools and Applications,2022,81(8): 11587–11604.

[27] Reddy S K, Ahmed S M, Manohar K. Improving performance & power in multicore processors[J]. Journal of Cloud Computing and Data Base Management, 2023, 8(3): 119 –125.

[28] Sideris A, Sanida T, Dasygenis M. Hardware acceleration design of the SHA-3 for high throughput and low area on FPGA[J]. Journal of Cryptographic Engineering, 2024, 14 (2):193–205.

[29] Dong Jiankuo,Zheng Fangyu,Lin Jingqiang,et al.EC–ECC: Accelerating elliptic curve cryptography for edge computing on embedded GPU TX2[J].ACM Transactions on Embedded Computing Systems,2022,21(2):1–25.

[30] Feng Zonghao, Xie Qipeng, Luo Qiong, et al. Accelerating elliptic curve digital signature algorithms on GPUs[C]// Proceedings of the SC22: International Conference for High Performance Computing, Networking, Storage and Analysis.Dallas:IEEE,2022:1–13.

[31] Li Xupeng,Li Xuheng,Dall C,et al.Design and verification of the arm confidential compute architecture[C]//Proceedings of 16th USENIX Symposium on Operating Systems Design and Implementation(OSDI'22).Carlsbad:USENIX, 2022:465–484.

[32] Reagen B, Choi W S, Ko Y, et al. Cheetah: Optimizing and accelerating homomorphic encryption for private inference [C]//Proceedings of the 2021 IEEE International Symposium on High-Performance Computer Architecture(HPCA).Seoul:IEEE,2021:26–39.

[33] Lu Wenjie, Huang Zhicong, Hong Cheng, et al. PEGASUS: Bridging polynomial and non-polynomial evaluations in homomorphic encryption[C]//Proceedings of the 2021 IEEE Symposium on Security and Privacy(SP). San Francisco: IEEE,2021:1057–1073.

[34] Lu Yibiao, Wu Zecheng, Zhang Bingsheng, et al. Efficient secure computation from SM series cryptography[J]. Wireless Communications and Mobile Computing, 2023, 2023: 6039034.

[35] Li Fengyin,Liu Zhongxing,Li Tao,et al.Privacy-aware PKI model with strong forward security[J]. International Journal of Intelligent Systems,2022,37(12):10049–10065.

[36] Aboubakar M, Kellil M, Roux P. A review of IoT network management: Current status and perspectives[J]. Journal of King Saud University–Computer and Information Sciences, 2022,34(7):4163–4176.

[37] Amiri H, Shahbahrami A. SIMD programming using Intel vector extensions[J]. Journal of Parallel and Distributed Computing,2020,135:83–100.

[38] Alharbi H A, Elgorashi T E H, Elmirghani J M H. Energy efficient virtual machines placement over cloud-fog network architecture[J].IEEE Access,2020,8:94697–94718.

[39] Aalam Z, Kumar V, Gour S. A review paper on hypervisor and virtual machine security[J].Journal of Physics:Conference Series,2021,1950(1):012027.

[40] Jin Ling, Cao Yinzhi, Chen Yan, et al. ExGen: Cross-platform,

automated exploit generation for smart contract vulnerabilities[J].IEEE Transactions on Dependable and Secure Computing,2023,20(1):650–664.

[41] Kannengießer N, Lins S, Sander C, et al. Challenges and common solutions in smart contract development[J]. IEEE Transactions on Software Engineering,2022,48(11):4291–4318.

[42] Albert E, Gordillo P, Rubio A, et al. Synthesis of super-optimized smart contracts using max-SMT[M]//Computer Aided Verification.Cham:Springer International Publishing, 2020:177–200.

[43] Ma Fuchen, Ren Meng, Fu Ying, et al. Security reinforcement for ethereum virtual machine[J].Information Processing & Management,2021,58(4):102565.

[44] Lakhan A, Mohammed M A, Rashid A N, et al. Smart-contract aware ethereum and client-fog-cloud healthcare system[J].Sensors,2021,21(12):4093.

[45] Fu Ying, Ren Meng, Ma Fuchen, et al. EVMFuzz: Differential fuzz testing of Ethereum virtual machine[J].Journal of Software:Evolution and Process,2024,36(4):e2556.

张小松，高端人才特聘教授，博士生导师，中国计算机学会会士，中国通信学会会士，中国电子学会会士。牵头获得国家科技进步奖一等奖和二等奖各1项，国家重点研发计划首席科学家。电子科技大学网络空间安全学院院长、信息与软件工程学院院长，数字经济智能与安全川渝共建重点实验室（四川）主任，区块链安全与平台技术教育部工程研究中心主任。获2021年四川省“两优一先”优秀共产党员称号、2020年第二届“全国创新争先奖”、2017年国家“网络安全优秀人才奖”、2022年第三届“四川省杰出人才奖”、2024年首届“全国科创名匠”称号、2024年第六届杰出工程师奖，入选天府万人计划杰出科学家。

Research Framework and Anticipated Results of Key Technologies for Distributed Certificate-less Network Identity Systems

ZHANG Xiaosong[1,2], *CAO Sheng*[1*], *LU Tianbo*[3], *YANG Kun*[4,5], *GUI Xun*[1], *XIE Guotao*[6], *NIU Weina*[1]

(1.School of Computer Science and Engineering (School of Cyber Security), University of Electronic Science and Technology of China, Chengdu 611731, China;
2.Shenzhen Institute for Advanced Study, University of Electronic Science and Technology of China, Shenzhen 518110, China;
3.School of Computer Science (National Pilot Software Engineering School), Beijing University of Posts and Telecommunications, Beijing 100876, China;
4.The State Key Laboratory of Blockchain and Data Security, Zhejiang University, Hangzhou 310007, China;
5.School of Cyber Science and Technology, Zhejiang University, Hangzhou 310007, China;
6.China Information Telecommunication Design & Consulting Institute Company Limited, Beijing 100080, China)

Abstract:

Significance Due to the continuous evolution and deepening of the Internet of everything, the scale of digital businesses such as the industrial Internet, energy Internet, and vehicular Internet continues to expand, as various software and hardware devices and systems become increasingly intelligent and complex. Traditional centralized identity authentication methods face increasingly prominent performance and security threats, while there remains a significant lack of technologies and platforms suitable for certificate-less distributed network identity authentication. In this context, this research focuses on the key technologies of certificate-less distributed network identity authentication to address issues such as secure and efficient key system management, hardware-accelerated authentication for massive access, and parallel optimization of smart contract execution, effectively responding to the severe challenges in network identity authentication. The research outcomes hold considerable importance and value for scientific research, technological development, and industrial promotion and application in the field of network identity authentication within certificate-less distributed environments. They not only improve the security and efficiency of digital identities but also provide robust support for the high-quality and secure development of the national digital economy, underpinning major strategic implementations in cyberspace security and governance. Future reliance on a comprehensive platform for large-scale IoT identity authentication based on domestic chips, targeting enterprises and institutions across industries, enables the promotion and application of platform products and distributed identity authentication services, directly and indirectly supporting annual transaction volumes of tens of billions in various internet businesses.

Progress This research adopted a comprehensive technical route of authentication architecture design, efficient key management, access process acceleration, parallel execution of smart contracts, and demonstration application, and systematically studied the key technologies of certificate-less distributed network identity authentication. The study focused on three fundamental scientific challenges in certificate-less distributed network identity authentication: secure and efficient key system management, hardware-accelerated authentication for large-scale access, and parallel optimization of smart contract execution. It explored five key research directions: high-performance certificate-less network identity authentication technologies and architectures, certificate-less distributed key management, hardware-enhanced high-parallel distributed terminal access, multi-level parallelized smart contract virtual machines, and large-scale distributed IoT identity authentication applications and validation. The study

aimed to achieve breakthroughs in ten critical technologies, including high-performance distributed identity marking and consensus mechanisms, certificate-less identity authentication protocol families and network architectures, smart contract-based automated certificate-less key management, attack-resistant distributed key generation, distribution, and revocation, intrinsically secure high-performance hardware layer construction, integrated hardware acceleration for secure cross-domain access of heterogeneous terminals, smart contract parallel co-processing architectures, optimized scheduling for smart contract virtual machines, lightweight certificate-less public key identification frameworks, and IoT identity management based on national cryptographic standards. In addition, the research developed five core systems and tools: a comprehensive digital identity management system, a full-lifecycle key management system, a hardware-enhanced high-performance concurrent terminal access system, a smart contract co-processor system based on domestic chips, and a large-scale distributed digital identity system evaluation and testing tool. Targeting network identity authentication scenarios in certificate-less distributed environments for industrial applications such as the energy IoT and vehicular IoT, the study aimed to establish a large-scale distributed IoT identity authentication platform that integrated national cryptographic standards and IoT identity authentication mechanisms to ensure trusted device identities, secure access, and robust security management. The project made significant progress across five key research areas. In high-performance certificate-less network identity authentication technology and architecture, a distributed certificate-less authentication framework, a lightweight attack-resistant consensus mechanism, and a cross-domain hierarchical authentication model were designed. In certificate-less distributed key management, smart contract-based key management schemes and multi-party attack-resistant key agreement protocols were developed, achieving breakthroughs in distributed key generation and anonymous secure data transmission. In hardware-enhanced high-parallel distributed terminal access, optimized acceleration schemes for IoT nodes and secure integration of heterogeneous terminals were designed, achieving authentication hash computing speeds of up to 200 Gbit/s and IoT authentication traffic handling of up to 100 Gbit/s. In multi-level parallel smart contract virtual machines, a co-processing architecture was developed, overcoming challenges in vector instruction set design and memory management, which led to the implementation of a smart contract co-processor on domestic chips. Lastly, in large-scale distributed IoT identity authentication applications and validation, a lightweight public key identification model based on national cryptographic standards was designed, achieving breakthroughs in GBA protocol integration and AI-driven certificate-less authentication, with evaluation tools developed to simulate IoT networks with at least 300 nodes.

Conclusions and Prospects This research aims to address challenges such as the design of authentication architectures, efficient key management, acceleration of access processes, and parallel execution of contracts, ensuring functionalities such as data allocation on demand and anonymous identity verification, while guaranteeing user privacy, security, and supporting dynamic collaborative computing for massive terminals. This project provides theoretical models and technical methods for digital identity authentication that are suitable for large-scale IoT identity authentication by constructing a high-performance hardware layer and developing multi-level smart contract virtual machines. The research introduces four key innovations: a distributed certificate-less identity authentication framework, a resilient and attack-resistant distributed key management system, hardware-enhanced integrated acceleration for large-scale heterogeneous terminal authentication, and a multi-level parallel smart contract virtual machine co-processing technology optimized for domestic hardware acceleration. The research not only helps mitigate risks associated with centralized management but also supports the development of the national digital economy, serving identity authentication needs in various sectors such as industry, energy, and vehicular networks, promoting the construction of a community of shared future in cyberspace.

Key words: cyberspace security; blockchain; certificate-less; key management; hardware enhancement; parallel processing; identity authentication

（编辑　赵　婧）

引用格式: Zhang Xiaosong,Cao Sheng,Lu Tianbo,et al.Research framework and anticipated results of key technologies for distributed certificate-less network identity systems[J].Advanced Engineering Sciences,2025,57(3):1–10.[张小松,曹晟,陆天波,等.分布式无证书网络身份系统的关键技术研究构想和成果展望[J].工程科学与技术,2025,57(3):1–10.]