区块链中的公钥密码:设计、分析、密评与展望

黄 可 李 雄 袁 晟 刘星宇 张小松

(电子科技大学计算机科学与工程学院(网络空间安全学院) 成都 611731)

摘 要 比特币的成功,吸引了人们研究区块链、加密货币以及相关的公钥密码算法的兴趣.然而,将公钥密码算法成功应用于新的加密货币设计,仍然面临很多挑战.一方面,设计适用于区块链的公钥密码算法并非易事,这是因为区块链具有独特的结构和应用环境,对密码算法提出了严苛的要求,如短签名长度、无需可信第三方等.随着区块链向多功能发展,需要考虑更多需求和功能.其中,安全性、隐私性和去中心化这三个问题涉及"三元悖论",同时解决两个或更多问题通常较为困难.当前的研究文献主要关注区块链技术及其原理,对相关密码算法的系统调研和分析不足.为了帮助读者了解和逐步掌握公钥密码算法设计的技巧和经验,并填补相关调研文献的空白,本文对相关密码算法的现状与研究进行了系统而深入的调研.通过 8 个案例、2 个通用构造以及相关证明技巧的讨论,本文为读者提供了由易到难的算法设计教程和相关经验.此外,本文还探讨了商用密码应用与安全性评估(简称"密评")相关的概念和研究,以促进区块链相关密码技术按照国家技术标准的要求进行实际应用.最后,本文对相关密码算法的设计难点进行了系统总结,并展望了未来的研究热点和具有挑战性的问题.

关键词 区块链;公钥密码算法;算法设计;复杂性分析;密评

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2024.00491

Public-Key Cryptography in Blockchain: Design, Analysis, Assessment and Prospect

HUANG Ke LI Xiong YUAN Sheng LIU Xing-Yu ZHANG Xiao-Song

(*College of Computer Science and Engineering (College of Cyber Security), University of Electronic Science and Technology of China, Chengdu* 611731)

Abstract The rapid ascent of cryptocurrencies has ignited a surge in interest among researchers worldwide, propelling them into the intricate realm of Public-Key Cryptography (PKC). While mathematical theories serve as a sturdy framework for the study of PKC, their mastery demands a substantial level of expertise. Furthermore, blockchain technology introduces a set of exacting criteria that underpin the design and execution of PKC algorithms, including the need for concise outputs and trustless setups. Additionally, modern blockchains grapple with an expanding array of considerations, notably the Trilemma encompassing security, privacy, and decentralization. The endeavor to address multiple challenges within a single solution presents an enduring challenge. Existing research predominantly gravitates toward elucidating the fundamental concepts and principles of pertinent techniques, often neglecting a systematic and in-depth exploration of the core design and analysis of PKC algorithms. This paper seeks to rectify this gap, aiming to consolidate the essential techniques and insights associated with designing and analyzing PKC algorithms for blockchain applications. It embarks on a comprehensive and meticulous examination

收稿日期:2023-02-25;在线发布日期:2024-01-04.本课题得到国家自然科学基金(62002048,62332018,U19A2066,62072078,U22B2029)、四川省应用基础研究(2022NSFSC0876)、国家电网有限公司总部科技项目(5700-202355311A-1-1-ZN)、成都交子金控集团区块链研究院的资助.**黄 可**,博士,副教授,主要研究方向为公钥密码学、区块链等.E-mail:huangke@uestc.edu.cn.**李 雄**(通信作者),博士,教授,主要研究领域为数据安全和隐私计算.E-mail:lixiong@uestc.edu.cn.**袁 晟**,硕士研究生,主要研究方向为卫星互联网和应用密码学.**刘星宇**,硕士研究生,主要研究方向为软件安全和应用密码学.**张小松**,博士,教授,主要研究领域为区块链安全、人工智能安全等.

of the present state and ongoing advancements in cryptographic algorithms relevant to the field. In pursuit of this objective, we present eight cryptographic schemes as use cases, providing an insightful exploration of their intricacies. Additionally, we delve into two generic methods for practical designs, offering a roadmap for those engaged in the practical implementation of PKC algorithms within blockchain systems. To elucidate these design choices and methodologies, we scrutinize and evaluate proving techniques through concrete examples, enabling a clearer understanding of their practical implications. Moreover, this article navigates through the labyrinth of concepts and research related to security evaluation. A nuanced exploration of security assessment methods and practices is crucial in fostering the robust and secure application of blockchain-based cryptographic technology, aligning with national technical standards. By shedding light on these considerations, we hope to facilitate the seamless integration and utilization of cryptographic solutions within blockchain ecosystems. In conclusion, this paper underscores the pressing need for a more comprehensive and systematic approach to PKC algorithm design and analysis in the context of blockchain technology. As a parting note, we outline the foreseeable challenges and avenues for further exploration, emphasizing the dynamic and evolving nature of this field. As we venture into the future, the fusion of PKC and blockchain promises to shape the landscape of digital security and decentralized trust in unprecedented ways, forging new frontiers in cryptographic innovation.

Keywords blockchain; public-key cryptography; algorithm design; complexity analysis; security evaluation

1 引 言

自中本聪[1]于 2008 年提出比特币的概念以来，加密货币经历了快速的发展. 作为目前最成功的加密货币，比特币在全球加密货币市场中处于主导地位. 在过去的十多年间，越来越多的研究者和科技工作者参与到加密货币的研究与应用中. 作为比特币的核心技术，区块链技术获得了深入的研究和广泛的应用. 具有代表性的加密货币有：比特币[1]、以太币[2]、莱特币、达世币、门罗币、零币[3]、零钞[4].

区块链本质上是一条由哈希函数将多个区块联系在一起的链式结构，其中每一个区块中都包含了多条通过数字签名认证的交易数据. 由于区块链的核心功能依赖于底层密码技术(尤其是安全性，见第 3.1 节)，对相关密码算法的研究和分析变得尤为重要. 密码学是主要研究通信保密的学科. Diffie 和 Hellman[5]在 1976 年正式提出了公钥密码体制，并由此开启了公钥密码学的纪元. 公钥密码体制与最初基于替换和置换的对称密码体制完全不同，它基于数学函数且使用了两个独立的密钥. 在过去的四十多年时间里，研究者对数字签名[6]、公钥加密[7]、零知识证明[8]等多种公钥密码算法[9-11]开展了广泛和深入的研究. 由于许多公钥密码算法建立在特定的数学模型和困难问题猜想下，相关研究与分析需要借助科学的基础理论和严格的数学分析手段，主要包括计算复杂性理论[12](见第 2.4 节)和可证明安全理论[6](见第 2.4 节). 前者提供了一套数学范式和方法，用于评估算法的最大执行开销，后者提供了一套研究与 NP(非确定性多项式)难题相关的算法安全性的方法. 图 1 展示了不受认可和受认可的安全算法设计思路. 其中受认可的思路主要使用“归约”(见第 2.5 节)的方式来证明公钥密码算法的安

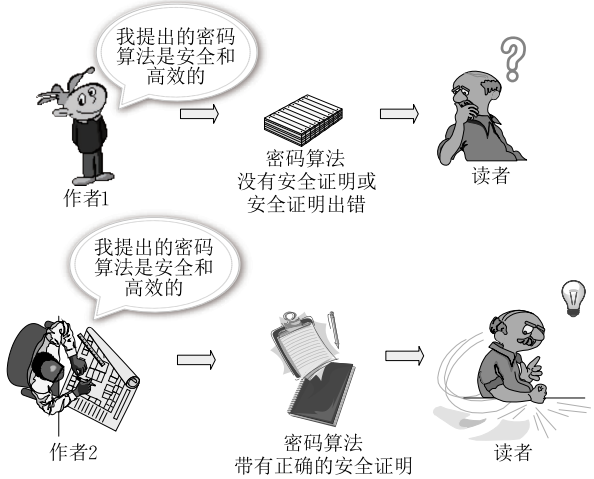

图 1 不受认可(上)的和受认可(下)的安全算法设计思路

全性.

目前，现实应用对加密货币提出了越来越多的功能和安全需求，而公钥密码算法则是实现这些新需求的重要工具[13-14]. 以隐私保护功能为例，非交互式的零知识证明[9]被用于设计零币的匿名支付功能[3]，环签名算法被应用于设计门罗币的匿名支付协议，例如 RingCT[15]（Ring Confidential Transaction，环机密交易）、RingCT 2.0[16]和RingCT 3.0[17]协议. 针对不断升级的网络安全威胁，如勒索病毒、数据泄露、系统漏洞等，用户倾向于选择更安全和隐私更有保障的加密货币. 同时，新的安全和应用功能也能够帮助区块链更快地吸引用户和投资[18].

然而，设计者如何才能证明所使用的密码算法是安全的？类似的，这也需要借助相关的基础理论和分析手段. 特别地，相较于传统的中心化密码应用（如 SSL/TLS 协议中的密码应用），以区块链为代表的去中心化应用通常对其底层的公钥密码算法提出严苛的性能要求[19]，比如短的签名长度、高效的签名验证等（见第 3.3 节）. 因此，更需要在算法设计过程中精心地谋划和慎重地权衡. 图 2 给出了相关的算法、理论、产品与技术之间的关系. 通常，面向区块链安全的算法设计的具体步骤如图 3 所示，步骤包括如下：

（1）明确动机. 首先，明确算法在区块链中的具体应用场景. 比如，对链上数据进行加密或者认证，需要设计相应的加密算法或签名算法，以保障数据的机密性或完整性，明确基本的设计需求.

（2）建立目标. 进一步提出具体的算法需求，包括安全性、功能性和性能需求等. 围绕上述需求，建立安全和威胁模型，构造算法的黑盒设计. 例如，算法大致分为几个子算法，每个子算法包含的参数及

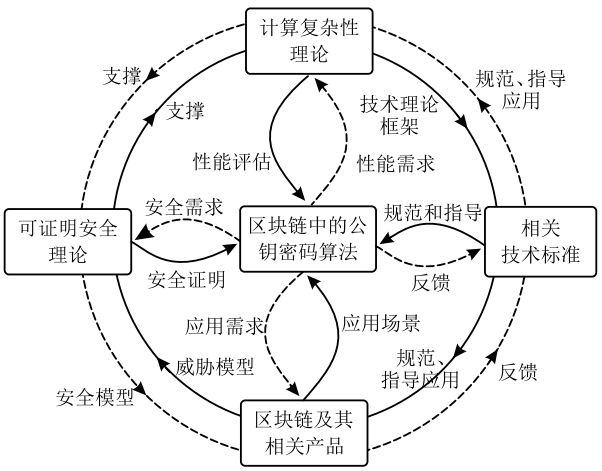

图 2　算法、理论、产品与技术的关系

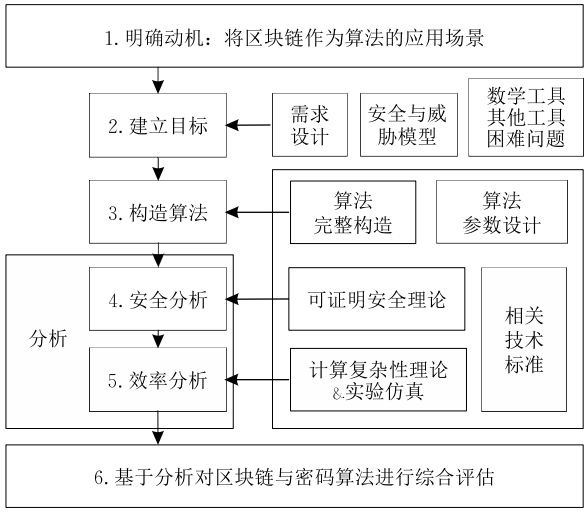

图 3　设计与分析密码算法的步骤

含义等. 此外，给出算法所依赖的数学困难问题和工具.

（3）构造算法. 基于上述目标，进一步开展算法的具体构造，包括安全参数的选取、具体群组的选取等. 还包括算法的每一步输入和输出对应的具体参数. 构造算法的过程中通常会引入特殊的数学符号，而这些数学语言通常与步骤（2）中所选取的困难问题相对应.

（4）安全分析. 基于可证明安全理论，结合安全模型、威胁模型和算法具体构造，开展安全归约，将算法的安全性归约到相关的数学困难问题的求解上来. 对敌手攻破算法以及求解相关困难问题的概率进行分析，实现高效的归约（见第 2.5 节）. 此外，还可以参考相关技术标准（见第 7.2 节）来评估密码算法.

（5）效率分析. 基于计算复杂性理论，对算法开展复杂性分析. 同时，可以借助软件或者硬件，对算法开展仿真实验，测试算法的实际性能. 此外，还可以参考相关技术标准（见第 7.2 节）来评估密码算法.

（6）综合评估. 基于步骤（4）和（5）的结果，对算法的实用性进行评估. 最后，总结所设计算法的实用性. 若未达到预期的效果，可以重复步骤（1）～（5）.

1.1　相关的研究

当前的调研文献主要聚焦区块链涉及的技术和原理，缺乏对相关密码算法设计的系统调研与“阶梯式”的教程.

蔡晓晴等人在文献[20]中重点调研了区块链及其相关技术的研究现状. 单进勇与高胜在文献[21]中总结了区块链技术的研究方向与现状. 刘明达等人在文献[22]中分析了区块链在数据机密性、完整

性和可用性方面的研究成果. 祝烈煌等人在文献[23]中主要探讨了区块链涉及的隐私保护技术. Conti 等人[24]以及 Zhang 等人[25]分别对比特币的安全和隐私问题进行了调研,并对比特币密码技术进行了分析. 此外,还有一系列的文献[26-27]从不同角度对区块链进行了研究调查.

需要注意的是,李威翰等人[28]对 zk-SNARK 进行了系统和深入的调研,并总结了相关的热点和研究方向. 然而,该文献主要关注非交互式零知识证明[29],并未聚焦区块链或零知识证明以外的密码算法. 赵臻等人[30]介绍了公钥密码方案构造和安全证明的关键知识点和方法,然而,该文献并未重点涉及与区块链相关的密码方案及前沿研究.

综上,目前缺乏一篇文献聚焦区块链中相关的密码算法,特别是围绕算法设计与分析的角度给出案例分析. 本文致力于填补该类调研文献的空缺,通过调研与分析,为读者提供相关密码算法的设计思路与经验.

本文使用的简写[1,15,29,31-44]及其含义对照表如表 1 所示.

表 1 本文涉及的简写及其含义对照表

简写	全称	中文含义
CRS[29](或者 crs)	Common Reference String	公共参考字符串
ECDLP[31]	Elliptic Curve Discrete Logarithm Problem	椭圆曲线上的离散对数问题
ECDSA[31]	Elliptic Curve Digital Signature Algorithm	椭圆曲线数字签名算法
EU-CMA[31-32]	Existential Unforgeability against Chosen Message Attack	选择消息攻击下的存在性不可伪造
IND-CCA1[33]	Indistinguishability under Chosen Ciphertext Attack	选择密文攻击下的不可区分性
IND-CCA2[34]	Indistinguishability under Adaptive Chosen Ciphertext Attack	适应性选择密文攻击下不可区分性
IND-CPA[35]	Indistinguishability under Chosen Plaintext Attack	选择明文攻击下的不可区分性
MAC[36]	Message Authentication Code	消息认证码
NIZK[29]	Non-Interactive Zero-Knowledge	非交互式零知识证明
PoW[1]	Proof of Work	工作量证明
QAP[37]	Quadratic Arithmetic Program	二次算数程序
R1CS[38]	Rank-1 Constraint System	一阶约束系统
RingCT[15]	Ring Confidential Transaction	环机密交易
ROM[39]	Random Oracle Model	随机预言机
UHP[40]	Universal Hash Proof	通用哈希证明
UTXO[41]	Unspent Transaction Output	未花费的交易输出
ZKP[8]	Zero-Knowledge Proof	零知识证明
zk-SNARK[42-43]	Zero-Knowledge Succinct Non-Interactive Argument of Knowledge	简短非交互式零知识论据
zk-STARK[44]	Zero-Knowledge Scalable Transparent Argument of Knowledge	零知识可扩展透明知识证明

1.2 面临的挑战

虽然遵循上述设计和分析密码算法的 6 个步骤可以有针对性地设计相关算法,但是该设计过程并非一帆风顺. 主要的挑战存在于上述步骤(1)~(4),具体原因列举如下:

挑战 1. 寻找合适的设计出发点:虽然早期的区块链采用了一些高效或简单的签名设计,如 ECDSA[31](Elliptic Curve Digital Signature Algorithm)或 BLS[32](Boneh-Lynn-Shacham),但随着区块链朝着多样化功能发展,其算法设计和应用变得更加复杂. 一个典型的例子是在零钞[4]中使用构造复杂的简短非交互式零知识论据[4](zero-knowledge Succinct Non-interactive Argument of Knowledge,zk-SNARK)实现匿名支付. 此外,提升现有算法的安全性通常也会引入复杂的构造,例如将公钥加密算法的安全性提升至 IND-CCA2(Indistinguishability under Adaptive Chosen Ciphertext Attack,见第 5.4 节)安全. 因此,有针对性地选择适用于区块链场景的课题或进行算法设计变得尤为重要. 这样的选择有助于避免由于选题失误而导致前期工作的白白浪费.

挑战 2. 尽可能确立理想且可达的安全目标:由于新的网络安全攻击方式层出不穷,并且设备存在的异构性等问题,分析和检测新的安全攻击并非易事. 一些侧信道攻击难以通过现有的密码框架进行完善的讨论. 部分理想的安全目标(如 IND-CCA2)未必能够在实际环境中得到应用. 因此,确立理想且可达的安全目标,并给出算法的黑盒设计是设计实用算法的必经之路.

挑战 3. 给出算法的具体构造:为了将理想的算法设计实例化,通常需要给出算法在某些数学困难问题下的具体构造. 在构造算法时,设计者通常会引入特殊的数学符号,而这些数学语言通常与困难问题相对应. 所依赖的困难问题不同,密码算法的构造也会完全不同. 相应地,其安全性归约所采用的证明

方法也会截然不同. 虽然设计者可能将两个经典算法的设计融合在一个方案中，但这在步骤 4 中也会遇到不小的挑战.

挑战 4. 给出高效和正确的归约：针对算法的具体构造与安全模型，开展正确和高效的安全归约并非易事，其中涉及诸多方法和技巧. 归约的成功开展取决于分析者的能力和经验. 针对归约的构造问题，Guo 等人在文献[45]中进行了系统的讲解. 对于长期从事密码设计与分析的研究者来说，安全归约的学习是一条必经之路，通常需要反复的练习和长期的坚持.

1.3　研究动机

本文致力于总结面向区块链的公钥密码算法的设计经验. 针对第 1.2 节列举的挑战 1～4，本文的研究动机罗列如下：

(1) 针对挑战 1，从加密货币面临的安全性、隐私性和可扩展性问题入手，为读者提供全面的区块链研究背景(详见第 3 节).

(2) 针对挑战 2，在第 4～6 节中分别给出相关算法的通用的安全模型、算法定义与构造方法，为读者提供基本的算法设计思路和经验. 第 7 节为算法的应用和落地提供指导.

(3) 针对挑战 3 和 4，通过在第 4～6 节中分别提供具体的案例分析，为读者提供可参考的算法案例，以及相应的安全归约方法.

(4) 最后，系统总结相关密码算法的设计经验，并展望未来的研究热点和挑战性问题.

1.4　主要的贡献

(1) 本文主要对区块链中涉及的相关密码算法进行了系统调研和分析，旨在帮助读者了解和掌握公钥密码算法的构造和分析的形式化方法.

(2) 本文旨在为读者提供以下内容：① 设计与分析面向区块链的密码算法的思路和所需的理论知识；② 相关密码算法的通用构造方法和逐步分析的案例研究，从简单的签名到复杂的零知识证明；③ 探索密码学与区块链的交叉研究点以及共性问题，揭示亟需突破的挑战性问题.

1.5　内容安排

本文的具体内容安排如下：第 2 节系统地回顾设计和分析区块链中的公钥密码算法所需的基础理论知识；第 3 节介绍当前加密货币和区块链的主要研究问题，这些问题是进行相关密码算法研究的动机和背景；第 4～6 节分别对公钥加密、签名和零知识证明进行系统介绍和案例分析；第 7 节介绍区块链与公钥密码算法有关的密评和研究工作；第 8 节对本文的调研内容进行总结，并展望未来的算法设计思路和问题.

2　基础知识和概念

2.1　区块链的定义

区块链通过哈希函数将多个区块按照先后顺序链接在一起. 其中，每一个区块中都包含了多条交易数据，每一条交易数据都通过数字签名进行认证. Garay 等人[46]对比特币的骨干协议进行了正式定义，在本文中我们沿用该定义. 设 $G(\cdot)$ 和 $H(\cdot)$ 为安全的哈希函数，其输出为 k 比特的 0,1 字符串. 设 $s\in\{0,1\}^{\kappa}$ 为链上某一区块的哈希值. $x\in\{0,1\}^{*}$ 代表区块的内容. $ctr\in N$ 代表一个寄存器. 用三元组 $B=\langle s,x,ctr\rangle$ 代表一个区块. 用 $validblock_q^D(B)$ 来表示判断区块 B 有效性的断言：

$$validblock_q^D(B)=H(ctr,G(x,s))<D\wedge(ctr\leq q) \tag{1}$$

如果满足 $validblock_q^D(B)=1$，则区块 B 为有效区块. 此外，需要满足哈希值的一致性：$s_{i+1}=H(ctr_i,G(s_i,x_i))$. 这里，参数 $D\in N$ 代表的是区块对应的挖矿难度值. $q\in N$ 代表的是寄存器 ctr 的边界值. 进一步的，定义最右边的区块为“链头”，将链头定义为 $head(C)$. 定义最左边的区块为创世区块. 为了将一个新的区块 $B=\langle s,x,ctr\rangle$ 添加到一条链头为 $head(C)=\langle s',x',ctr'\rangle$ 的链 C 后面，设添加后的新链为 $C_{\text{new}}=CB$. 需要满足下式：

$$head(\mathcal{C}_{\text{new}})=\mathcal{B},\ s=H(ctr',G(s',x')) \tag{2}$$

2.2　密码算法基础

数学基础. 数学是现代密码学的基础. 经过几十年的发展，我们现在能够利用不同的代数结构来构建公钥密码方案，例如基于环、群[47]、格[48]等的密码方案. 不同的代数结构对应着不同的数学基础难点. 密码学涉及到数论、近世代数、计算复杂度理论、信息论和概率论等多个数学理论. 这些理论在设计密码体制和协议时起着重要的作用.

在现代密码学中，经常会涉及到大整数分解、素性检测、求解平方根、求解同余式方程组等数论知识. 群、环和域是近世代数的研究重点，主要讨论由能进行代数运算的元素组成的集合及其上的运算. 现代密码学的安全性基于计算复杂性理论模型，这类密码体制的安全性基于某些困难问题的假设. 这意味着一般的计算方法无法有效解决这类问题.

为了精确定义算法的有效性,图灵提出了一种通用的计算设备:图灵机.图灵机至今仍被广泛应用于计算复杂性理论的研究中.简单来说,图灵机是计算机的理想化数学模型,由一条无限长的磁带和一个读写头组成.一个问题的计算复杂性取决于解决该问题的算法的计算复杂性.由于解决一个问题可能有多个算法,它们的计算复杂性各不相同,因此理论上将一个问题的计算复杂性定义为解决该问题的最有效算法的计算复杂性.

算法的定义.算法一般包含了一系列步骤,用于实现特定的安全服务.每一个算法通过一个或多个步骤,从给定的输入计算得到一个输出.这里,密码算法可以分为确定性和非确定性密码算法.前者指对于同一个输入,总是返回相同的输出.后者指对于同一个输入,总是产生不同的输出.

用(t,ϵ)来表示算法基于给定的输入在时间t内产生输出的概率为ϵ.ϵ可以用于表示概率或者优势.这两个概念在不同的讨论情形下代表不同的含义.比如,当对一个算法输出的结果进行讨论(或者用于和另一算法进行比较时),ϵ代表的是优势,否则,它用于表示概率.

$t(\lambda)$指的是函数t以安全参数λ作为输入.用λ来表示密码原语的安全参数,比如加密算法中的加密密钥的长度.称$t(\lambda)$为一个多项式函数,当且仅当$t(\lambda)=\mathcal{O}(\lambda^{n_0})$且$n_0>0$.进一步地,称$\epsilon(\lambda)=\frac{1}{\mathcal{O}(\lambda^{n_0})}$是不可忽略的优势,当且仅当$n_0>0$.

基于上述,我们正式定义一个安全的公钥密码算法如下:如果敌手不能够以不可忽略的优势(即$\epsilon(\lambda)=\frac{1}{\mathcal{O}(\lambda^{n_0})}$)在多项式时间内(即$t(\lambda)=\mathcal{O}(\lambda^{n_0})$,$n_0>0$)以及安全参数$\lambda$下攻破该方案,那么我们认为该方案是安全的.进一步地,我们说一个(t,ϵ)算法能够在多项式时间t内以不可忽略的优势ϵ和λ攻破一个方案(或者一个公开的数学困难问题),我们称它为一个破解相关密码算法的有效算法.

为了证明算法是安全的,我们需要构造一个归约将对目标方案的破解归约到困难问题的求解上.换言之,为了构造这样一个归约,我们通常从一个用于破解目标方案的算法入手.然而,由于困难问题的假设,这样一个高效的算法是不存在的.这样一来,就可以顺理成章地将破解目标方案归约到困难问题的求解上来,以此完成对目标方案的安全性证明.详见第 2.4 节.

分析密码的思路.根据柯克霍夫斯(Kerckhoffs)原则[①],评估一个密码算法的安全性时,必须假设攻击者不知道密钥,但知道密码算法的所有细节.换言之,密码算法的安全性应该基于密钥的保密,而不是所用算法的隐蔽性.密码算法分析的目的是通过各种攻击方式找到密码算法的弱点或者不完美的地方.

以加密算法为例,按照攻击者获取信息的能力,可以将密码分析划分为唯密文攻击、已知明文攻击、选择明文攻击和选择密文攻击四种方式.公钥密码的设计一般依赖于计算困难的数学问题.公钥密码的设计一般都可以做到可证明安全,即证明了如果底层的数学问题是困难的,上层的公钥密码方案也是安全的.因此,对公钥密码分析多集中于对底层困难问题的分析,以及上层方案实际安全性的分析.

在本文中,我们侧重于基于计算复杂性理论(见第 2.3 节)和可证明安全理论(见第 2.4 节)对公钥密码算法进行分析,并辅以密评技术(见第 7 节)作为补充.

2.3 计算复杂性理论

例如,假设一个算法为A,λ为该算法的安全参数.我们说执行算法A的时间受限于$O(\lambda)$,即执行算法A的最坏时间被定义为$O(\lambda)$.相应地,上述说法也可以用于空间和存储复杂性的定义中.基于上述定义,可以进一步开展形式化的算法性能分析[49].

在衡量算法的计算复杂性时,往往不需要表示出影响算法复杂性的常系数.为了便于阅读,我们可以使用基于阶数的符号来表达算法的复杂性.

定义 1. 阶数符号:设$f(n)$,$g(n)$为函数,$c>0$为常数,N为一个自然数.如果对于所有$n\geq N$,存在c和N使得$|g(n)|\leq c|f(n)|$成立,我们可以用$\mathcal{O}(f(n))$来表示函数$g(n)$的渐进上界复杂度.

有关计算复杂性理论的其他基本概念还包括确定型图灵机和随机存储机,以及一些困难问题的程序设计方法,如贪心法和背包问题.读者可以通过相关教材和在线学习资源深入了解这些内容.

计算难度和可解性.证明一个算法是在某个问题上最有效的求解算法是非常困难的.因此,在实际应用中,我们通常将可计算的问题粗略地分为三类:

(1)P 类问题(Polynomial Time,确定性多项式时间可解类)指那些可以在多项式时间内解决的问题的集合,又称为易解问题.

① http://accu.cc/content/cryptography/kerckhoffs_principle/

(2) NP 类问题(Nondeterministic Polynomial Time，非确定性多项式时间可解类)指那些可以在多项式时间内验证一个解的问题的集合. 如果给定一个解，可以在多项式时间内验证这个解的正确性，但不一定能在多项式时间内找到解，又称为难解问题.

(3) NP 完全类问题(NP-Complete，非确定性多项式时间可解完全类)指同时属于 NP 类并且被认为是 NP 类中最难的问题的集合. NP 完全类问题具有两个性质：① 它属于 NP 类，即可以在多项式时间内验证一个解；② 所有属于 NP 类的问题都可以在多项式时间内归约到它. NP 完全类问题又称为困难问题.

Cook[50] 和 Karp[51] 奠定了 NP 完全理论的基础. NP 完全理论的目标不是寻找解决 NP 完全类问题的算法，而是关注证明这类问题的等价性，即证明它们的难度相当. 目前，NP 类问题是否等价于 P 类问题仍然是本世纪最重要的数学问题之一. 本文中，我们将计算问题粗略地分为简单问题和困难问题两大类，而不严格区分“难解问题”和“困难问题”这两种说法. 密码方案的构造和安全归约证明(见第 2.5 节)与简单问题密切相关，而方案的安全性与困难问题密切相关. 简单问题是指可以在多项式时间内解决的计算问题，而困难问题是指无法在多项式时间内解决的计算问题[29].

计算模型与安全模型的考虑. 计算模型和安全模型的选择为设计实用且安全的密码方案提供了框架和背景. 评估密码方案的安全性有多种标准，包括无条件安全性、计算安全性和可证明安全性(见第 2.4 节). 无条件安全性指的是即使攻击者拥有无限的计算能力和资源，也无法通过计算来破解密码方案. 然而，实现无条件安全性非常困难，通常需要高昂的计算和通信成本. 计算安全性指的是在现实世界的有限计算资源下，密码方案仍然能够保持安全，通常基于某些数学问题的计算难度，例如大素数的快速分解问题. 可证明安全性建立在严格的数学模型和证明技术上，通过数学证明来验证密码方案的安全性，具有强大的安全性保证.

为了达到特定的安全目标，通常需要借助安全模型提供的统一框架和指导进行算法设计和分析. 在安全模型下对敌手进行建模时，需要在计算模型的指导下构建威胁模型. 计算模型定义了对攻击者计算资源的限制，威胁模型定义了攻击者发动攻击的能力. 通常情况下，攻击者的计算能力、存储能力和通信能力是有限的. 现代密码学将算法的安全性构建在计算复杂性理论模型中，依赖于公开的困难问题的难解性. 这里的难解性指的是通过现有计算方法或手段难以高效解决. 在实际应用中，通常将算法的计算安全性视为算法的安全性，即无论使用当前或未来的可用资源，算法都不能被破解.

然而，目前设备计算能力普遍不太强大的情况可能是短暂的. 随着量子计算机的发展，更强大的计算模型和设备出现，设备的并行计算能力可以指数级增长. 这可能导致基于现有计算复杂性理论模型和困难问题的密码方案变得不安全. 例如，使用量子计算机进行整数分解的开销可能接近使用现有计算设备进行整数乘法计算的开销，从而使基于 RSA 的密码系统不再安全.

因此，为了确保密码方案的安全性，需要考虑当前设备的计算能力，并使用适当的算法和参数来应对计算能力增强带来的风险. 同时，随着技术的进步，需要不断评估和更新密码方案，以适应未来计算能力的发展. 目前，量子计算机尚未广泛普及和应用，因此本文主要考虑设备计算能力相对较弱的情况. 通过传统的复杂性理论模型和方法，对现有的公钥密码算法进行研究和分析.

2.4　可证明安全理论

可证明安全理论[45,52] 是密码方案安全性分析的重要方法. 它采用一种公理化的研究方法，旨在提供一种形式化和严格的方式来评估和证明密码系统、协议或算法的安全性. 可证明安全理论利用数学方法和逻辑推理，通过严谨的证明过程来确保系统在特定攻击模型下满足安全性要求. 该理论通常通过“归约”在给定的威胁模型和安全模型下证明方案能够达到特定的安全目标. 研究者通常借助基于矛盾和基于定理的证明方法来实现可证明安全. 此外，还将介绍两种不同的安全性分析框架：随机预言机模型和标准模型.

安全模型是可证明安全理论中的关键概念之一. Goldwasser 等人[6] 首次提出了可证明安全性的概念，其中包括两个关键名词：威胁模型和安全模型. 安全模型通常用于定义算法需要满足的安全目标，而威胁模型则用于定义敌手对算法发动攻击的能力. 安全模型是对特定密码概念的安全需求进行抽象定义的，不涉及具体密码方案. 它通过一个游戏(Game)的形式，让挑战者和敌手交互来描述现实世界中的攻击. 安全模型一般包括初始化、询问、攻击和优势四个部分. 初始化阶段是系统的初始化和参数分配，询问阶段允许敌手向挑战者提出问题，攻击

阶段是敌手试图攻破安全目标,优势是衡量敌手成功攻破方案或解决问题的概率.安全模型的强度取决于敌手的询问限制,限制越少则安全模型越强.在后续的章节中,将逐步介绍数字签名、公钥加密和零知识证明等常见密码概念的安全模型.这些安全模型包括敌手的攻击方式(即询问的内容和时间)以及挑战者的安全目标.其他密码概念的安全模型与这些密码概念的安全模型存在许多相似之处.

基于矛盾的证明方法.基于矛盾的证明方法是一种常见的数学证明方法,它通过假设待证明的命题为假,并从这一假设出发推导出矛盾的结论来证明原命题的真实性.具体而言,首先需要一个已知的公开困难问题.然后,假设敌手能够攻破目标密码算法.接着,通过归约来证明敌手的攻击可以被归约到对应困难问题的求解上.紧接着,可以基于攻击者攻破密码算法的概率(或优势)进一步推导出破解相关困难问题的概率(或优势),从而完成对密码算法的安全归约.基于矛盾的安全归约成立当且仅当我们可以在敌手的帮助下高效地解决密码算法对应的困难问题.如果在当前计算模型下,困难问题是简单的,或者我们无法构造困难问题的解,那么给出的归约就不能使得矛盾成立.换言之,该证明方法会失败.然而,没有矛盾的安全归约并不代表方案就是不安全或非可证明安全的,但这样的归约可能无法令人信服.基于矛盾的证明思路在逻辑上比较直观,是一种强有力的证明方法,在数学和逻辑推理中得到广泛应用.

基于定理的证明方法.基于定理的证明[53]是一种使用数学定理和推理规则来证明系统安全性的方法.它通过前置定义来陈述密码算法的安全性,是基于研究者经验知识的专家系统,并常用于对算法安全性进行建模和分析.这种方法提供了一种形式化和可验证的方式来评估和证明密码方案的安全性.该方法首先对密码算法进行正式化的定义,然后构造安全归约来对这个正式定义的算法进行分析.然而,这种证明方法缺乏对敌手模型(威胁模型)的完整定义,即缺乏对敌手所有恶意行为的刻画.此外,该方法只能刻画敌手的静态攻击行为,并且只能将算法作为黑盒来讨论.因此,基于定理的证明无法检测由于密码算法设计不合理所引起的缺陷.然而,由于该证明方法使用严格的数学推理和逻辑推导,执行快捷且可验证,可以减少人为错误和漏洞的存在,因此被广泛应用于安全证明中.

随机预言机模型[39](**Random Oracle Model, ROM**).ROM 为密码算法的分析提供基于询问的响应服务,是可证明安全理论的重要组成部分和理想工具.一个随机预言机 H 将 n 比特的字符串映射到 m 比特的字符串,并满足公开可访问性、随机性、不可预测性、机密性和一致性.对外部用户而言,ROM 的内部结构是不可知的,外部用户只能看到他们发出的询问以及收到的响应.在 1993 年,Bellare 和 Rogaway[39]对 ROM 的设计思想进行了总结和归纳.目前,绝大多数可证明安全的公钥密码算法是基于 ROM 模型设计的[54].具体而言,设计者首先需要设计基于 ROM 的密码算法,并针对该算法给出基于特定困难问题的安全归约.与此同时,需要假设 ROM 的存在,然后将 ROM 替换为标准的哈希函数 H',例如 SHA-256.

标准模型.哈希函数确实不能产生完全随机化的输出,因此无法确保密码算法在实际环境下的安全性.到目前为止,已经有一些在随机预言机模型下可证明安全但在实际应用中却不安全的方案[55-56].与随机预言机模型(ROM)不同,标准模型不依赖于类似 ROM 这样的理论假设.例如,在使用哈希函数时,标准模型的方案只利用了哈希函数的标准性质,如抗碰撞性,而不是随机性.因此,在设计密码算法的敌手模型时,敌手的攻击能力只受到计算时间和存储空间的限制.然而,设计标准模型下的密码算法是一项具有挑战性的工作.尽管标准模型下的方案可能面临构造复杂的困扰,但该模型下的密码算法具有更理想的安全性,并且其安全性更受到外界的信任[56-57].

2.5 安全证明方法

接下来,介绍两种实现安全性证明的主流方法:安全归约证明(Single Game)和 Game Hopping(Game Sequence).

方法 1. 安全归约:安全归约是将敌手对方案的攻击转化为一个困难问题实例的解的过程.通过构造模拟方案并与敌手进行交互,我们将困难问题嵌入到模拟方案中,使敌手的攻击成为解决困难问题的一部分.归约证明不是数学证明,而是提出一个归约算法,其正确性需要进行分析和验证.

归约证明的框架可以分为三个阶段:模拟、解决困难问题和分析.在模拟阶段,使用问题实例生成模拟方案,并与敌手进行交互.成功的模拟必须以不可忽略的概率发生.解决困难问题阶段是将敌手的攻击结果转化为困难问题实例的解.需要注意的是,敌手的攻击并非总能解决困难问题,这是常见的归约

证明错误. 最后，在分析阶段，需要证明如果敌手可以在多项式时间内攻破方案，那么我们构造的模拟方案也能在多项式时间内找到困难问题的解. 分析的重点是假设敌手具有无限计算能力[29].

如何构造安全归约. 归约证明的具体内容因密码概念、密码方案构造、安全模型和困难问题而异，但框架相似. 模拟、解决困难问题和分析是归约证明的核心步骤，共同确保方案的正确性. 通常来说，安全归约需要满足以下性质：

(1) 归约是高效和紧凑的[58-59]. 对于低效的归约而言，虽然归约算法的执行时间是多项式时间，但该归约算法并没有给困难问题的求解带来实际的优势. 对于紧凑的归约而言，攻击密码算法的执行开销在理论上接近或等同于对困难问题的求解.

(2) 对密码算法而言，其依赖的困难问题的数学假设应该越弱越好. 这是因为越弱的假设越容易通过实际和可行的密码构造来实现. 换言之，使用弱假设的密码系统相较于使用强假设的密码系统能够提供更强的安全性.

归约需要考虑的因素. 基于威胁模型和安全模型，我们可以将密码算法的安全性归约到已知困难问题的求解之上. 然而，在设计密码算法的具体构造时，设计者通常会引入特殊的数学符号，而这些数学语言通常与困难问题相对应(例如，Diffie-Hellman 四元组与判定性 Diffie-Hellman 猜想对应). 依赖于不同的困难问题，密码算法的构造会完全不同，所采用的归约方法也会截然不同. 那么如何正确地构造安全归约呢？要系统地回答这个问题并非易事，详见文献[45]. 简言之，当我们构造安全归约时，通常需要考虑以下几点：

(1) 安全模型与安全目标是否吻合？是否考虑到敌手在现实环境下所有可能的攻击行为？

(2) 难解问题是否被恰当地嵌入到归约中？从归约出发是否能够正确推导得到困难问题的答案？

(3) 攻击者对随机预言机发出询问的次数是否足够小或为常量？

(4) 攻击者的攻击能力是否受条件限制？或者其计算能力是否受限？换言之，攻击者是否能够访问随机预言机，或者能否在发出挑战后仍然能够继续询问？

需要指出的是，安全归约(或安全证明)并不是完美的[54]. 随着量子密码学的发展，敌手的攻击能力将会超出现有安全模型的描述范围，这将导致该模型下的现有安全分析失效. 此外，安全模型需要刻画所有潜在的网络攻击. 然而，随着信息技术的发展，不断升级的网络攻击手段和网络及设备的异构性，在实际环境中及时地检测到密码算法的漏洞不是一件易事. 这都使得安全模型的刻画以及安全归约的实现变得困难.

方法 2. Game Hopping[60]：Game Hopping 通过使用一系列的 Games(如 Game 0，Game 1，…，Game n)来实现安全归约，n 为一个常数. 这里，Game 0 为最初的安全模型. 设 S 为敌手在 Game 中发动一次成功的安全攻击的事件，相应的，设 S_i 为敌手在 Game i 中发动一次成功安全攻击的事件. 设 $Pr[S_i]$ 为敌手在 Game i 中发动一次成功的安全攻击的概率. 基于 Game 的安全归约旨在证明对于 $i=0,\cdots,n-1$ 而言，概率 $Pr[S_i]$ 和概率 $Pr[S_{i+1}]$ 是无限接近的. 因此概率 $Pr[S_n]$ 与目标概率 $Pr[S_0]$ 是等同或者无限接近的.

攻击者在每一个 Game 刻画的特殊攻击环境下拥有未知的胜利概率. 通过将攻击环境(即每一个 Game 的定义)进行略微修改，直到可以计算攻击者的胜利概率为止[60-61]. 每一次的修改对攻击者来说应该是无法区分的(基于对修改前后环境的谈论和分析). 我们将从 Game i 修改到 Game $i+1$ 的过程称之为迁移. 主要有两种迁移：基于不可区分性的迁移和基于失败事件的迁移.

基于不可区分性的迁移. 在基于不可区分性的迁移中，每一步都会做微小的修改. 如果这一修改被敌手检测出来，那么我们可以立即构造出一种区分两个本应不可区分的集合分布(后称“分布”)的方法. 比如，我们假设 P_1 和 P_2 是在计算上不可区分的两个分布. 为了证明条件概率 $|Pr[S_i]|Pr[S_{i+1}]|$ 是可忽略的，我们可以通过证明存在一个区分算法 D，它能够在 Game i 和 Game $i+1$ 之间进行判别：即当给定一个来自 P_1 区间的元素作为输入，D 以 $Pr[S_i]$ 的概率输出 1，当给一个来自 P_2 区间的元素作为输入，D 以 $Pr[S_{i+1}]$ 的概率输出 1. 因此，基于之前的不可区分性假设，我们可以得到条件概率 $|Pr[S_i]|Pr[S_{i+1}]|$ 是可忽略的.

基于失败事件的迁移. 在基于失败事件的迁移中，除非一个失败事件 F 发生，否则 Game i 和 Game $i+1$ 的执行过程相同. 特别的，需要在同一概率分布区间内定义两个 Game，它们之间唯一的区别是计算特定随机变量的规则 F. 这样一来，我们说

两个 Game 是相同的当且仅当 F 发生，即

$$S_i \wedge \neg F \Leftrightarrow S_{i+1} \wedge \neg F \tag{3}$$

式(3)代表事件 $S_i \wedge \neg F$ 和事件 $S_{i+1} \wedge \neg F$ 是相同的. 如果上述成立，则我们可以使用以下引理.

引理 1. 区分引理. 设 A,B,F 代表三个概率分布对应的事件，并且 $A \wedge \neg F \Leftrightarrow B \wedge \neg F$. 那么，满足 $|Pr[A]-Pr[B]| \leq Pr[F]$.

证明. 引理的推导过程如下：

$$\begin{aligned}|Pr[A]-Pr[B]| &= |Pr[A \wedge F]+Pr[A \wedge \neg F]- \\ &\quad Pr[B \wedge F]-Pr[B \wedge \neg F]| \\ &= |Pr[A \wedge F]-Pr[B \wedge F]| \leq Pr[F]\end{aligned} \tag{4}$$

等式(4)的第二行是根据 $A \wedge \neg F \Leftrightarrow B \wedge \neg F$ 的关系得到. 因此，可以进一步推导得到 $Pr[A \wedge \neg F]=Pr[B \wedge \neg F]$. 由此，在最终的不等式中，我们可以推导得到概率 $Pr[A \wedge F]$ 和概率 $Pr[B \wedge F]$ 都在 0 到 $Pr[F]$ 的区间范围内.

为了证明概率 $Pr[S_i]$ 与概率 $Pr[S_{i+1}]$ 是无限接近的，需要证明概率 $Pr[F]$ 是可忽略的. 在一些特殊情形下，可以通过一个安全性假设来完成证明(比如当事件 F 发生的时候，敌手找到了哈希碰撞或者伪造了 MAC[36])，在其他情形下，也可以使用基于信息论的论据(Argument)来证明. 本质上来说，对事件 F 的定义和分析是围绕两个相邻 Game 的随机变量来展开的.

3 研究问题与现状

图 4 重点讨论了比特币区块链的安全性、隐私性和可扩展性这三个研究问题. 这些问题为相关密码算法的设计提供了重要线索和动机. 基于这些研究问题，表 2 对当前的一些加密货币项目[1-4,62-64]进行了比较. 随后，我们将扩大讨论范围，包括其他加密货币、区块链项目以及底层密码算法，具体见表 3～5. 基于对相关情况的综合考虑，我们进一步提供了现状分析.

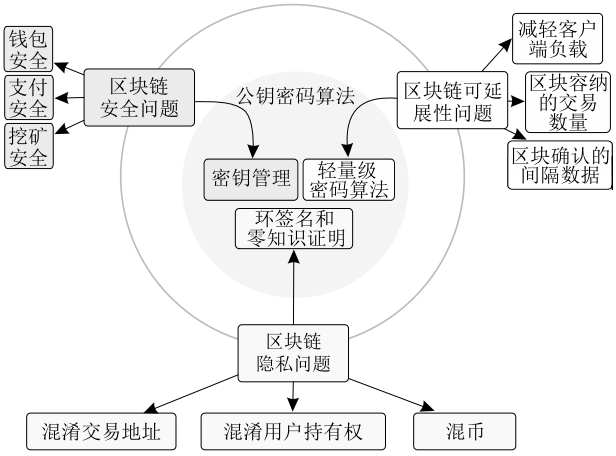

图 4 比特币区块链研究涉及的主要问题

表 2 加密货币与相关问题[14]

加密货币			比特币[1]*	莱特币†	以太币[2]‡	门罗币☆	达世币#	零币[3]‖	零钞[4]**
发行时间			2009	2011	2014	2014	2014	2016	2016
问题	安全	抗“双花”	○	○	○	○	○	○	○
		抗“51%”攻击	○	○	○	○	○	○	○
	隐私保护	支付者隐私保护	化名	Mimble-Wimble 协议[62]	化名	可链接环签名[63]	扩展版 CoinJoin 协议	承诺和零知识证明	嵌套密码承诺[4]
		接收者隐私保护				CryptoNote		×	使用秘密密钥进行加密
		隐藏交易数额	×	×	×	采用承诺[64]	×	×	采用承诺[64]
	可延展性	速度	慢	中	快	中	中	慢	中
		区块大小	1 MB	可变尺寸	可变尺寸	可变尺寸	2 MB	2 MB	2 MB
		每秒交易数量	7	56	20	10	28	14	27
		生成区块时间	10 min	2.5 min	15 min	2 min	2.5 min	10 min	2.5 min

注：○：基本可以，×：不可以.
*https://Bitcoin.org/, †https://litecoin.com/en/, ‡https://ethereum.org/en/, ☆https://getmonero.org/,
#https://www.dash.org, ‖http://zerocoin.org/, **https://z.cash/.

3.1 安全问题与现状分析

比特币[1]的安全性对于确保用户的资金和交易的机密性至关重要. 同时，保护比特币网络免受恶意攻击也是必要的. 为了实现这些目标，比特币采用了一系列密码算法和协议[14]，如公钥加密、数字签名和工作量证明机制. 这些安全措施对于确保比特币网络的稳定性和安全性起着重要的作用. 接下来将逐一讨论这些问题. 表 3 总结了用于保障区块链系统安全的密码算法[13,65-72]及其安全现状.

表 3　区块链中密码算法的安全现状

区块链底层密码算法面临的常规威胁[13]		
威胁类型和案例	防范措施	解　释
密钥泄露（攻击钱包或者盗取钱包密钥[66]）	强化密钥管理、密钥更新、密钥加密存储、访问控制、强化身份验证等	周期性地更新密钥，撤销被泄露的密钥，使用多重签名方案，选择足够长的密钥长度
签名伪造（攻击 ECDSA[65]、环签名[67]）	采用多重签名、增加密钥长度、更新密钥、使用强随机数、强化签名算法等	周期性地更新密钥，撤销被泄露的密钥，使用安全的随机数生成器，使用安全的哈希函数来计算消息摘要等
密文破译（攻击 RSA[68]、Pedersen 承诺）	加强密钥管理、数据加密传输、使用强随机数、强化加密算法等	使用专门且安全的硬件设备来保护密钥，使用安全的加密通信协议，使用安全的随机数生成器，升级算法等
哈希碰撞（攻击区块链底层哈希函数[69]）	使用安全哈希函数、增加哈希长度、使用强随机数、强化密钥管理和访问控制、强化哈希算法等	选择公认为安全的哈希函数，增加哈希值的位数，降低碰撞的概率，使用安全的随机数生成器，选取严格的密钥管理和访问控制措施升级哈希算法等

量子计算对底层密码算法造成的威胁[70]			
密码算法	密码类型	功能	造成威胁
AES*	对称密码	加密	攻击难度减半
SHA-2，SHA-3†	哈希函数	哈希	攻击难度减小
RSA‡	公钥密码	加密	攻破
ECDSA☆，ECDH#	公钥密码	签名，密钥交换	攻破
DSA‖	公钥密码	签名，密钥交换	攻破

区块链钱包安全[23]			
钱包类型	面临的威胁	密钥保存方式	保护措施
离线钱包	设备丢失或者损坏	离线设备、纸钱包**、脑钱包††	冗余备份、加密存储
本地钱包	网络攻击或者设备故障	存储在主机或者移动设备上	加密钱包、钱包备份
在线钱包	服务器遭受入侵	存储在服务器上	多重签名[71]

注：*AES(Advanced Encryption Standard)：高级加密标准，†SHA(Secure Hash Algorithm)：安全散列算法，‡RSA[72](Rivest Shamir Adleman)：一种公钥密码算法，☆ECDSA[31](Elliptic Curve Digital Signature Algorithm)：椭圆曲线数字签名算法，#ECDH(Elliptic Curve Diffie-Hellma)：椭圆曲线 Diffie-Hellman 密钥交换，‖DSA(Digital Signature Algorithm)：安全数字签名算法，**纸钱包(Paper Wallet)：包含可用于接收比特币的公共地址和私钥的文档，††脑钱包(Brain Wallet)：用户自己选择口令作为私钥的密码，然后将该密码记住即可，无需存储私钥，降低了私钥丢失的风险.

钱包安全. 每个用户需要拥有一个数字钱包来进行比特币的转账和接收. 电子钱包为用户提供了一对公私钥. 其中，公钥用作接收比特币转账的地址. 比特币采用了椭圆曲线数字签名算法[31](ECDSA)用于认证交易. 为了进行比特币转账，用户选择一个新鲜的随机数，并使用私钥生成 ECDSA 签名. 使用不安全的随机数可能会导致受到“双花”攻击[65]. 只有掌握私钥的用户才能访问对应的钱包并执行秘密操作(如转账). 然而，一旦用户在使用过程中丢失了私钥，通常没有强有力的补救措施来挽回. 因此，用户的私钥是需要保护的资产.

支付安全. 为了确保支付安全，研究主要关注防止“双花”交易. 双花指的是用户在两个不同的交易中花费同一个比特币. 比特币通过 UTXO 模型和 PoW 来解决双花问题. 该模型要求使用先前的比特币作为后续交易的输入. 同时，UTXO 模型由基于 PoW 的共识算法强制执行，该算法实现了一 CPU 一票的方式来验证结果并在节点之间达成共识. 如果一个矿工检测到具有相同输入的两个交易，他们只会处理其中一个，而拒绝另一个. 然而，根据调研[24]，完全消除双花攻击往往是不太可能的. 目前的研究主要集中在设定合适的下限，并通过检测和分析来识别双重支付.

挖矿安全. 共识协议是区块链实现去中心化的关键，因为它允许用户在没有任何信任的情况下达成共识. 比特币使用 PoW[1] 作为其共识协议，该协议要求矿工解决与密码学相关的难题，以便全网矿工就区块历史达成共识. 一旦难题得到解决，奖励将分享给协助解决该难题的矿工. 在 PoW 中，这样的密码难题是要求哈希值以特定数量的零开头.

然而，PoW 容易受到“51%”攻击的影响. 在这种攻击下，如果攻击者控制了超过 50%的全网计算能力，就能够随意操纵区块链数据. 近年来的研究显示[73]，矿池经常遭受内部威胁和外部攻击的双重威胁，而外部攻击往往难以应对，因为与诚实挖矿相比，操控其他矿池可以带来更高的经济利益.

安全现状分析. 表 3 指出了密码算法面临的常规安全威胁、量子计算的威胁以及钱包安全方面的问题，并提供了相应的防范措施. 我们的分析如下：

(1) 在区块链的数据层面，存在加密算法被高性能计算破解[68]、密钥管理不当、密码组件代码漏洞[66]等安全性问题. 区块链中的密码算法存在被直接攻破的危险[69].

(2)为了应对量子计算的威胁,需要考虑采取相应的防护措施.研究量子密码学的方案(如量子密钥分发、量子认证[48]和量子随机数生成)以及基于复杂数论的算法(如格密码学),可以为区块链的安全性提供更长期的保障.

(3)为了真正解决区块链应用系统的安全问题,需要对密码应用在区块链中的合规性、正确性和有效性进行研究.考虑到区块链面临的严峻安全形势,对相关算法进行测评(详见第 7 节)工作是必要的.密评不仅是应对安全形势的紧迫需求,也是提升区块链安全的必然要求,更是网络运营者和主管部门的法定责任[74-75].

3.2 隐私问题与现状分析

表 4 提供了区块链隐私保护的现状以及相关技术和方案[3-4,13,23,63-64,76-92]的对比.

表 4 区块链的隐私保护现状

混币机制的现状[23]				
混币协议	是否依赖第三方	是否需要混币费	遭盗窃风险	拒绝服务攻击风险
Mix*	√	√	高	低
Mixcoin[76]	√	√	中	低
盲币(BlindCoin)[77]	√	√	中	低
达世币(Dash)†	√	√	中	低
混币(CoinJoin)‡	×	×	低	高
洗币(CoinShuffle)[78]	×	×	低	高
Xim☆	×	√	低	低
CoinParty[79]	×	×	低	低
门罗币(Monero)#	×	×	低	低

基于同态加密的隐私保护与区块链方案[80]		
同态密码技术	特 点	有关应用
基于同态承诺的保密交易[81]	使用 Pedersen 承诺[64]实现对交易金额的隐藏,满足隐藏性和绑定性	Elements‖,零币[3],MimbleWimble[62],门罗币,FabZK[82],零钞[4]
Pailier 算法[83]	半同态加密算法,该算法基于复合剩余类困难问题	Zheng 等人[84]的方案,Wang 等人[85]的方案,Yaji 等人[86]的方案等
Twisted-ElGamal[87]	加法同态密码算法,解密效率优于 Pailier 算法,是零知识证明友好的	PGC** [88]

基于环签名的隐私保护与区块链方案[13]			
环签名技术	密码框架	签名长度	困难问题
环机密交易 2.0(RingCT 2.0)[16]	PKI	$\mathcal{O}(1)$	DDHP,k-SDHP
环机密交易 3.0(RingCT 3.0)[17]	PKI	$\mathcal{O}(1)$	DLP,q-DDHIP
YLA+13[89]	PKI	$\mathcal{O}(\sqrt{n})$	SDHP,DDHIP
ALS+13[90]	IDB	$\mathcal{O}(1)$	DLP,DDHP

基于零知识证明的隐私保护与区块链方案[80]				
零知识技术	可信初始化	证明长度	证明复杂度	验证复杂度
zk-SNARKs††[91]	√	$\mathcal{O}(1)$	$\mathcal{O}(n\log(n))$	$\mathcal{O}(\ell)$
zk-STARKs‡‡[44]	×	$\mathcal{O}(\log^2(n))$	$\mathcal{O}(n\ \mathrm{poly}\log(n))$	$\mathcal{O}(\mathrm{poly}\log(n))$
Bulletproofs[92]	×	$\mathcal{O}(\log(n))$	$\mathcal{O}(m\log(n))$	$\mathcal{O}(n\log(n))$

注:*https://leastauthority.com/blog/introduction-to-mix-networks-and-anonymous-communication-networks/,†https://www.dash.org/,‡https://www.investopedia.com/terms/c/coinjoin.asp,☆https://ximcoin.com/,#https://getmonero.org/,‖https://elementsproject.org/,**PGC(Pretty Good Confidential Transaction System):基于密码算法的机密交易系统[88],DDHP:判定性 Diffie-Hellman 问题,k-SDHP:k 阶强 Diffie-Hellman 问题,DLP:离散对数问题,q-DDHIP:q-判定性 Diffie-Hellman 逆元问题,PKI(Public-Key Infrastructure):基于公钥的基础架构,IDB(Identity-Based Infrastructure):基于身份的基础架构,††zk-SNARK(Zero-Knowledge Succinct Non-Interactive Argument of Knowledge):零知识简洁非交互式知识证明,‡‡zk-STARK(Zero-Knowledge Scalable Transparent Argument of Knowledge):零知识可扩展透明知识证明,设 n 为电路门数,设 ℓ 为实例大小,$\mathcal{O}(\mathrm{poly}\log(n))$表示:对于可用对数空间可计算电路表示陈述的验证效率[80].

比特币的原始设计不能保证完整的隐私性,它仅仅提供了基于“假名”(pseudonym)的机制.该机制允许用户拥有多个比特币地址.然而,攻击者可以建立起发送者和接收者地址之间的一对多关联关系,从而揭示用户的实际身份.为了实现完整的用户身份隐私和交易隐私,研究者们要么直接将具有隐私保护功能的密码算法封装到加密货币的设计中(如门罗币[15]、零币[3]、零钞[4]),要么开发具有隐私保护功能的方案作为外部的技术组件,并允许其被集成到区块链系统的设计中(如 CryptoNote、混币

技术[76]）. 接下来，我们重点介绍在加密货币中实现隐私保护的思路.

隐藏地址洗牌. 在比特币交易中，通过将发送者和接收者的公钥地址与其他地址混淆（又称“洗牌”），可以打破交易流的可追溯性. 一种理想的密码工具是环签名，它允许签名者将自己的身份隐藏在由多个用户身份节点构成的环上，通过不暴露身份的方式对消息进行认证. 这样一来，可以极大简化签名算法的初始化计算，避免了中心化的群管理所带来的缺陷. CryptoNote 是一个为比特币提供洗牌的基础方案，它使用非交互式零知识证明生成一次性环签名，将发送者的地址与其他地址混合，实现了发送者身份的隐私保护. 许多加密货币都采用了 CryptoNote 作为基础方案，如莱特币、门罗币、DarknetCoin、Aeon、Boolberry 等. 特别地，门罗币利用了 CryptoNote 和环机密交易（RCT）[15] 提供的一次性环签名来保护付款人和收款人的隐私. 由于门罗币采用了可链接的环签名[63]，它允许外界在不破坏用户匿名性的前提下，通过标签的可链接性来计算并检测交易是否存在双花问题. 这种方法是在匿名条件下解决双花问题的理想手段. 其他采用环签名的加密货币有 Stealthcoin、ShadowCash 等.

通过对持有权进行“洗牌”可以有效防止重要信息的泄露，例如防止泄露有关所用户拥有的货币数量. 零知识证明（ZKP）是打破货币和所有权之间关联关系的理想密码原语. ZKP 使得证明者 P 能够在不泄露任何有效信息的情况下让验证者 V 通过验证零知识证明来相信某声明的真实性. 一个实际的例子是零币[3]. 零币是一种由比特币扩展而来的加密货币，能够与比特币之间进行互相转换. 用户使用 ZKP 作为凭证来匿名消费零币. 由于涉及复杂的执行过程，零币在计算上不易扩展. Garman 等人[93] 通过减少 ZKP 的证明长度和消除基于 ROM 的假设，改进了零币方案. 此外，Pinocchio 币[94] 作为零币的扩展方案，需要一个中心化和一次性的算法初始化过程. 然而，上述项目都没有实现对交易金额的隐藏.

Sasson 等人[4] 提出了零钞. 与零币不同，零钞采用了一种实用的 ZKP 变种：简短非交互式零知识论证（zk-SNARK），实现了较强的匿名性. zk-SNARK 能够提供具有较小和恒定长度的零知识论证，它通过假设敌手具有有界的计算能力来形式化地构建安全模型. zk-SNARK 使用基于两层的承诺来隐藏用户的公钥和交易金额，其中用户需要将一定金额的零钞对应的密码承诺[64] 写入列表中. 当用户希望花费零钞时，他需要生成 zk-SNARK，以在不泄露任何有用信息的条件下证明他确实知道零钞序列号和零钞金额对应的承诺. 具体的，零钞采用的 zk-SNARK 利用同态加密（具有同态性的密码承诺[64]）的性质来实现序列号、地址和交易金额的机密性和隐私性. Sasson 等人[4] 对提出的零钞方案进行了正式的分析. 然而，采用 zk-SNARK 的零钞系统存在不可扩展性和处理效率低下的问题.

混币技术. 混币技术可以用于混淆比特币交易的输入和输出地址. 混币可以通过中心化[76] 和去中心化[78] 的方式来实现. 中心化的混币服务通常会指派一个中央服务器来将目标用户的输入和输出地址与服务器混币池中的地址进行混淆，从而可以让用户从混币服务器那里放心地接收或使用比特币. 去中心化的混币服务通常不需要一个中心化的可信第三方参与，从而降低了单一混币服务器作恶所带来的风险.

隐私保护现状分析. 分析如下：

（1）根据表 4 和表 5 所示，近些年的用户开始倾向于选择能够提供可靠匿名性的加密货币（如达世币、门罗币）. 这表明当前用户越发注重对个人隐私的保护. 然而，隐私保护的功能也给市场监管带来了挑战[23]. 滥用这一功能可能滋生违法犯罪活动，例如勒索病毒（Wannacry）的爆发. 勒索病毒使用比特币来接收勒索赎金，给全球 30 万名用户带来了巨大的经济损失. 比特币的去中心化和匿名化给治理这类违法活动带来了困难.

（2）实现高度隐私保护通常需要使用复杂的加密算法和协议，这会增加不小的计算开销，并带来一系列问题，例如系统吞吐量限制、扩展性挑战（见第 3.3 节）、监管问题等. 此外，使用了复杂密码学技术的加密货币可能面临更多的安全漏洞和攻击面[67].

（3）针对以上两点，为了确保密码算法（或密码模块）在加密货币与区块链中得到正确和有效应用，需要对采纳的密码算法开展测试与评估（见第 7 节）.

（4）截至目前，达世币和门罗币已经超越了零币[3] 的市值，它们是目前最受欢迎且提供较强隐私保护功能的加密货币. 其中，门罗币提供了更高的隐私保护级别. 然而，由于达世币在早期的推广和广告活动方面取得了成功，在商家和交易平台上的综合普度程度更高，具有更广泛的用户群体.

3.3　可拓展问题和应用现状分析

可扩展性是区块链的重要指标之一，它关系到区块链在实际环境中的应用和落地. 表 5 展示了区

块链相关项目和研究的应用现状[95-105]. Croman 等人[106]对比特币的可扩展性指标(最大吞吐量、延迟、交易平均开销等)进行了分析和讨论. 近些年涌现出一批区块链的扩展技术(如分片、隔离见证等),但这些技术通常会打破比特币的原始设计或需要对比特币系统进行重大修改. 此外,为了提高可扩展性,往往需要牺牲部分安全性或匿名性. 在提升可扩展性的同时,兼顾加密货币的安全性和去中心化等要求通常是一项具有挑战性的工作[107],因为这打破了区块链的"不可能三角"(又称为"三元悖论").

表 5 区块链的应用现状

加密货币应用现状[95]*					
加密货币	匿名支付	实时支付	币总值*(美元)	每秒交易量[95]	排名*
比特币	×	×	5830 亿	3.5	1
以太币	×	×	2220 亿	5.4	2
零币	√(zk-SNARK)	×	4.77 亿	0.06	80
莱特币	×	√(通过调整难度)	62.3 亿	0.35	11
达世币	√	√(Instant-Send 功能)	90 亿	0.07	7
点点币†	×	×	1.2 亿	0.01	195
瑞波币	×	√	240 亿	10.75	6
门罗币	√	×	30 亿	0.06	25
多链币‡	n/a☆	n/a	0.49 亿	1000	353
超级账本#[96]	n/a	n/a	n/a	可变	n/a

著名的区块链项目[97]			
项目	加密机制	安全机制	应用场景
Corda‖[98]	基于 Tear-offs 和混合密钥的保密机制	Corda 加密套件/TLS 协议	金融业务平台
Quorum**[99]	基于 Enclave 的保密和合约执行机制	证书/HTTPS	分布式应用
Libra††	SHA3-256/爱德华曲线数字签名算法(EdDSA‡‡)	Diffie-Hellman	加密货币
Blockstack[100]	去中心化存储系统,身份验证系统	安全骨干网络	互联网基础设施
Filecoin☆☆	SECP256K1##(ECDSA),BLS[32]	TLS 协议	文件存储与共享

面向隐私保护的区块链项目[101]			
项目	涉及密码技术	隐私策略	应用场景
Identity Mixer***	直接匿名证明	盲签名	企业级身份管理
Hawk[102]	两级智能合约管理	访问权限控制	涉及资金交易的场景
Mediledger†††	zk-SNARK	无	医药供应链景

面向访问控制的区块链研究[103]		
有关研究	研究思路	应用场景
区块链赋能不同的访问控制模型	区块链+RABE‡‡‡或ABAC☆☆☆ 或 CapBAC### 等	身份认证,访问控制
基于区块链的访问控制模型	基于比特币[104](或以太坊[105])的访问控制方案	身份认证,访问控制

注:*https://cn.investing.com/crypto/,截至 2023-06-28,†https://www.peercoin.net/,‡https://www.multichain.com/,☆n/a:不支持或无法获知,#https://www.hyperledger.org/use/fabric,‖https://corda.net/,**https://consensys.net/quorum/,††https://www.diem.com/en-us/,‡‡EdDSA(Edwards-curve Digital Signature Algorithm):爱德华曲线数字签名算法,☆☆https://filecoin.io/,##http://www.secg.org/sec2-v2.pdf,***https://www.zurich.ibm.com/pdf/csc/Identity_Mixer_Nov_2015.pdf,†††https://www.mediledger.com/,‡‡‡RABE(Role-Based Access Control):基于角色的访问控制,☆☆☆ABAC(Attributes-Based Access Control):基于属性的访问控制,###CapBAC(Capability-Based Access Control):基于权能的访问控制.

借助轻量级密码学. 比特币和以太坊等区块链使用 ECDSA[31]来认证交易. ECDSA 是一种高效且可扩展的公钥密码算法. 除了 ECDSA 之外,越来越多的公钥密码算法被引入到区块链设计中,例如:零币和零钞采用 ZKP 来实现交易的匿名性. 然而,ZKP 的复杂构造通常会导致处理效率较低. 另外,门罗币所采纳的环签名也因为其复杂构造而存在性能低下的问题. 因此,使用轻量级的密码构造或简化现有区块链里的密码方案是非常必要的. 然而,对具有隐私保护功能的加密货币进行扩展是一项具有挑战性的工作,因为它涉及到解决"三元悖论"[19,107]. 此外,在共识机制的设计中选择适当的难解问题(Puzzle)也是改善可扩展性的一种思路. 目前,比特币的工作量证明协议因需要消耗大量电力资源来执行而广受批评. 包括中国在内的一些国家,已经明令禁止比特币有关的"挖矿"活动.

从客户端转移走计算开销. 改善区块链性能的一个直接且可行的方法是将计算开销从客户端转移到其他地方,例如委托给第三方计算平台. 隔离见证(SegWit)[108]是比特币协议的一种出色的可扩展解决方案. SegWit 通过从每个交易中移除签名数据,以回收更多的存储空间. 另一个著名的解决方案是分片技术[109]. 分片通过将区块链网络中的节点划分为相对独立的多个分片,每个分片处理规模较小的事务,实现多个分片并行处理事务. 理论上,这种方法可以提高整个网络的吞吐量. 然而,上述方法仍

处于起步阶段.

另外一个提升交易处理能力的技术称为：支付通道或者状态通道技术. 著名的通道技术有比特币的闪电网络①和以太坊的雷电网络②. 以以太坊为例，支付通道通过智能合约在两个区块链节点之间创建私有通道，允许节点在通道内进行交易并自行维护余额，而无需将这些交易记录到区块链上，从而显著提高了可扩展性. 多个支付通道形成支付网络，使得即使没有直接支付通道的两个节点，也可以通过多跳方式在区块链之外进行交易. 然而，在建立支付通道时，需要解决初始余额的资金分配问题，而这在多跳交易的情况下变得更加复杂.

此外，为了处理频繁发生的小额交易，微支付协议[110]被认为是理想的密码解决方案. 作为一种去中心化的概率性支付方案，微支付允许用户在小规模范围内高效地交换货币激励.

权衡区块中的交易数量. 增加每个区块的容量可以提高吞吐量，但同时会减慢区块的传播过程，并给验证区块的过程增加更多计算开销. 相反的，减少交易数量可能会加快区块确认过程，但会降低吞吐量. 通常情况下，比特币需要 10 分钟的间隔时间来确认新的区块(同时防止“双花”攻击和分叉攻击[24]). 权衡区块中的交易数量意味着在区块链的安全性和可扩展性之间找到一个平衡的解决方案.

权衡区块间隔时间. 区块的间隔时间是影响区块链可扩展性的关键因素，它由领导节点的选举和交易传播过程决定. 在比特币协议中，通常每 10 分钟进行一次领导节点选举，每个节点可以向链尾添加一个新区块. 有三种情况需要讨论：固定的领导节点(如 Hyperledger Fabric[96])、单一领导节点(如 Bitcoin-NG[111])和集体领导节点(如 Byzcoin). 区块间隔时间主要由领导节点的选举机制决定.

可扩展性现状分析. 根据表 2 和表 5，对区块链可扩展性的分析如下：

(1) 区块链技术从诞生至今一直存在着效率方面的瓶颈问题[112]. 区块链系统的效率受到系统架构、共识算法、网络能力、密码算法以及智能合约虚拟机计算这五个因素的制约. 例如，比特币和以太坊系统采用基于工作量证明(PoW)的共识算法，要求每笔交易和区块都得到全网络中节点的确认. 随着网络规模的增大，共识所需时间也随之增加. 此外，由于存在网络传输速率的限制，许多区块链系统声称每秒可处理 100 万笔交易，但在现实中很难达到这一水平. 另外，以椭圆曲线加密算法为代表的密码算法的自身计算开销也限制了区块链的效率. 智能合约执行效率较低也是一个问题.

(2) 值得注意的是，当前网络算力是影响区块链可扩展性和安全性的重要因素. 对于区块链来说，算力决定了安全性、共识机制和去中心化程度，对于密码算法来说，算力影响着加密算法的安全性和抵御攻击的能力. 随着平均计算能力的提升，攻击者拥有更多资源来破解密码，但这也意味着更高的挖矿效率和达成共识的效率. 因此，算力的提升既带来了机遇，也带来了挑战. 需要结合现有的计算模型和安全需求(如第 2.3 节所讨论的)，设计实用且安全的区块链或密码算法.

应用现状分析：结合表 5 给出的应用现状，我们进行如下分析：

(1) 加密货币是区块链技术最早和最广泛应用的领域之一. 目前，具备隐私保护功能的成熟加密货币备受用户青睐. 为了规范加密货币市场，防止加密货币的匿名性和去中心化特性被滥用，同时又不抑制市场参与的积极性，柔性化的监管措施(如沙盒监管)在全球范围内不断推进. 这也反映出对包括区块链中密码算法使用的一系列密码产品进行评估(或测试)的必要性[74].

(2) 区块链已积极应用于各个领域[97]，包括金融服务[98]、身份管理[113]、访问控制[103]、供应链管理、物联网[103]、医疗领域[114]、知识产权保护等. 尽管区块链在许多领域都有潜力和应用，但目前仍存在一些挑战，如性能问题、缺乏标准化和监管、与现有系统的集成等问题.

4　区块链中的公钥签名算法

4.1　公钥签名简介

公钥签名算法(Public-Key Signature，PKS)是实现身份认证的基本密码工具，使用 PKS 进行身份认证的场景如下：

(1) Alice 希望使所有参与方相信她确实发布了消息 m. 为此，她首先生成一个公私钥对(pk, sk)，并将 pk 发布给验证者.

(2) Alice 使用私钥 sk 对消息 m 进行签名，得到签名 σ.

(3) 在接收到(m, σ)后，任何接收方都可以用

① https://lightning.network/
② https://raiden.network/

pk 去验证签名 σ 的有效性，确认消息 m 的来源.

公钥签名算法(PKS)有两大主要的分类：一种是基于大整数分解问题的 RSA 范式[72]，另一种是基于离散对数问题(DLP)的 ElGamal 范式[115]. 离散对数问题可以进一步划分为有限域或椭圆曲线上的离散对数问题. Miller[116]首次将椭圆曲线引入公钥密码系统. 自此以后，椭圆曲线密码由于其出色性能而被采纳和应用. 比如，使用 160 位密钥长度的椭圆曲线密码与使用 1024 位密钥长度的 RSA 密码方案一样安全. 根据依赖的不同困难问题，可以将公钥签名分为以下三类：

(1) 基于整数分解(IF)的签名方案：例如RSA[72]和Rabin[117]方案.

(2) 基于离散对数(DL)的签名方案：基于有限域上的离散对数困难问题的难解性，例如 ElGamal[115]，Schnorr[118]，DSA 和 Nyberg-Rueppel[119]方案.

(3) 基于椭圆曲线(EC)的签名方案：基于椭圆曲线上的离散对数困难问题(ECDLP)的难解性，例如 ECDSA[31].

4.2 PKS 的定义和安全需求

公钥签名方案通常由以下算法组成：

(1) $Setup_{\mathrm{PKS}}(1^{\lambda})\rightarrow(SP)$：该算法的输入为安全参数 λ，输出为系统参数 SP.

(2) $KeyGen_{\mathrm{PKS}}(SP)\rightarrow(pk,sk)$：该算法的输入为系统参数 SP，输出为公私钥对 (pk,sk).

(3) $Sign_{\mathrm{PKS}}(m,sk,SP)$：该算法的输入为消息 m、私钥 sk 和系统参数 SP，输出为签名 σ.

(4) $Verify_{\mathrm{PKS}}(m,\sigma,pk,SP)$：该算法的输入为消息签名对 (m,σ)、公钥 pk 和系统参数 SP. 如果 σ 是有效签名，则输出 1，否则输出 0.

为了检验公钥签名算法是否达到预期的安全性，通常遵循安全模型开展相应的正确性和安全性分析. 我们将其归纳如下：

(1) 正确性. 给定系统安全参数 SP，对于任意 (pk,sk,m,σ)，如果 σ 是用 sk 对消息 m 产生的有效签名，验证算法 $Verify_{\mathrm{PKS}}(m,\sigma,pk,SP)$ 总返回 1.

(2) 安全性. 给定系统安全参数 SP，在没有掌握私钥 sk 的情况下，任意概率多项式时间(Probabilistic Polynomial Time，PPT)敌手都难伪造一个新消息 m' 的有效签名 σ'，即满足 $Verify_{\mathrm{PKS}}(m',\sigma',pk,SP)=1$.

公钥签名方案的安全模型是围绕挑战者和敌手之间运行一个游戏来模拟的. 在两者交互的过程中，挑战者产生一个签名方案，敌手试图破坏该签名方案. 不可伪造性是公钥签名方案的基本安全需求，它用于刻画恶意用户伪造签名的行为. 具体的，针对选择消息攻击下的存在性不可伪造(EU-CMA)安全性要求任何概率多项式时间敌手 $\mathcal{A}$ 都很难伪造一个新消息 m' 的有效签名 σ'，并且该消息未被询问过. 我们形式化的定义 EU-CMA 安全性如下.

初始化. 挑战者 C 运行 $Setup_{\mathrm{PKS}}$ 生成系统参数 SP. 执行 $KeyGen_{\mathrm{PKS}}$ 产生公私钥对 (pk,sk). C 将 pk 和 SP 发送给敌手 $\mathcal{A}$，C 将 sk 保密. C 控制 sk 用于应对 $\mathcal{A}$ 的签名查询.

查询. $\mathcal{A}$ 自适应地选择消息 m_i 进行签名查询. 为了响应签名查询，C 使用 sk 执行 $Sign_{\mathrm{PKS}}$ 算法计算 σ_{m_i}，然后将 σ_{m_i} 发送给 $\mathcal{A}$.

伪造. $\mathcal{A}$ 返回一个对消息 m^* 的伪造签名 σ^*. 如果以下条件均满足，则 $\mathcal{A}$ 赢得该游戏：

(1) σ^* 是消息 m^* 的有效签名.

(2) 消息 m^* 在查询阶段未被询问过.

为了完成安全性分析，还需要限定敌手 $\mathcal{A}$ 在上述游戏中获胜的概率 ϵ 等价于返回一个有效的伪造签名的概率. 然而，这里的概率并不一定完全等同于优势，还需要考虑签名成功的伪造可能来自于随机猜测这一情形. 公钥签名方案的通用安全需求可以定义如下.

定义 2. EU-CMA. 我们说一个公钥签名方案在 EU-CMA 模型下是 (t,q_s,ϵ) 安全的，当且仅当没有任何敌手在至多发起 q_s 个签名询问后，能够在时间 t 内以 ϵ 的概率赢得上述游戏.

4.3 经典签名算法分析

包括比特币[1]和以太坊[2]在内的许多区块链系统采纳椭圆曲线数字签名算法(ECDSA)对交易进行认证. ECDSA 最早由 Scott Vanstone[31]在 1992 年提出，它可以理解为椭圆曲线(Elliptic Curve，EC)上的 DSA 算法. ECDSA 的签名形式可以描述为 (r,s). 特别的，ECDSA 选择使用 EC 群而不是有限域的原因是：

(1) EC 算法效率高，处理速度快.

(2) 目前没有任何已知的算法可以在亚指数时间内求解 ECDLP 问题.

一般认为在 EC 群 $E(F_q)$ 中的 ECDLP 问题比大小为 q 的有限域中的 DLP 问题更难解决[120].

非形式化的安全分析. ECDSA 签名[31]是由 (r,s) 组成的，其中使用到随机数 k 用于计算 r 和 s. 如果 k 在计算过程中遭到泄露，会导致用户私钥被外部攻击者获取. 较为典型的例子是使用低熵信源后导致的随机数泄露问题. 针对该问题，RFC6979 方案[121]建

议增强随机数的产生源. 此外，重复使用随机数 k 也会导致私钥泄露. 一般来说，针对 ECDSA 的攻击可以归纳如下：

(1) 针对 ECDLP 难解性的攻击.

(2) 针对 ECDLP 底层哈希函数的攻击.

(3) 其他攻击，如 Vaudenay 攻击[122]，重复签名密钥选择，侧信道攻击[123]等.

形式化的安全分析. 需要遵循我们在定义 2 中描述的(EU-CMA)模型来开展安全分析. Brown[124]在假设底层哈希函数是抗碰撞的以及在通用群的前提下，证明了 ECDSA 的安全性. 此外，在文献[125-126]中，DSA 和 ECDSA 的一些变体也已被证明在 EU-CMA 模型下是安全的. 由于 ECDSA 的安全分析主要是通过数学推理进行的，它不涉及复杂或者精巧的证明方法[124].

ECDSA 的更多分析. De Dormale 和 Quisquater[127]讨论了在硬件加速器上部署椭圆曲线密码算法的执行效率，涉及椭圆曲线、参数、群组的选取等问题. Driessen 等人[128]围绕签名算法在能耗、存储开销、密钥长度、性能等多个方面开展了对比和分析. Fan 和 Verbauwhede[129]总结了针对椭圆曲线上密码算法的攻击以及防范措施. Abdouli 等人[130]按照不同的困难问题将签名有关的安全威胁进行列举和分析. 特别的，文献[129,131]讨论了针对椭圆曲线密码的物理攻击，特别是侧信道攻击和故障攻击. 然而，上述文献未系统讨论针对签名算法的理论攻击.

4.4　更多的案例分析和证明技巧

我们给出两个著名的 PKS 方案的案例分析，其中，后者主要用于具有隐私保护功能的区块链.

Boneh 等人[32]的短签名方案(BLS). BLS 签名[32]常被用于与 ECDSA 签名[31]以及 Schnorr 签名[118]做对比，是一种经典的签名算法. BLS 已被以太坊[2]、Dfinity[132]、Algorand[133]和 Chia 等多个区块链采用. BLS 的安全性遵循我们在第 4.2 节定义的 EU-CMA 模型. 其安全证明使用到的技巧包括基于 Game 的证明(见第 2.4 节)、基于定理的证明(见第 2.4 节)以及条件分析.

Shen 和 Mackenzie[134]的群签名方案(MLSAG). MLSAG[134]是门罗币的环机密交易 1.0 协议(RCT 1.0)所采纳的签名方案. MLSAG 方案的安全性基于 Liu 等人[63]的可链接自组织匿名群(Linkable Spontaneous Anonymous Group，LSAG)签名方案. 其安全性证明用到的技巧包括基于矛盾的证明(见第 2.4 节)和“倒带”仿真(见文献[62,125,135]).

4.5　拓展与讨论

环签名在确保数据认证的同时保护签名者匿名性，是实现区块链隐私保护的重要工具. 门罗币在发展过程中不断优化环签名技术. 早期版本的门罗币使用了一次性环签名算法，该算法是对 Fujisaki 和 Suzuki 工作[136]的改进①. 后来，门罗币采用了对 Liu 等人提出的 LSAG 方案的[63]改进版本. 然而，该方案只能支持单输入交易的身份混淆. 为了解决这个问题，后续版本的门罗币引入了环机密交易协议[15](Ring Confidential Transactions，RingCT). RingCT 提出了多层可链接自组织匿名群(Multilayer Linkable Spontaneous Anonymous Group，MLSAG)签名方案. 后来又陆续提出了更先进的改进版本，例如 RingCT 2.0[16]和 RingCT 3.0[17].

尽管门罗币的混币过程无需第三方参与且不需要交易双方互动，但门罗币的混币技术也存在一些安全缺陷，需要研究相关的防范措施[137-138]. 关于门罗币的具体执行细节，可以参考相关的研究文献[113]. 对于 RingCT 2.0[16]和 RingCT 3.0[17]的详细分析留给读者自行完成.

5　区块链中的公钥加密算法

5.1　公钥加密算法简介

使用公钥加密算法对消息进行加解密的场景描述如下：

(1) 假设 Bob 想给 Alice 发送一条隐私信息 m. Alice 和 Bob 都在基于证书的公钥密码架构上注册，以获得一个公私钥对 (pk, sk). Alice 和 Bob 之间无需协商密钥.

(2) Bob 将 Alice 的公钥 pk_A 和消息 m 输入到公钥加密算法中. Bob 得到一个密文 c 并将其发送给 Alice.

(3) 在接收到 c 时，Alice 使用她的私钥 sk_A 解密 c 得到 m.

Diffie 和 Hellman[5]在 1976 年提出了公钥密码学(PKI)的概念，开启了公钥密码学的时代. PKI 较好地解决了与对称加密相关的两个主要问题：(1)密钥分发，(2)数字签名. 和 PKS 类似的，目前的公钥加密算法(PKE)仍可根据所依赖的困难问题大致划分为：基于 IF 的 Rabin 算法[117]，基于有限域上 DLP 的 ElGamal 算法[115]，以及基于 ECDLP 的

① https://bytecoin.org/old/whitepaper.pdf

算法[31]. 早期的 PKE(如 Pedersen 承诺[64])只考虑单向性安全,即它只试图阻止敌手从给定的密文中恢复出整个明文. 然而,哪怕仅仅泄漏密文中的一位敏感信息也是存在安全隐患的. Goldwasser 和 Micali[35]通过定义一种称为选择明文攻击下的不可区分性(IND-CPA)来刻画这种单比特安全性. 1990 年,Naor 和 Yung[33]提出了一种更强的模型:选择密文攻击下的不可区分性(IND-CCA1). 1991 年,Rackoff 和 Simon[34]进一步提出了最强的安全概念:自适应选择密文攻击下的不可区分性(IND-CCA2)安全. 为了满足实际应用场景下的安全需求,学者们普遍认为公钥加密算法需要满足 IND-CCA2 安全性.

5.2 PKE 的定义和安全需求

公钥加密方案通常由以下算法组成:

(1) $Setup_{\mathrm{PKE}}(1^{\lambda})\rightarrow(SP)$:该算法的输入为安全参数 λ,输出为系统参数 SP.

(2) $KeyGen_{\mathrm{PKE}}(SP)\rightarrow(pk,sk)$:该算法的输入为系统参数 SP,输出为公私钥对(pk,sk).

(3) $Enc_{\mathrm{PKE}}(m,pk,SP)\rightarrow(c)$:该算法的输入为消息 m、公钥 pk 和系统参数 SP,输出密文 c.

(4) $Dec_{\mathrm{PKE}}(c,sk,SP)\rightarrow(m \text{ or } \perp)$:该算法的输入为密文 c,私钥 sk 和系统参数 SP. 如果密文 c 是有效密文,输出明文 m,否则,输出$\perp$表示失败.

为了检验公钥加密算法的是否达到预期的安全性,通常需要遵循安全模型开展正确性和安全性分析. 我们将其归纳如下:

正确性. 给定任意(SP,pk,sk,m,c),如果 $c=Enc_{\mathrm{PKE}}(SP,pk,m)$是使用 pk 对消息 m 加密的密文,则使用密钥 sk 对 c 进行解密将返回消息 m,且 $m\neq\perp$.

安全性. 如果没有密钥 sk,敌手很难在概率多项式时间内从给定的密文 $c=Enc_{\mathrm{PKE}}(SP,pk,m)$中恢复得到消息 m,哪怕仅仅是一比特的信息.

公钥加密方案的安全模型是通过挑战者和敌手之间的游戏来模拟的. 具体来说,不可区分性是一种从密文中提取一比特信息的概念. 选择密文攻击下的不可区分性要求敌手$\mathcal{A}$很难有效地区分来自两个不同的消息的加密结果,同时允许敌手$\mathcal{A}$自适应地发起解密询问. 对 IND-CCA2 的形式化描述如下:

初始化. 挑战者$\mathcal{C}$运行 $Setup_{\mathrm{PKE}}$和 $KeyGen_{\mathrm{PKE}}$生成系统参数 SP 和密钥对(pk,sk). 然后$\mathcal{C}$将(SP,pk)发送给敌手 A. $\mathcal{C}$持有 sk 用来产生响应$\mathcal{A}$的解密询问.

阶段 1. $\mathcal{A}$自适应地选择密文对$\mathcal{C}$发起解密查询. 当收到密文 c_i的解密询问时,$\mathcal{C}$执行 $m_i\leftarrow Dec_{\mathrm{PKE}}(c_i,sk,SP)$,并将解密结果 m_i发送给$\mathcal{A}$.

挑战. $\mathcal{A}$选择两个不同的消息 m_0,m_1,它们满足 $m_0\neq m_1$,$|m_0|=|m_1|$. $\mathcal{C}$随机选择 $b\in\{0,1\}$,然后计算一个挑战密文$c_b^*=Enc_{\mathrm{PKE}}(SP,pk,m_b^*)$. C 将 c_b^* 发送给$\mathcal{A}$.

阶段 2. 和阶段 1 类似的,$\mathcal{C}$回答来自$\mathcal{A}$的解密询问,敌手不被允许询问 c_b^*.

猜测:$\mathcal{A}$输出一个猜测值 b',如果 $b'=b$,则敌手$\mathcal{A}$获胜.

提示 1. 如果将上述的阶段 2 去掉,即是 IND-CCA1 安全模型. 如果将上述的阶段 1 和阶段 2 中的解密预言机同时去掉,则得到 IND-CPA 安全模型.

5.3 实际案例

由于 IND-CCA2 加密方案存在算法构造复杂和算法性能低下的问题,没有在区块链中得到广泛采纳. 我们回顾一些在区块链中已被采纳的标准化 PKE 方案,如基于椭圆曲线密码(Elliptic Curve Cryptography,ECC)的加密[139]、基于 RSA 的加密[72]和 Pedersen 承诺[64].

(1) 比特币采用的 ECC 加密. ECC 基于 PKI 架构. 椭圆曲线是由方程定义的平面代数曲线,而基于 ECC 的加密算法则建立在椭圆曲线上. ECC 相对于 RSA,在相同安全性级别下所需的密钥长度更短. 由于 ECC 的计算强度较低,因此它适用于计算资源受限的环境. 基于 ECC 的签名(ECDSA)首次在比特币中采用. 在 ECDSA 的同一套参数下,可以在比特币中直接使用 ECC 加密.

(2) 加密货币广泛采用的 RSA 加密标准. RSA[72]是当前信息系统(包括区块链在内)广泛使用的公钥加密方案. RSA 的安全性依赖于大整数分解的困难性. 在创建数字钱包时,为用户分配一个公共地址用于接收比特币和加密信息,而私钥则用于花费比特币和解密密文[1]. RSA 作为一种经典的加密方案,读者可以很容易找到相关的学习资源.

(3) 隐私保护的加密货币采纳的 Pedersen 承诺[64]. Pedersen 承诺是具有同态性质的密码承诺. 同态承诺(或加密)被广泛用作加密货币的底层模块,已被用于设计零币[3]、零钞[4]、门罗币等. 简单来说,它允许通过使用同态加密技术,在不向外界透露一个消息的前提下,产生一个消息的承诺值. 同态承诺本质上是一个单向陷门函数. 由于仅仅满足 IND-CPA 安全性,同态承诺常常被认为是一种简单但不安全的加密方案(这里忽略了解密的需求). 为了满足实

际应用环境的安全需求，通常需要 PKE 算法满足 IND-CCA2 安全性.

5.4　如何构造 IND-CCA2 安全的 PKE 算法

为了满足包括区块链在内的一系列实际应用场景的安全需求，公钥密码算法通常需要达到 IND-CCA2 安全性. IND-CCA2 与 IND-CCA1 的区别在于：敌手在前者的模型中，在获得挑战密文 c_b^* 之后和发动攻击之前，仍然可以向解密预言机继续发起询问. 然而，根据我们之前在第 5.3 节所述，由于性能受限的问题，尚未有具备理想安全性的 PKE 方案被投入到大规模运营的区块链项目中. 这也是提升区块链系统安全性所面临的巨大挑战. 实现 IND-CCA2 安全性的方式列举如下：

(1) 基于非交互式零知识证明(NIZK)的构造. 在基于 NIZK 的 PKE 方案中，也会使用一对密钥用于证明和验证. NIZK 证明用于证实该密钥确实参与了密文的计算. 通过使用通用的归约，可以将加密案例的安全性归约到一类 NP 完备问题(NPC)[29]上来. 目前尚未有高效的 NIZK 证明系统，即便是在一些特殊的猜想或者密码架构之下，见第 6.3 节.

(2) 基于随机预言机的构造. Bellare 和 Rogaway[39]正式定义了 ROM 模型下的安全证明方法. Fujisaki 和 Okamoto[140]首次提出了在随机预言机模型下将任何 IND-CPA 安全的概率性单向陷门函数转化为 IND-CCA2 安全加密方案的通用方法. 在文献[141]中，他们还去掉了对单向陷门函数的 IND-CPA 安全性要求，但是提出的方法只能转化得到 IND-CCA1 安全的加密方案.

(3) 基于通用哈希证明(UHP)系统的构造. UHP 是针对某个语言的一类特殊的 NIZK 系统. Cramer 和 Shoup[40]首次正式定义了 UHP 的概念. 随后，他们[142]提出了第一个仅依赖于 DDHP(判定性 Diffie-Hellman 问题)且在标准模型下具有 IND-CCA 安全性的 PKE 算法. 一般来说，标准模型下的安全加密方案更加可靠和接近实际的安全环境. 一些在 ROM 模型下声称可证明安全的 PKE 方案后来被证实存在安全漏洞[55-56]. 然而，标准模型下的 PKE 往往由于严谨的设计导致性能糟糕，难以得到实际应用.

(4) 从身份基加密(Identity-Based Encryption，IBE)进行转换的构造. Canetti 等人[143]提出可以从任何满足 IND-CPA 安全性的身份基加密方案中得到 IND-CCA2 安全的 PKE 方案. 基于文献[143]的思路，Boneh 和 Boyen[144]提出了两个在标准模型下选择身份安全的 IBE 方案，并将其转化为两个接近于 Cramer 和 Shoup 方案[142]的 IND-CCA2 安全的 PKE 方案.

(5) 基于混合加密(HY)的构造. 由于常规的 PKE 方案将待加密消息的取值限定在某个群上的元素，因此无法处理任意长度的消息. 混合加密的思想是使用对称加密来加密消息本身，使用公钥加密来加密密钥本身. Cramer 和 Shoup[145]通过定义和结合密钥封装机制(KEM)和数据封装机制(DEM)，正式提出了混合加密的概念. 具体的，他们提出了将任何弱安全的非对称和对称加密算法转化为在随机预言机模型下具备 IND-CCA2 安全的 PKE 算法.

(6) 基于扩展的 ElGamal 加密[115]的构造. ElGamal[115]是一个非 IND-CCA2 安全的经典 PKE 方案. 通过上述提到的 IND-CCA2 实现方法，可以将 ElGamal 方案提升至 IND-CCA2 安全性. 许多 PKE 方案都是从 ElGamal 方案转化而来的，例如基于 DDHP 的 Cramer 和 Shoup 方案[142]、Kurosawa 和 Desmedt 方案[146]、基于广义双线性 Diffie-Hellman 假设(GHDH 猜想)的 Kiltz 方案[147]，以及基于 DH 猜想的标准模型下安全的 Diffie-Hellman 融合加密方案[148](DHAES).

5.5　经典加密算法分析

我们给出两个著名的 PKE 方案的分析以及证明技巧，它们通常被作为学习安全归约和 IND-CCA2 方案的经典案例.

(1) Boneh 和 Franklin[149]的身份基加密方案(IBE). IBE 将用户的唯一身份标识符作为公钥，而不采用数字证书. Boneh 和 Franklin[149]首次提出实用的身份基加密方案. 该方案基于双线性对构造，在 ROM 模型下是 IND-ID-CCA2(Indistinguishability under Chosen Identity and Adaptive Chosen Ciphertext Attack)安全的. IND-ID-CCA2 是一种强于 IND-CCA2 安全的模型，区别在于敌手可以任意获取有关身份对应的私钥(而不仅仅是他选择攻击的那个身份). IBE 方案的证明部分依赖于 Fujisaki 和 Okamoto 的混合加密的引理[141]. 此外，IBE 方案的证明是从基础方案演进至完整方案的两个证明步骤. 这里面使用到的证明技巧包括基于错误事件迁移的证明、基于归约的证明和条件分析.

(2) Cramer 和 Shoup[142]的标准模型下安全的加密方案(CS). CS 方案是首个实用的标准模型下符合 IND-CCA2 安全的 PKE 方案，它不依赖于 ROM. CS 方案的证明过程同样遵循从基础方案演

进至完整方案的两个证明步骤. 该方案使用到的证明技巧包括基于矛盾的证明方法、基于定理的证明方法以及条件分析. 特别地,由于 CS 方案涉及的数学术语(如超平面)和概念(如超平面相交得到的线)不易理解,这使得构造标准模型下的安全归约更加困难. 简单来说,CS 方案的证明是对密文分布集合 R 和 D 进行统计分析测试,并依托该测试构造解决 DDH 猜想的算法,从而完成安全归约.

5.6 拓展与讨论

近年来,涌现出了一批与区块链紧密结合的公钥密码学研究,包括基于区块链的可搜索加密[150]、属性基加密[151-152]和身份基加密等. 以下对三篇值得关注的研究工作进行了简要介绍:

(1) Jiang 等人[150]的可搜索加密方案. 他们解决了密文搜索中可能存在的泄露隐私数据的问题,并引入了"不经意密文搜索"的概念. 他们提出了一种在分布式存储环境下实现点对点密文搜索的方法,并确保搜索信息的隐私数据不被泄露.

(2) Derler 等人[151]的属性基加密和变色龙哈希. 他们重新审视了 Ateniese 等人在 EuroS&P 2017 提出的可编辑区块链的工作. 为了满足对区块链进行细粒度编辑的需求,他们将属性基加密嵌入到变色龙哈希的设计中,提出了一种基于策略的变色龙哈希算法. 他们给出了通用的算法构造,并进行了严格的安全性建模和证明.

(3) Xu 等人[152]的属性基加密和变色龙哈希方案. 他们延续了 Derler 等人的设计思路,提出了可撤销的属性基加密和变色龙哈希算法,并给出了严谨的安全建模和具体算法构造.

总体而言,现有的基于区块链的加密算法研究主要将区块链作为"黑盒"使用,只关注其输入和输出[150-152],而不考虑其内部实现细节. 然而,还有一些研究考虑利用区块链的内在特性(如时间敏感性)来开展新型密码算法的设计,例如 Zhang 等人[153]的云数据完整性审计协议. 这些研究为区块链与公钥密码学的融合设计提供了新的思路.

6 区块链中的零知识证明

6.1 零知识证明简介

零知识证明(Zero-Knowledge Proof, ZKP)是密码学中的一类基本问题,它涉及一个两方交互式的游戏,其中证明方 P 向验证方 V 提供一个证词,该证词可以让 V 相信某个陈述的正确性,同时不泄露任何关于 P 如何生成该证词的信息. 零知识协议是在 P 和 V 之间运行的交互过程,其中 V 的计算能力被限制在多项式时间内. 该协议允许 P 使用一些额外信息生成关于一个 NP 问题的解,使得外界除了知道 P 的证词是否正确之外,V 无法获知 P 用于生成证词的任何有效信息.

目前,零知识证明已经从理论构想发展到实际应用. 证明的大小可以减小到几百字节,验证方的验证时间可以缩短到几毫秒,并且不受证词大小的限制. 零知识证明的快速发展使其广泛应用于区块链项目(如 Hawk[102])和加密货币的隐私保护业务(如零币[3]). 然而,目前大部分的零知识证明系统仍面临着计算开销过高的问题,这主要是由于证明方在计算零知识证明时需要执行一系列密码运算,例如椭圆曲线群上的指数运算. 更糟糕的是,这些开销的复杂性随着 ZKP 陈述(或证明)的长度增加呈超线性增长. 因此,设计具有线性或亚线性的计算复杂度、短证明长度和支持快速验证的零知识证明系统是一个公认的难题. 该问题获得解决将极大地推动零知识证明与密码学的发展.

6.2 零知识证明和论据

Goldwasser 等人[8]正式提出了 ZKP 的概念. 它是构造密码协议的基本模块之一. ZKP 允许证明方 P 在不泄露任何有效信息的情况下使验证方 V 相信其陈述的真实性. 假设 L 是由一个包含 R 中所有陈述的语言,给定一个语言 L 的 ZKP 协议,如果定义 P 仅具有多项式有界的计算能力,则称 (P,V) 为零知识论据(Zero-Knowledge Argument, ZKA). 我们通常需要上述要求来确保协议的稳固性. 当我们强调使用 ZKA 时,它能为我们提供更强的条件限定,即要求 P 能够说服 V 关于某段陈述的真实性当且仅当 P 知道对应的证据[154]. 然而,论据(Argument)的定义不如证明(Proof)的定义严谨,尤其是当 P 是计算不受限的实体时,该定义可能变得没有意义. 换言之,区分证明(Proof)和论证(Argument)的关键来自于对敌手能力的假设.

6.3 非交互式零知识证明(NIZK)

我们通过以下假设来描述 NIZK 的使用场景:

(1) 证明方 P 和验证方 V 都是数学家[29].

(2) 证明方 P 想在四处环游世界的同时发现并证明新的数学定理,并想通过 ZKP 向 V 证明这些新的数学定理.

(3) 证明方 P 可能没有固定地址来接收邮件,并且会在任何邮件到达之前离开.

(4)在上述情况下，就需要用到非交互式零知识证明，因为 NIZK 的使用将帮助 P 使得 V 确信他证明了新的数学定理，并且不泄露任何有关证明过程的有效信息.

当前的 ZKP 研究文献[37,155-156]中，关于 NIZK 最高效的实施方案是 Gennaro 等人[157]对二次算数程序(QAP)进行改进，并将其融合到一个编译器中用于产生与待证明的陈述等价的适宜 QAP 方案. QAP 的概念见第 6.6 节. 接下来，我们根据文献[29]来定义 NIZK 算法. 假设 R 是(x,y)上的 NP 关系. 假设语言 L 满足：$L_R=\{y|\exists x \text{ s.t.}(x,y)\in R\}$. 一个 NIZK 证明系统可以简单表示如下：

(1) $Gen_{\text{NIZK}}(1^\lambda)\rightarrow(crs)$：该随机性算法的输入为安全参数 λ，输出一个公共参考字符串 crs.

(2) $Prove_{\text{NIZK}}(crs,x,y)\rightarrow(\pi)$：该随机性算法的输入为公共参考字符串 crs，一对值$(x,y)\in R$，x 是陈述，y 是证据，输出一个 NIZK 证明(或论据)π.

(3) $Verify_{\text{NIZK}}(crs,x,\pi)\rightarrow(0 \text{ or } 1)$：该确定性算法的输入为公共参考字符串 crs，陈述 x 和证明(或论据)π，输出 0 表示验证失败，输出 1 表示验证成功.

为了检验 NIZK 是否达到预期的安全性，需要根据安全模型来开展完整性和安全性分析. NIZK 需要满足的性质如下：

完整性. 如果 P 知道一个可以证明一段陈述的真实性的证据，那么 P 可以说服 V.

可靠性. 如果陈述是错误的，那么任何恶意的 P 皆无法说服 V.

零知识. 恶意的 V 除了知道一段陈述为真以外，无法获知任何有效的信息. 特别的，为了实现更强的零知识安全性(如合成的零知识证明[158]，Composable Zero-Knowledge)，需要额外定义以下算法[158].

(1) $SimCrs_{\text{NIZK}}(1^\lambda)\rightarrow(crs,tk)$：该算法输入一个安全参数 λ，输出一个模拟的公共参考字符串 crs 和对应的陷门密钥 tk.

(2) $Sim_{\text{NIZK}}(crs,x,tk)\rightarrow(0 \text{ or } 1)$：该算法输入公共参考字符串 crs，陈述 x 和对应的陷门密钥 tk，如果满足 $Verify_{\text{NIZK}}(crs,x,\pi)=1$，则输出 1，否则输出 0.

6.4　简短非交互式零知识论据(zk-SNARK)

zk-SNARKs 是非交互式零知识证明的实用变体. NIZKs 需要一次性且可信的初始化阶段来生成公共参考字符串 crs. 同样，zk-SNARKs 也需要执行这样的初始化阶段来生成证明和验证所需的密钥. 总的来说，它们区别在于 zk-SNARK 的性能更高. 在 NIZK 中，证明长度和验证时间取决于被证明的 NP 语言. 相反的，在 zk-SNARK 中，证明长度仅取决于所选取的安全参数，验证时间仅取决于样例的大小. 因此，zk-SNARKs 被认为是简短且带有短证明长度和更快验证速度的 NIZKs.

假设 L 为 NP 语言，C 为给定实例大小为 n 的 L 上的非确定性决策电路. 对于大小为 n 的实例，zk-SNARK 可用于证明和验证语言 L 中的所属成员资格. 举个例子，使用 C 作为输入，一个可信方通过执行一次性的初始化阶段来获得两个公钥：证明密钥 pk 和验证密钥 vk. pk 允许任何证明方 P 产生一个证明 π，π 可以用于证实 $x\in L$ 的事实. 任何验证方 V 都可以使用验证密钥 vk 来检查证据 π 的有效性. 此外，zk-SNARK 产生的证明 π 是公开可验证的. 任何人都可以验证 π，而无需与生成 π 的证明方进行交互. 有关 zk-SNARK 的构造细节和安全性，见文献[42-43].

6.5　经典零知识证明算法分析

隐私保护是当前区块链用户关注的焦点. 为了防止外界轻易将某一笔比特币交易与具体用户的身份关联起来，人们通常只将比特币地址作一次性使用. 零知识证明是实现上述目的的基本工具.

(1)零币[3]中采纳的 NIZK. 在早期比特币的扩展方案中，例如零币[3]，采用了非交互式零知识证明(NIZK). 零币利用了 NIZK 将比特币转换为零币，用户可以通过 ZKP 证明自己拥有某个比特币，以便花费一定数量的零币. 具体而言，根据 Fiat-Shamir 方法[159]，可以将知识证明转化为非交互式零知识证明，从而实现零币的匿名交易. 然而，该方法产生的零知识证明长度较大且验证时间较长，难以满足实际需求[160]. 为了改进零币的性能，Garman 等人[93]通过减小证明长度并消除随机预言机的假设对零币进行了改进. 此外，零币的其他扩展方案(如 Pinocchio 币[37])通常需要一个中心化且一次性的初始化阶段来生成系统参数.

(2)零钞[4]中采纳的 zk-SNARK. 另一个采用零知识证明的隐私保护方案是零钞[4]，其中采用了 zk-SNARK. zk-SNARK 具有快速验证和短证明长度的特点，其用于生成零钞中的匿名交易. 关于 zk-SNARK，可以参考文献[4].

(3)其他采纳 ZKP 或 zk-SNARK 的加密货币. 采纳 ZKP 的加密货币还有：Zether[161]、MimbleWim-

ble[62]、Coinjoin 等. 此外，zk-SNARK 的实际应用不限于加密货币或区块链，见文献[37,43,155].

6.6 如何构造 zk-SNARK

当前 zk-SNARK 方案主要遵循基于算数电路的可满足性的构造. 在这类构造中，最高效的构造方案是 QAP[91,162-163]. 这类构造方案具有：(1)线性的密钥计算复杂度；(2)准线性的证明计算复杂度；(3)线性的验证计算复杂度. 此外，当前 zk-SNARK 安全性通常基于指数知识猜想和双线性群组上的 Diffie-Hellman 猜想的变种. 见文献[164-165].

Buterin 在文献[166]中给出了构造 zk-SNARK 的方法，Banerjee 等人[167]也给出了一种通用的方法来构造 zk-SNARK. 简单来讲，zk-SNARK 通常用来创造一个函数(或协议)，该函数通过输入证明方 P 计算的证明，为验证方 V 判断该证明的有效性. 具体的，为了验证一个 zk-SNARK 证明，V 需要执行以下步骤：首先，将需要进行的计算转换为算数电路. 然后为电路中的每一个线路赋值以指定电路的输入. 然后，将算数电路中的每一个计算的节点(也称为“门”)转换为一个约束来验证赋值的输入线路所对应的输出线路. 此过程涉及到将陈述转换到可执行的的 zk-SNARK 格式.

当我们把 zk-SNARK 应用到一个具体的问题时，首先要将该问题转化为正确的“形式”，即二次算数程序(QAP). 然后，再将函数代码转换为一个高度非平凡的函数代码. 举个例子，请读者给出三次等式 $x^3+x+5=35$ 的解(提示：答案是 3). 配合该问题的求解过程，以及文献[166]，读者可以学习到构造 zk-SNARK 的关键知识. 遵循 Buterin[166]提出的通用方法，可以一步步的实现 zk-SNARK，过程如下：

(1)将计算问题转换为算数电路.

(2)将算数电路转换为一阶约束系统(R1CS).

(3)将 R1CS 转换为二次算数程序(QAP).

(4)最终实现 zk-SNARK.

提示 2. 通常来说，ZKP(特别是 zk-SNARK)涉及的方案构造和证明是较为复杂的. 为了便于读者“阶梯式”的掌握 ZKP 有关的构造和安全分析，我们推荐读者从方案 GS08[168]、方案 GR16[169]和方案 CA17[170]分别入手开展系统学习. 其中，Groth 和 Sahai[168]在 GS08 方案中给出了基于双线性对的 NIZK 构造. Groth[169]在方案 GR16 测量了基于双线性对的 NIZK 的性能. Campanelli 等人[170]在方案 CA17 中分析了两个 ZKP 方案的缺陷，并给出了改进方案. 读者也可以前往文献[13]了解上述方案的分析和证明技巧. 上述方案有助于读者快速掌握分析 ZKP 方案的技巧和经验. 更多有关 ZKP 的知识详见文献[28].

6.7 拓展与讨论

早期的零知识证明系统由于效率问题，一直停留在理论层面. 直到最近的 10 年里，零知识证明系统才得到了快速的发展. 其中最重要的两个里程碑是 2010 年 Groth 发表的论文[91]和 2015 年零钞使用的零知识证明系统[4]. 此外，Groth 提出的算法[169]，即 GR16 方案，对零知识证明的大小进行了精简，是目前已知的最快、证明最小的 zk-SNARK 方案，通常被作为基准与新的 zk-SNARK 算法进行比较. 目前安全性最高的零知识算法是 zk-STARKs 算法[44]. 随后，Sonic[171]、Halo[172]、Marlin[173]、Plonk[174]等算法相继对 zk-SNARK 算法的一些方面进行了改进.

综上，零知识证明在近些年取得了密集的突破. 零知识证明技术已经成为设计新型区块链方案的关键技术. 表 4 和表 5 给出的应用现状也侧面佐证了零知识的快速发展与成功.

7 区块链与公钥密码的标准与评测

本节主要讨论区块链以及国内商用密码应用与安全性评估(密评)的相关工作.

7.1 概念和术语

标准及其划分. 根据我国的标准法定义，标准包括国家标准、行业标准、地方标准、团体标准和企业标准. 其中，国家标准在全国范围内适用，不受行业的限制. 我们主要关注国家标准①(简称“国标”). 在发布的标准文件前缀中，GB 代表强制性国家标准，GB/T 代表推荐性国家标准.

等保和密评. 信息安全等级保护(等保)是国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护. 密评工作与等保工作相互衔接[75].

商密和国密. 国家密码管理局认定的国产密码算法，即商用密码(SM 系列). 在某些场合中，商密特指国产密码算法. 国家商用密码管理办公室制定了一系列密码标准②，包括 SM1、SM2、SM3、SMS4、SM7、SM9、祖冲之密码算法等. 其中，SM1、SMS4、

① https://openstd.samr.gov.cn/bzgk/gb/

② http://www.gmbz.org.cn/main/bzlb.html

SM7、祖冲之密码是对称算法，SM2、SM9 是非对称算法，SM3 是哈希算法.

政策法规.《密码法》于 2020 年 1 月 1 日开始实施. 随着《密码法》的颁布和实施，原有的《商用密码管理条例》等法规将随之修订，以《密码法》为主导的全新密码管理法律法规体系将逐步形成.

密评的必要性[75]. 密评的必要性体现在三个方面：(1) 密评是应对网络安全严峻形势的迫切需要；(2) 密评是系统安全维护的必然要求；(3) 密评是相关责任主体的法定职责.

7.2　有关技术标准

国密的技术标准. 目前，我国密码标准化工作的顺利开展以及密码行业标准化技术委员会的积极运作，使得与密码算法和应用相关的国家标准多达 46 条. 在相关部门的共同努力下，我国密码标准正迅速走向国际化，并取得了密码算法走向国际的重大突破[75]. 随着国密系列算法逐步纳入国际标准并被集成于国际主流密码工具包中，国密算法的重要性越来越明显，对增强我国行业信息系统的“安全可控”能力具有重要意义[175]. 国密算法作为我国自主可控的密码技术，在提升我国网络信息安全和自主可控水平方面具有重要战略意义.

区块链的技术标准. 中国在区块链技术的发展上一直处于积极探索和发展阶段. 各行业及多个省市也开始积极协助制定和推出区块链行业或地方标准. 然而，截至 2023 年 6 月，仅有 3 条待实施的区块链(推荐性)国家标准. 这主要是因为目前区块链技术在国内的发展时间较短，制定一个国家标准需要经过广泛的研究、讨论和试验，以确保其质量和可行性. 在行业标准方面，国家密码管理局发布的区块链密码应用技术要求(GM/T 0111-2021)中明确指出，区块链中配置和使用的密码算法应采用国家密码管理主管部门批准的算法，具体包括分组密码算法、非对称密码算法和密码杂凑函数等.

在区块链中采用国密的优势. 区块链是一个密集使用加密技术的领域. 国家对国密算法在区块链中的应用也提出了一定要求. 根据当前待实施的 3 条区块链国家标准，对区块链中使用的密码技术的要求参照了《GB/T 37092-2018 信息安全技术(密码模块安全要求)》、《GB/T 39786-2021 信息安全技术信息系统密码应用基本要求》和《GB/T 22239-2019 信息安全技术网络安全等级保护基本要求》. 此外，随着安全形势的演进，一些密码算法已不再安全(如 RSA1024 算法). 因此，政府和企业单位需要按照《GB/T 39786-2021 信息安全技术信息系统密码应用基本要求》，基于国密算法对信息系统进行密码应用改造(简称“密改”). 采用国密算法和进行密改的好处包括：(1) 具备自主知识产权，能够保障关键设施的安全可控性；(2) 部分算法的安全性在国际上更高；(3) 更加规范，符合国家技术标准要求.

7.3　面向国密的测试技术与解析

密文随机性检测. 密文的随机性是评估密码系统安全性能的重要指标. 密文的随机性通常指密文的无规律性和不可预测性. 无规律性要求数据具备良好的随机统计特征，并且在相同条件下不能得到重复的结果. 不可预测性要求即使了解数据生成算法的细节和历史输出，也不能推断之后的输出结果. 目前无法证明符合密码安全需求的伪随机数生成器确实存在，现代密码算法所生成的密文虽具有一定程度的随机性，但仍然存在一定的规律，不是真正的随机数，上述因素为区分密文(或算法)、开展加密流量分析、匿名网络溯源提供了思路.

随机性检测是密评工作中的一项重要任务. 为了研究密文的随机性，需要选择对密文随机性有区分价值的指标，并设计有效的区分算法或分类模型. 上述技术通常是评估机构用于检测密文随机性的基本手段. 为了实现该工具，通常以 NIST 随机性检测指标①为基准，生成随机性合格的密文. 进一步地，设计特征提取算法，分别提取随机文件和不同密码算法的密文文件的特征值，并统计其分布. 根据具有区分性的随机性检测指标，借助合适的区分算法和模型(如深度神经网络模型)，来有效区分不同(加密算法所产生的)密文的特征. 该技术可以用作检测密文是否来自于商密算法(或是否采纳商密算法)的判断依据.

针对密码模块的安全测试. 尽管区块链本身是一种分布式的软件技术，但在某些情况下，为了增强其功能和安全性，可以使用专门的硬件模块，例如节点、挖矿、钱包和密码模块硬件. 在这里我们主要关注密码模块的测试. 密码模块是指一系列包含于密码边界之中的硬件、软件、固件或其组合的集合，至少使用一个经国家密码管理局认可的密码算法、协议，实现一项或多项已定义的密码服务(如加解密、数字签名、密钥管理等). 由于密码技术对维护信息安全的基础性价值，密码模块一直以来都是安全测试的重要对象[175]. 在我国现有与密码模块安全测

① https://blog.csdn.net/samsho2/article/details/106046997

试相关的技术中,GB/T 18336 和 GM/T 0028 的接受度最高,已被广泛用于大量密码模块的安全测试.

目前国内外针对密码模块的安全测试技术的研究重点是密码算法的标准化.多个国家,如美国、韩国和日本,近几十年来已开始研究密码模块的安全测评.例如,美国颁布了密码模块安全要求联邦信息处理标准 FIPS 140,而中国制定了密码模块安全测评相关技术标准 GB/T 18336(是对国际通用测试技术准则的等同翻译,简称 CC 测试)和 GM/T 0028.CC 测试的认证产品列表中包含了数千款与密码模块相关的产品.与 CC 标准的通用性目的不同,GM/T 0028 标准是专门针对密码模块安全测试而编写的.标准化方法对于保障密码模块安全测试的规范性至关重要,但不能将其视为静态的模板,仍需要不断完善相关的安全测试技术.

针对敏感安全参数泄露的测试技术. 根据国密算法的软件实现过程,需要分析敏感安全参数面临的各种安全威胁,并开展对国密实现过程中敏感安全参数泄露的安全测试技术的研究[176].首先,针对国密算法的软件实现过程,分析该过程中可能存在的敏感安全参数泄露问题,其中包括随机数和密钥数据.随机数发生器是各种密码计算参数的来源[177],包括密钥、初始化向量、随机填充值等,它们应具备足够的随机性(即信息熵),以确保攻击者无法预测.在计算机系统中,已经有大量相关研究,探讨如何利用外界环境的不确定因素(即熵源)构造不可预测且高速的随机数发生器[177].然而,即使是经过多年制定的随机数发生器系列标准,仍然时常出现安全问题的披露.国家密码管理局已发布了 GM/T 0062《密码产品随机数检测要求》标准,该标准的作用类似于美国国家标准技术研究院(NIST)制定的 NIST SP 800-22 标准①.然而,我国尚未发布与随机数发生器相关的其他标准.同时,即使是广泛使用的、公开源代码的随机数发生器实现软件,也存在安全漏洞②.因此,随机数发生器标准并不能完全解决现实密码算法软件引擎中的随机数问题.

侧信道攻击是密码学研究中长久以来的重要方向[176].在密码计算过程中,当密钥比特有不同取值时,密码计算的执行会产生细微差异,从而影响攻击者观测到的外部状态.不论是软件形式还是硬件形式的密码算法实现,都面临侧信道攻击的威胁.此外,由于在计算机系统中,密钥也以内存空间中的数据变量形式存在,因此现有计算机系统中各种敏感数据所面临的攻击和安全问题同样会对密钥造成威胁.另外,各种计算机系统的软件内存漏洞也会导致攻击者非授权地读取密钥.例如,操作系统软件漏洞可能导致恶意进程绕过操作系统的内存隔离机制,读取其他进程甚至内核空间的内存数据.值得一提的是,现有的区块链系统也存在许多安全漏洞[178].

叠加掩码保护. 掩码方法的思想是在不改变运算结果的前提下,使得运算过程中产生的中间结果具有随机性,从而使其物理特征(如功耗)与密钥不再相关.通过对中间数据进行随机化处理,使其与功耗无关,是一种广泛使用的防护方法.典型的掩码方法包括复制法、预计算掩码法、在线计算掩码法、固定掩码法[179]、隐藏掩码法等.

基于深度学习的密码特征识别. 近年来,深度学习在各个领域展现出优于传统机器学习算法的能力[180].因此,可以进行基于深度学习的密码特征识别研究,选择多种不同的深度学习算法,设计密文特征并构建密码算法识别分类器,基于随机性检测指标对多种密码算法进行识别(如之前在密文随机性检测部分讨论的).评估深度学习算法在密码算法识别任务中的有效性,并分析不同网络参数对识别准确率的影响.可以将当前在密码算法识别任务中应用最广泛的随机森林算法[181]作为比较基准,分析深度学习算法在密码算法识别任务中的表现,并对深度学习算法优于随机森林算法的原因进行进一步分析.

其他密评技术的研究. 包括密码协议合规性测试[182]、数字证书的解析[183]、控制流劫持攻击检测[184]、非授权访问密码服务的行为检测等[176].

8 总结与展望

本文主要关注区块链中的公钥密码算法的设计与分析.首先介绍了区块链和公钥密码的概念和理论知识.接着列举并分析了比特币的安全性、隐私性和可扩展性的相关问题,上述问题是开展公钥密码研究的线索和动机.接下来,本文讨论了区块链中涉及的公钥签名、加密和零知识证明,包括研究现状、应用场景、算法定义及安全性,并进行了案例分析.签名方面主要聚焦于 ECDSA、BLS、MLSAG,加密方面主要聚焦于 IBE、CS 和 IND-CCA2 安全的通用构造,零知识证明主要聚焦于 NIZK 和 zk-SNARK

① https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final

② https://csrc.nist.gov/News/2022/proposal-to-revise-sp-800-22-rev-1a

的定义和通用构造. 虽然文中列举了部分 ZKP 案例[168-170]，但未进行具体分析. 更多的案例分析可以参考文献[13].

8.1 总　结

表 6 对本文涉及的案例进行了比较. 总体而言，针对相关公钥密码算法开展安全性归约并非易事，这取决于方案所依赖的具体数学困难问题. 此外，这个过程要求通过形式化的分析来建立算法与数学困难问题之间的严密逻辑关系. 安全归约的开展通常依赖长期从事安全证明方面的经验积累. 由于作者的能力和精力有限，无法对本文涉及的案例进行进一步的分析. 然而，相信读者可以通过反复和正确的学习，跨越证明技巧和分析能力方面的障碍. 接下来，对本文涉及的相关密码算法进行总结.

公钥签名. 签名是区块链中最早采用且最具代表性的公钥密码算法. 早期的区块链主要采用了短签名长度（如 ECDSA）和结构简单的签名方案（如 BLS）. 然而，随着区块链应用的多样化发展以及公民对个人隐私的日益重视，群签名和环签名的研究逐渐成为研究热点. 与 ECDSA 或 BLS 相比，群签名和环签名在设计上更为复杂，并且签名长度随着环的增长而线性递增. 与此同时，这些方案的安全性证明更加复杂，特别是考虑到门限方案（多个签名者）或协议交互式运行的场景. 无论是针对新型签名方案进行设计还是进行分析，读者都需要从经典方案中掌握相关技巧和经验.

表 6　本文涉及的密码算法案例分析[13]

方案	构造及特点	安全性及主要证明技巧
	公钥签名算法案例	
ECDSA[31]	基于 ECDLP 的构造，短签名长度	EU-CMA 安全性，基于矛盾的证明
BLS[32]	构造简单，基于 GDHP 和双线性对	EU-CMA 安全性，基于 Game 的证明
MLSAG[134]	基于 DLP 和 DDHP 的构造，随环线性增长的签名长度	EU-CMA 安全性，基于倒带仿真的证明[63]
	公钥加密算法案例	
IBE[149]	基于混合加密[141]的构造	ROM 模型下 IND-ID-CCA2（见第 5.5 节）安全性，基于错误事件迁移的证明
CS[142]	基于 DDHP 且满足实用安全性的构造	标准模型下 IND-CCA2 安全，基于矛盾的证明
	零知识证明案例分析	
GS08[168]	基于双线性对的 NIZK 构造	基于 NIWI 的安全性，基于推理的证明
GR16[169]	基于双线性对的 NIZK 构造	抗泄露的安全性，基于条件分析的证明
CA17[170]	揭示修改 CRS 带来的安全隐患	提出基于检测 CRS 的改进措施

注：GDHP：基于 Gap Diffie-Hellman 的群组上的困难问题，在该群组上 CDHP 是困难的，而 DDHP 是容易的，NIWI：非交互式证据的不可区分性[168].

公钥加密. 加密是保护数据机密性的基本手段. 尽管大多数公钥加密算法无法满足实时加密的需求，但是实际环境普遍要求公钥密码满足 IND-CCA2. 遵循实现 IND-CCA2 的通用构造方法，读者可以获得构造 IND-CCA2 安全加密算法的多种灵感和启发. 通过对 IBE 和 CS 方案的案例分析，读者不仅可以在设计实用公钥加密方案方面获得指导，还可以循序渐进地掌握（从基础方案到完整方案的）公钥加密构造，以及安全性证明方法. 目前虽然还没有满足 IND-CCA2 安全性的区块链加密标准可供参考，但我们相信任何一个具备 IND-CCA2 安全性且带有严谨安全性证明的算法都足以为区块链提供可靠的安全保障.

零知识证明. 零知识证明是一种能够在证明过程中不泄露任何有效信息的密码原语. 它已经被应用于零钞和零币，并且被其他加密货币广泛研究和使用. 从 ZKP 到实用的 zk-SNARK，我们逐步介绍了相关概念，并简要讨论了构造 zk-SNARK 的通用方法. 具体的，虽然 zk-SNARK 目前被认为是在区块链上实现隐私保护的理想工具，但其构造通常较为复杂，无法在区块链中高效部署和应用. 此外，即使绕过 zk-SNARK 复杂的构造，将 zk-SNARK 直接部署到区块链仍然存在安全隐患. 例如，公共参考字符串（CRS）的生成可能受到恶意攻击，参数初始化依赖可信第三方等. 同时，读者很难在不参考历史研究文献的前提下，弄清楚包括算术电路在内的一系列 ZKP 术语和概念. 这也是为什么我们将 ZKP 章节放在本文末尾的原因. 读者应该从前面的章节中学习到足够的知识和技巧，配合参考文献，逐步了解 ZKP. 总之，ZKP 的研究更像是一个进阶的学习过程，需要读者具备相当的知识储备和长期的跟进学习.

密评和密改. 随着国密 SM 系列算法逐步纳入国际标准并被广泛集成于国际主流密码工具包中，国密算法的重要性日益凸显. 国密算法对于增强我国区块链系统的“安全可控”能力具有重要意义，也

促进了我国的密码算法在新型计算平台上的普及和应用.因此,加强对区块链系统的国密(和商密)测评和改造有助于推动国密(和商密)算法和区块链技术标准的转化应用,为我国密码和区块链产业创造更广阔的发展空间.

8.2 展 望

区块链及其有关公钥密码的发展和应用面临着一系列公开问题和挑战.公钥密码算法的突破通常是通过新的数学理论、对现有算法的新漏洞和弱点的发现和利用,以及总体算力的提升实现的.然而,受限于计算复杂性理论(某些数学问题的复杂性并未得到严密的理论证明)、量子计算威胁以及实施和部署的困难,公钥密码算法在发展的过程中面临着理论和技术瓶颈.上述问题和挑战是当前公钥密码研究和实践中的焦点,并随着技术的发展不断演进.接下来,我们对本文涉及的议题进行展望:

(1)区块链签名的公开问题.在为区块链设计实用的公钥签名方案时,签名大小、安全性、生成签名和验证签名的效率都是关键因素.签名长度与所选群或环的大小呈线性关系,这使得签名难以高效地部署到区块链中,因为区块链中的每个区块通常较小且难以扩展.此外,签名方案需要具备更强的安全性,要求设计依赖尽可能弱的数学猜想,并能够捕捉更实际攻击的安全模型,并在该模型下证明签名的安全性.然而,随着网络攻击和设备异构性等问题的加剧,检测和防御相关攻击并不容易.此外,但随着区块链的可扩展性提高,对签名的验证效率也需要同步提高.解决这些问题需要设计一种高效、短且恒定长度的签名方案,并且具备强大的安全性.上述要求往往意味着要突破区块链的"三元悖论".

(2)区块链加密的公开问题.虽然学者们普遍认为在区块链中部署的公钥加密方案需要满足IND-CCA2安全性来应对实际的安全威胁,但目前已有的构造方法要么依赖理论假设(如随机预言机),要么使用不实用的技术或难以实现的构造(如NIZK)来获得理想的安全性.此外,围绕IND-CCA2加密方案进行安全性分析是一种高度逻辑化的推理过程,依赖于长期从事密码安全证明的技巧和经验.这使得初学者很难进行实际的设计和分析.此外,现有PKE方案在标准模型下实现理想安全性更加困难,因为它们依赖于巧妙的数学证明技术和严密的分析(如在CS方案的安全性分析中讨论超平面相交的情形).此外,另一个需要长期考虑的因素是目前PKE方案的性能不足问题.虽然可以使用对称加密来处理链上数据,但使用公钥加密来处理加密密钥也引出了密钥管理和密钥托管等问题.总之,设计一个同时具备理想安全性和高效性能的PKE方案是一项挑战.

(3)区块链零知识证明的公开问题.零知识证明(ZKP)是构建安全且功能多样的区块链的理想工具.然而,实现ZKP及其实用的变体并不容易.构建通用的zk-SNARK方法可能看起来容易,但需要研究者长期地跟进和耐心地学习相关知识.ZKP的研究通常涉及晦涩的术语和持续的方案演进历史.如果没有持续跟进和长期研习ZKP的历史设计,很难理解其中设计细节的含义和精髓,这使得初学者在阅读ZKP文献时充满困惑.尽管zk-SNARK的研究备受关注,但它通常依赖于可信第三方来执行参数初始化.尽管一些研究给出了解决方案,但相关的补救措施要么带来高昂的计算开销,要么引入了不切实际的假设从而削弱了方案的安全性.总之,设计一个具备去中心化的参数初始化阶段且实用的zk-SNARK方案是一项挑战.

(4)密评的公开问题.在区块链系统中使用密码模块时,设计和实现中的问题可能对区块链的安全性造成严重威胁.这些问题包括设计中未发现的错误或漏洞[176]、密码算法的实现与技术标准不一致等.因此,在将密码模块应用于区块链之前,对其进行一致性测试并确定相应的安全级别非常必要[185].在密码算法的遴选过程中,需要建立全面的评估策略,涵盖安全性、计算开销、底层数学难题或者基础组件等.同时,在密码算法评估过程中,如何自动、快速、高效地检测密码算法的表现至关重要.密码算法的安全性分析是密码算法研究的核心问题,只有在安全性得到保证的情况下才能考虑其他因素.密码技术是信息安全的核心,推广国密算法对于维护我国网络信息安全具有重大意义.然而,我国商用密码产业近年来发展迅速,但国密算法普遍存在实现效率较低的问题[186].为了探索国密算法替代国际密码算法的可行性,需要建立健全的国密算法检测标准体系,包括对国密算法性能和相应产品功能的评估标准.当前国密算法检测标准体系的不完善[186]影响了国产商用密码的进一步发展.

以上问题和挑战是基于当前的研究和实践情况,并可能随着技术的发展和创新而不断演变.

9 结束语

设计具备理想安全性和性能的公钥密码算法,

并对其进行严谨的安全分析和评估，对推动区块链研究和产业的发展具有重要意义. 本文总结了设计和分析相关密码算法的知识、技巧和经验. 文章从浅入深地介绍了相关算法的设计思路和分析技巧，其中包括 8 个案例分析、2 种通用安全模型和 2 种通用算法构造. 此外，本文还讨论了与密评相关的概念和研究，以促进区块链和密码算法按照国家技术标准要求的落地和应用. 考虑到在区块链上进行密码算法设计是一个较新且多学科交叉的研究方向，希望本文能够起到抛砖引玉的作用.

参　考　文　献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. White Paper, 2008

[2] Wood G. Ethereum: A secure decentralized generalised transaction ledger. Ethereum Project Yellow Paper, 2014, 151(2014): 1-32

[3] Miers I, Garman C, Green M, et al. Zerocoin: Anonymous distributed E-cash from Bitcoin//Proceedings of the IEEE Symposium on Security and Privacy. San Francisco, USA, 2013: 397-411

[4] Sasson E B, Chiesa A, Garman C, et al. Zerocash: Decentralized anonymous payments from Bitcoin//Proceedings of the IEEE Symposium on Security and Privacy. San Jose, USA, 2014: 459-474

[5] Diffie W, Hellman M. New directions in cryptography. IEEE Transactions on Information Theory, 1976, 22(6): 644-654

[6] Goldwasser S, Micali S, Rivest R L. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing, 1988, 17(2): 281-308

[7] Bellare M, Rogaway P. Optimal asymmetric encryption// Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques. Perugia, Italy, 1994: 92-111

[8] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof systems. SIAM Journal on Computing, 1989, 18(1): 186-208

[9] Blum M, De Santis A, Micali S, et al. Noninteractive zero-knowledge. SIAM Journal on Computing, 1991, 20(6): 1084-1118

[10] Malone-Lee J. Identity-based signcryption. IACR Cryptology ePrint Archive: Volume 2002. https://eprint.iacr.org/2002/098.pdf

[11] Di Pietro R, Sorniotti A. Boosting efficiency and security in proof of ownership for deduplication//Proceedings of the ACM Symposium on Information, Computer and Communications Security. Seoul, Korea, 2012: 81-82

[12] Anderson P. Perspective: Complexity theory and organization science. Organization Science, 1999, 10(3): 216-232

[13] Huang K, Mu Y, Rezaeibagha F, et al. Design and Analysis of Cryptographic Algorithms in Blockchain. Boca Raton, USA: CRC Press, 2021

[14] Huang K, Mu Y, Rezaeibagha F, et al. Building blockchains with secure and practical public-key cryptographic algorithms: Background, motivations and example. IEEE Network, 2021, 35(6): 240-246

[15] Noether S. Ring signature confidential transactions for Monero. IACR Cryptology ePrint Archive, 2015: 1098

[16] Sun S F, Au M H, Liu J K, et al. RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency Monero//Proceedings of the European Symposium on Research in Computer Security. Oslo, Norway, 2017: 456-474

[17] Yuen T H, Sun S, Liu J K, et al. RingCT 3.0 for blockchain confidential transaction: Shorter size and stronger security// Proceedings of the International Conference on Financial Cryptography and Data Security. Kota Kinabalu, Malaysia, 2020: 464-483

[18] Chuen D L K, Guo L, Wang Y. Cryptocurrency: A new investment opportunity? The Journal of Alternative Investments, 2017, 20(3): 16-40

[19] Kim S, Kwon Y, Cho S. A survey of scalability solutions on blockchain//Proceedings of the International Conference on Information and Communication Technology Convergence. Jeju Island, Korea, 2018: 1204-1207

[20] Cai Xiao-Qing, Deng Yao, Zhang Liang, et al. The principle and core technology of blockchain. Chinese Journal of Computers, 2021, 44(1): 84-131(in Chinese)
(蔡晓晴，邓尧，张亮等. 区块链原理及其核心技术. 计算机学报，2021，44(1)：84-131)

[21] Shan Jin-Yong, Gao Sheng. Research progress on theory of blockchains. Journal of Cryptologic Research, 2018, 5(5): 484-500(in Chinese)
(单进勇，高胜. 区块链理论研究进展. 密码学报，2018，5(5)：484-500)

[22] Liu Ming-Da, Chen Zuo-Ning, Shi Yi-Juan, et al. Research progress of blockchain in data security. Chinese Journal of Computers, 2021, 44(1): 1-27(in Chinese)
(刘明达，陈左宁，拾以娟等. 区块链在数据安全领域的研究进展. 计算机学报，2021，44(1)：1-27)

[23] Zhu Lie-Huang, Gao Feng, Shen Meng, et al. Survey on privacy preserving techniques for blockchain technology. Journal of Computer Research and Development, 2017, 54(10): 2170-2186(in Chinese)
(祝烈煌，高峰，沈蒙等. 区块链隐私保护研究综述. 计算机研究与发展，2017，54(10)：2170-2186)

[24] Conti M, Kumar E S, Lal C, et al. A survey on security and privacy issues of Bitcoin. IEEE Communications Surveys & Tutorials, 2018, 20(4): 3416-3452

[25] Zhang Rui, Xue Rui, Liu Ling. Security and privacy on blockchain. ACM Computing Surveys, 2019, 52(3): 1-34

[26] Tschorsch F, Scheuermann B. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 2016, 18(3): 2084-2123

[27] Zheng Z, Xie S, Dai H N, et al. Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 2018, 14(4): 352-375

[28] Li Wei-Han, Zhang Zong-Yang, Zhou Zi-Bo, et al. An overview on succinct non-interactive zero-knowledge proofs. Journal of Cryptologic Research, 2022, 9(3): 379-447(in Chinese)
(李威翰, 张宗洋, 周子博等. 简洁非交互零知识证明综述. 密码学报, 2022, 9(3): 379-447)

[29] Blum M, Feldman P, Micali S. Non-interactive zero-knowledge and its applications. Goldreich O ed. Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali. New York, USA: ACM, 2019: 329-349

[30] Zhao Zhen, Wu Ge, Lai Jian-Chang, et al. Key points and methodology in constructions and security proofs of public-key cryptosysems. Journal of Cryptologic Research, 2019, 6(1): 1-17(in Chinese)
(赵臻, 吴戈, 赖建昌等. 公钥密码方案构造及安全证明的知识要点和方法论. 密码学报, 2019, 6(1): 1-17)

[31] Rivest R L, Hellman M E, Anderson J C, et al. Responses to NIST's proposal. Communications of the ACM, 1992, 35(7): 41-54

[32] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Gold Coast, Australia, 2001: 514-532

[33] Naor M, Yung M. Public-key cryptosystems provably secure against chosen ciphertext attacks//Proceedings of the Annual ACM Symposium on Theory of Computing. Atlanta Georgia, USA, 1990: 427-437

[34] Rackoff C, Simon D R. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack//Proceedings of the Advances in Cryptology. Brighton, UK, 2001: 433-444

[35] Goldwasser S, Micali S. Probabilistic encryption. Journal of Computer and System Sciences, 1984, 28(2): 270-299

[36] Bellare M, Kilian J, Rogaway P. The security of the cipher block chaining message authentication code. Journal of Computer and System Sciences, 2000, 61(3): 362-399

[37] Parno B, Howell J, Gentry C, et al. Pinocchio: Nearly practical verifiable computation//Proceedings of the IEEE Symposium on Security and Privacy. Berkeley, USA, 2013: 238-252

[38] Wahby R S, Setty S, Howald M, et al. Efficient RAM and control flow in verifiable outsourced computation. IACR Cryptology ePrint Archive, 2014. https://eprint.iacr.org/2014/674.pdf

[39] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols//Proceedings of the ACM Conference on Computer and Communications Security. Fairfax, USA, 1993: 62-73

[40] Cramer R, Shoup V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Amsterdam, The Netherland, 2002: 45-64

[41] Delgado-Segura S, Pérez-Sola C, Navarro-Arribas G, et al. Analysis of the Bitcoin UTXO set//Proceedings of the Financial Cryptography and Data Security. Nieuwpoort, Netherlands, 2019: 78-91

[42] Bitansky N, Chiesa A, Ishai Y, et al. Succinct non-interactive arguments via linear interactive proofs//Proceedings of the Theory of Cryptography Conference. Tokyo, Japan, 2013: 315-333

[43] Ben-Sasson E, Chiesa A, Tromer E, et al. Succinct non-interactive zero knowledge for a Von Neumann architecture//Proceedings of the USENIX Security Symposium. San Diego, USA, 2014: 781-796

[44] Ben-Sasson E, Bentov I, Horesh Y, et al. Scalable, transparent, and post-quantum secure computational integrity. IACR Cryptology ePrint Archive, 2018: 46. https://eprint.iacr.org/2018/046

[45] Guo Fu-Chun, Susilo W, Mu Yi. Introduction to Security Reduction. Berlin, Germany: Springer, 2018

[46] Garay J, Kiayias A, Leonardos N. The Bitcoin backbone protocol: Analysis and applications//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Sofia, Bulgaria, 2015: 281-310

[47] Freeman D M. Converting pairing-based cryptosystems from composite-order groups to prime-order groups//Proceedings of the Advances in Cryptology. French Riviera, French, 2010: 44-61

[48] Alberto Torres W, Kuchta V, Steinfeld R, et al. Lattice RingCT v2. 0 with multiple input and multiple output wallets //Proceedings of the Information Security and Privacy. Christchurch, New Zealand, 2019: 156-175

[49] Manson S M. Simplifying complexity: A review of complexity theory. Geoforum, 2001, 32(3): 405-414

[50] Cook S A. The complexity of theorem-proving procedures//Kapron B M ed. Logic, Automata, and Computational Complexity: The Works of Stephen A. Cook. New York, USA: ACM, 2023: 143-152

[51] Karp R M. Reducibility Among Combinatorial Problems. Berlin, Germany: Springer, 2010

[52] Bellare M. Practice-oriented provable-security//Proceedings of the Information Security. Tatsunokuchi, Ishikawa, Japan, 1998: 221

[53] Sprenger C, Basin D, Backes M, et al. Cryptographically sound theorem proving//Proceedings of the IEEE Computer Security Foundations Workshop. Venice, Italy, 2006: 153-166

[54] Feng Deng-Guo. Research on theory and approach of provable security. Journal of Software, 2005, 16(10): 1743-1756(in Chinese)

(冯登国. 可证明安全性理论与方法研究. 软件学报，2005，16(10)：1743-1756)

[55] Gentry C，Ramzan Z. Eliminating random permutation oracles in the even-mansour cipher//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Jeju Island，Korea，2004：32-47

[56] Canetti R，Goldreich O，Halevi S. The random oracle methodology，revisited. Journal of the ACM，2004，51(4)：557-594

[57] Katz J，Lindell Y. Introduction to Modern Cryptography. Boca Raton，Florida，USA：CRC Press，2014

[58] Coron J S. On the exact security of full domain hash//Proceedings of the Annual International Cryptology Conference. Santa Barbara，USA，2000：229-235

[59] Shacham H，Waters B. Compact proofs of retrievability. Journal of Cryptology，2013，26(3)：442-483

[60] Dent A W. A note on game-hopping proofs. IACR Cryptology ePrint Archive，2006. https：//eprint. iacr. org/2006/260

[61] Shoup V. Sequences of games：A tool for taming complexity in security proofs. IACR Cryptology ePrint Archive，2004. https：//eprint. iacr. org/2004/332. pdf

[62] Fuchsbauer G，Orrù M，Seurin Y. Aggregate cash systems：A cryptographic investigation of MimbleWimble//Proceedings of the Advances in Cryptology. Darmstadt，Germany，2019：657-689

[63] Liu J K，Wei V K，Wong D S. Linkable spontaneous anonymous group signature for ad hoc groups//Proceedings of the Australasian Conference on Information Security and Privacy. Sydney，Australia，2004：325-335

[64] Pedersen T P. Non-interactive and information-theoretic secure verifiable secret sharing//Proceedings of the Annual International Cryptology Conference. Santa Barbara，USA，1991：129-140

[65] Wang Zi-Yu，Yu Hui，Zhang Zong-Yang，et al. ECDSA weak randomness in Bitcoin. Future Generation Computer Systems，2020，102：507-513

[66] Volety T，Saini S，McGhin T，et al. Cracking Bitcoin wallets：I want what you have in the wallets. Future Generation Computer Systems，2019，91：136-143

[67] Wijaya D A，Liu J，Steinfeld R，et al. Monero ring attack：Recreating zero mixin transaction effect//Proceedings of the 2018 TrustCom/BigDataSE. New York，USA，2018：1196-1201

[68] Grimes R A. Cryptography Apocalypse：Preparing for the Day When Quantum Computing Breaks Today's Crypto. Hoboken，USA：John Wiley & Sons，2019

[69] Li Ying-Xin，Liu Fu-Kang，Wang Gao-Li. New records in collision attacks on RIPEMD-160 and SHA-256. 2023. 02. 23. https：//eprint. iacr. org/2023/285

[70] Chen L，Chen L，Jordan S，et al. Report on post-quantum cryptography：Volume 12. US Department of Commerce，National Institute of Standards and Technology，2016

[71] Boneh D，Drijvers M，Neven G. Compact multi-signatures for smaller blockchains//Proceedings of the Advances in Cryptology. Brisbane，Australia，2018：435-464

[72] Rivest R L，Shamir A，Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM，1978，21(2)：120-126

[73] Zheng Zi-Bin，Xie Shao-An，Dai Hong-Ning，et al. An overview of blockchain technology：Architecture，consensus，and future trends//Proceedings of the IEEE International Congress on Big Data. Boston，USA，2017：557-564

[74] Tian Min-Qiu，Fu Da-Peng，Ma Yuan，et al. Security requirements and evaluation practices for cryptographic applications in level protection information systems. Computer Engineering and Applications，2018，54(S2)：1-18(in Chinese)
(田敏求，傅大鹏，马原等. 面向等级保护的信息系统密码应用安全要求与测评实践. 计算机工程与应用，2018，54(S2)：1-18)

[75] Huo Wei，Guo Qi-Quan，Ma Yuan. Commercial Cryptography Application and Security Assessment. Beijing：Publishing House of Electronics Industry，2020(in Chinese)
(霍炜，郭启全，马原. 商用密码应用与安全性评估. 北京：电子工业出版社，2020)

[76] Bonneau J，Narayanan A，Miller A，et al. Mixcoin：Anonymity for Bitcoin with accountable mixes//Proceedings of the Financial Cryptography and Data Security. Christ Church，Barbados，2014：486-504

[77] Valenta L，Rowan B. Blindcoin：Blinded，accountable mixes for Bitcoin//Proceedings of the Financial Cryptography and Data Security. San Juan，USA，2015：112-126

[78] Ruffing T，Moreno-Sanchez P，Kate A. CoinShuffle：Practical decentralized coin mixing for Bitcoin//Proceedings of the Computer Security. Wroclaw，Poland，2014：345-364

[79] Ziegeldorf J H，Grossmann F，Henze M，et al. CoinParty：Secure multiparty mixing of Bitcoins//Proceedings of the ACM Conference on Data and Application Security and Privacy. San Antonio，USA，2015：75-86

[80] Yao Shuang，Zhang Da-Wei，Li Yong，et al. A survey on privacy protection of transaction content in blockchain. Journal of Cryptologic Research，2022，9(4)：596-618(in Chinese)
(姚爽，张大伟，李勇等. 区块链交易内容隐私保护技术研究综述. 密码学报，2022，9(4)：596-618)

[81] Poelstra A，Back A，Friedenbach M，et al. Confidential assets //Proceedings of the International Conference on Financial Cryptography and Data Security. Curaçao，the Netherlands，2018：43-63

[82] Kang H，Dai T，Jean-Louis N，et al. FabZK：Supporting privacy-preserving，auditable smart contracts in hyperledger fabric//Proceedings of the Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Portland，USA，2019：543-555

[83] Paillier P. Public-key cryptosystems based on composite degree residuosity classes//Proceedings of the Advances in Cryptology. Czech Republic, 1999: 223-238

[84] Zheng Hai-Bin, Wu Qian-Hong, Xie Jan, et al. An organization-friendly blockchain system. Computers & Security, 2020, 88: 101598

[85] Wang Qin, Qin Bo, Hu Jian-Kun, et al. Preserving transaction privacy in Bitcoin. Future Generation Computer Systems, 2020, 107: 793-804

[86] Yaji S, Bangera K, Neelima B. Privacy preserving in blockchain based on partial homomorphic encryption system for AI applications//Proceedings of the International Conference on High Performance Computing Workshops. Bengaluru, India, 2018: 81-85

[87] Chen Y, Ma X, Tang C, et al. PGC: Decentralized confidential payment system with auditability//Proceedings of the European Symposium on Research in Computer Security. Guildford, UK, 2020: 591-610

[88] Chen Y, Ma X, Tang C, et al. PGC: Decentralized confidential payment system with auditability. IACR Cryptology ePrint Archive, 2019. https://eprint. iacr. org/2019/319. pdf

[89] Yuen T H, Liu J K, Au M H, et al. Efficient linkable and/or threshold ring signature without random oracles. The Computer Journal, 2013, 56(4): 407-421

[90] Au M H, Liu J K, Susilo W, et al. Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction. Theoretical Computer Science, 2013, 469: 1-14

[91] Groth J. Short pairing-based non-interactive zero-knowledge arguments//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Singapore, 2010: 321-340

[92] Bünz B, Bootle J, Boneh D, et al. Bulletproofs: Short proofs for confidential transactions and more//Proceedings of the IEEE Symposium on Security and Privacy. San Francisco, USA, 2018: 315-334

[93] Garman C, Green M, Miers I, et al. Rational zero: Economic security for zerocoin with everlasting anonymity//Proceedings of the International Conference on Financial Cryptography and Data Security. Christ Church, Barbados, 2014: 140-155

[94] Danezis G, Fournet C, Kohlweiss M, et al. Pinocchio coin: Building Zerocoin from a succinct pairing-based proof system//Proceedings of the ACM Workshop on Language Support for Privacy-Enhancing Technologies. Berlin, Germany, 2013: 27-30

[95] Kuo T T, Zavaleta Rojas H, Ohno-Machado L. Comparison of blockchain platforms: A systematic review and healthcare examples. Journal of the American Medical Informatics Association, 2019, 26(5): 462-478

[96] Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: A distributed operating system for permissioned blockchains//Proceedings of the EuroSys Conference. Porto, Portugal, 2018: 1-15

[97] Zeng Shi-Qin, Huo Ru, Huang Tao, et al. Survey of blockchain: Principle, progress and application. Journal on Communications, 2020, 41(1): 134-151(in Chinese)
(曾诗钦, 霍如, 黄韬等. 区块链技术研究综述: 原理、进展与应用. 通信学报, 2020, 41(1): 134-151)

[98] Hearn M, Brown R G. Corda: A distributed ledger. Corda Technical Whitepaper, Retrieved, 2016, 27: 2018

[99] Baliga A, Subhod I, Kamat P, et al. Performance evaluation of the quorum blockchain platform. arXiv preprint arXiv: 1809.03421, 2018

[100] Ali M, Nelson J, Shea R, et al. Blockstack: A global naming and storage system secured by blockchains//Proceedings of the USENIX Annual Technical Conference. Denver, USA, 2016: 181-194

[101] Dong Gui-Shan, Chen Yu-Xiang, Fan Jia, et al. Research on privacy protection strategies in blockchain application. Computer Science, 2019, 46(5): 29-35(in Chinese)
(董贵山, 陈宇翔, 范佳等. 区块链应用中的隐私保护策略研究. 计算机科学, 2019, 46(5): 29-35)

[102] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts//Proceedings of the IEEE Symposium on Security and Privacy. Fairmont, San Jose, USA, 2016: 839-858

[103] Shi Jin-Shan, Li Ru. Survey of blockehain access control in Internet of Things. Journal of Software, 2019, 30(6): 1632-1648(in Chinese)
(史锦山, 李茹. 物联网下的区块链访问控制综述. 软件学报, 2019, 30(6): 1632-1648)

[104] Shafagh H, Burkhalter L, Hithnawi A, et al. Towards blockchain-based auditable storage and sharing of IoT data//Proceedings of the 2017 on Cloud Computing Security Workshop. Dallas, USA, 2017: 45-50

[105] Zhang Yuan-Yu, Kasahara S, Shen Yu-Long, et al. Smart contract based access control for the Internet of Things. IEEE Internet of Things Journal, 2018, 6(2): 1594-1605

[106] Croman K, Decker C, Eyal I, et al. On scaling decentralized blockchains: (A position paper)//Proceedings of the Financial Cryptography and Data Security. Christ Church, Barbados, 2016: 106-125

[107] Wang Jia-Ping, Wang Hao. Monoxide: Scale out blockchains with asynchronous consensus zones//Proceedings of the USENIX Symposium on Networked Systems Design and Implementation. Boston, USA, 2019: 95-112

[108] Kedziora M, Pieprzka D, Jozwiak I, et al. Analysis of segregated witness implementation for increasing efficiency and security of the Bitcoin cryptocurrency. Journal of Information and Telecommunication, 2023, 7(1): 44-55

[109] Luu L, Narayanan V, Zheng C, et al. A secure sharding protocol for open blockchains//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. Hofburg Palace, Australia, 2016: 17-30

[110] Rivest R L, Shamir A. PayWord and MicroMint: Two simple micropayment schemes. Lecture Notes in Computer Science, 1997, 1189: 69-88

[111] Eyal I, Gencer A E, Sirer E G, et al. Bitcon-NG: A scalable blockchain protocol//Proceedings of the USENIX Symposium on Networked Systems Design and Implementation. Santa Clara, USA, 2016: 45-59

[112] Yu Hui, Zhang Zong-Yang, Liu Jian-Wei. Research on scaling technology of Bitcoin blockchain. Journal of Computer Research and Development, 2017, 54(10): 2390-2403 (in Chinese)
(喻辉, 张宗洋, 刘建伟. 比特币区块链扩容技术研究. 计算机研究与发展, 2017, 54(10): 2390-2403)

[113] Yao Qian, Zhang Da-Wei. Survey on identity management in blockchain. Journal of Software, 2021, 32(7): 2260-2286(in Chinese)
(姚前, 张大伟. 区块链系统中身份管理技术研究综述. 软件学报, 2021, 32(7): 2260-2286)

[114] Mao Ge, Li Jing, Zhu Qiao, et al. Application prospect of blockchain technology in medical field. Journal of Hubei University(Natural Science), 2021, 43(1): 1-5(in Chinese)
(毛戈, 李晶, 朱乔等. 区块链技术在医疗领域中的应用前景. 湖北大学学报(自然科学版), 2021, 43(1): 1-5)

[115] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 1985, 31(4): 469-472

[116] Miller V S. The Weil pairing, and its efficient calculation. Journal of Cryptology, 2004, 17(4): 235-261

[117] Rabin M O. Digitalized signatures and public key cryptosystems as intractable as factorization. MIT/LCS/TR212, Technical Report, Massachusetts Institute of Technology, Cambridge, USA, 1979

[118] Schnorr C P. Efficient identification and signatures for smart cards//Proceedings of the Conference on the Theory and Application of Cryptology. Houthalen, Belgium, 1989: 239-252

[119] Nyberg K, Rueppel R A. A new signature scheme based on the DSA giving message recovery//Proceedings of the ACM Conference on Computer and Communications Security. Fairfax, USA, 1993: 58-61

[120] Morain F. Building cyclic elliptic curves modulo large primes //Proceedings of the Advances in Cryptology. Brighton, UK, 1991: 328-336

[121] Pornin T. Deterministic usage of the digital signature algorithm (DSA) and elliptic curve digital signature algorithm (ECDSA). RFC 6979, 2013. https://datatracker.ietf.org/doc/html/rfc6979

[122] Vaudenay S. The security of DSA and ECDSA//Proceedings of the International Workshop on Public Key Cryptography. Miami, USA, 2003: 309-323

[123] Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm(ECDSA). International Journal of Information Security, 2001, 1(1): 36-63

[124] Brown D R. The exact security of ECDSA//Proceedings of the Advances in Elliptic Curve Cryptography. Santa Barbara, USA, 2000

[125] Pointcheval D, Stern J. Security proofs for signature schemes//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Saragossa, Spain, 1996: 387-398

[126] Brickell E, Pointcheval D, Vaudenay S, et al. Design validations for discrete logarithm based signature schemes// Proceedings of the International Workshop on Public Key Cryptography. Melbourne, Australia, 2000: 276-292

[127] De Dormale G M, Quisquater J J. High-speed hardware implementations of elliptic curve cryptography: A survey. Journal of Systems Architecture, 2007, 53(2/3): 72-84

[128] Driessen B, Poschmann A, Paar C. Comparison of innovative signature algorithms for WSNs//Proceedings of the ACM Conference on Wireless Network Security. Alexandria, USA, 2008: 30-35

[129] Fan J, Verbauwhede I. An updated survey on secure ECC implementations: Attacks, countermeasures and cost//Naccache D ed. Cryptography and Security: From Theory to Applications. Berlin, Germany: Springer, 2012: 265-282

[130] Abdouli A S, Baek J, Yeun C Y. Survey on computationally hard problems and their applications to cryptography// Proceedings of the International Conference for Internet Technology and Secured Transactions. Abu Dhabi, UAE, 2011: 46-52

[131] Danger J L, Guilley S, Hoogvorst P, et al. A synthesis of side-channel attacks on elliptic curve cryptography in smartcards. Journal of Cryptographic Engineering, 2013, 3(4): 241-265

[132] Hanke T, Movahedi M, Williams D. Dfinity technology overview series, consensus system. arXiv preprint arXiv: 1805.04548, 2018

[133] Gilad Y, Hemo R, Micali S, et al. Algorand: Scaling byzantine agreements for cryptocurrencies//Proceedings of the Symposium on Operating Systems Principles. Shanghai, China, 2017: 51-68

[134] Noether S, Mackenzie A. Ring confidential transactions. Ledge, 2016, 1: 1-18. http://ledger.pitt.edu/ojs/ledger/article/download/34/61

[135] Ohta K, Okamoto T. On concrete security treatment of signatures derived from identification//Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA, 1998: 354-369

[136] Fujisaki E, Suzuki K. Traceable ring signature//Proceedings of the International Workshop on Public Key Cryptography. Beijing, China, 2007: 181-200

[137] Möser M, Soska K, Heilman E, et al. An empirical analysis of traceability in the Monero blockchain. arXiv preprint arXiv:1704.04299, 2017

[138] Huang K, Mu Y, Rezaeibagha F, et al. Monero with multi-grained redaction. IEEE Transactions on Dependable and Secure Computing, 2023, 21(1): 241-253

[139] Hankerson D, Menezes A J, Vanstone S. Guide to Elliptic Curve Cryptography. New York, USA: Springer, 2004

[140] Fujisaki E, Okamoto T. How to enhance the security of public-key encryption at minimum cost//Proceedings of the International Workshop on Public Key Cryptography. Kamakura, Japan, 1999: 53-68

[141] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes//Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA, 1999: 537-554

[142] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack//Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA, 1998: 13-25

[143] Canetti R, Halevi S, Katz J. Chosen-ciphertext security from identitybased encryption//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Interlaken, Switzerland, 2004: 207-222

[144] Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles//Proceedings of the Advances in Cryptology. Interlaken, Switzerland, 2004: 223-238

[145] Cramer R, Shoup V. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing, 2003, 33(1): 167-226

[146] Kurosawa K, Desmedt Y. A new paradigm of hybrid encryption scheme//Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA, 2004: 426-442

[147] Kiltz E. Chosen-ciphertext secure key-encapsulation based on gap hashed Diffie-Hellman//Proceedings of the International Workshop on Public Key Cryptography. Beijing, China, 2007: 282-297

[148] Abdalla M, Bellare M, Rogaway P. Dhaes: An encryption scheme based on the Diffie-Hellman problem. IACR Cryptology ePrint Archive, 1999: 7. https://cseweb.ucsd.edu/mihir/papers/dhies.pdf

[149] Boneh D, Franklin M. Identity-based encryption from the Weil pairing//Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA, 2001: 213-229

[150] Jiang Peng, Guo Fu-Chun, Liang Kai-Tai, et al. Searchain: Blockchain-based private keyword search in decentralized storage. Future Generation Computer Systems, 2020, 107: 781-792

[151] Derler D, Samelin K, Slamanig D, et al. Fine-grained and controlled rewriting in blockchains: Chameleon-hashing gone attribute-based//Proceedings of the Network and Distributed System Security Symposium. San Diego, USA, 2019

[152] Xu Sheng-Min, Ning Jian-Ting, Ma Jin-Hua, et al. Revocable policy-based chameleon hash//Proceedings of the European Symposium on Research in Computer Security. Darmstadt, Germany, 2021: 327-347

[153] Zhang Yuan, Xu Chun-Xiang, Lin Xiao-Dong, et al. Blockchain-based public integrity verification for cloud storage against procrastinating auditors. IEEE Transactions on Cloud Computing, 2019, 9(3): 923-937

[154] Xie Tian-Cheng, Zhang Jia-Heng, Zhang Yu-Peng, et al. Libra: Succinct zero-knowledge proofs with optimal prover computation//Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA, 2019: 733-764

[155] Ben-Sasson E, Chiesa A, Genkin D, et al. SNARKs for C: Verifying program executions succinctly and in zero knowledge//Proceedings of the Annual Cryptology Conference. Santa Barbara, USA, 2013: 90-108

[156] Braun B, Feldman A J, Ren Z, et al. Verifying computations with state//Proceedings of the ACM Symposium on Operating Systems Principles. Farmington, USA, 2013: 341-357

[157] Gennaro R, Gentry C, Parno B, et al. Quadratic span programs and succinct NIZKs without PCPs//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Athens, Greece, 2013: 626-645

[158] Groth J. Simulation-sound NIZK proofs for a practical language and constant size group signatures//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Shanghai, China, 2006: 444-459

[159] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems//Proceedings of the Advances in Cryptology. Santa Barbara, USA, 1986: 186-194

[160] Benaloh J, De Mare M. One-way accumulators: A decentralized alternative to digital signatures//Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques. Lofthus, Norway, 1993: 274-285

[161] Bünz B, Agrawal S, Zamani M, et al. Zether: Towards privacy in a smart contract world//Proceedings of the International Conference on Financial Cryptography and Data Security. Kota Kinabalu, Malaysia, 2020

[162] Boneh D, Boyen X. Secure identity based encryption without random oracles//Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA, 2004: 443-459

[163] Gennaro R. Multi-trapdoor commitments and their applications to proofs of knowledge secure under concurrent man-in-the-middle attacks//Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA, 2004: 220-236

[164] Gentry C, Wichs D. Separating succinct non-interactive arguments from all falsifiable assumptions//Proceedings of the Annual ACM Symposium on Theory of Computing. San Jose, USA, 2011: 99-108

[165] Bitansky N, Canetti R, Chiesa A, et al. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again//Proceedings of the Innovations in Theoretical Computer Science Conference. Cambridge, USA, 2012: 326-349

[166] Buterin V. Quadratic arithmetic programs: From zero to hero. https://medium.com/@VitalikButerin/quadratic-arithmeticprograms-from-zero-to-hero-f6d558cea649

[167] Banerjee A, Clear M, Tewari H. Demystifying the role of zk-SNARKs in zcash//Proceedings of the IEEE Conference on Application, Information and Network Security (AINS). Kota Kinabalu, Malaysia, 2020: 12-19

[168] Groth J, Sahai A. Efficient non-interactive proof systems for bilinear groups//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Istanbul, Turkey, 2008: 415-432

[169] Groth J. On the size of pairing-based non-interactive arguments//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vienna, Austria, 2016: 305-326

[170] Campanelli M, Gennaro R, Goldfeder S, et al. Zero-knowledge contingent payments revisited: Attacks and payments for services//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. Dallas, USA, 2017: 229-243

[171] Maller M, Bowe S, Kohlweiss M, et al. Sonic: Zero-knowledge snarks from linear-size universal and updatable structured reference strings//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. London, UK, 2019: 2111-2128

[172] Bowe S, Grigg J, Hopwood D. Recursive proof composition without a trusted setup. IACR Cryptology ePrint Archive, 2019. https://eprint.iacr.org/2019/1021.pdf

[173] Chiesa A, Hu Y, Maller M, et al. Marlin: Preprocessing zkSNARKs with universal and updatable SRS//Proceedings of the Advances in Cryptology. Zagreb, Croatia, 2020: 738-768

[174] Gabizon A, Williamson Z J, Ciobotaru O. Plonk: Permutations over Lagrange-bases for oecumenical noninteractive arguments of knowledge. IACR Cryptology ePrint Archive, 2019. https://eprint.iacr.org/2019/953.pdf

[175] Shi Hong-Song, Li He-Xing, Yang Yong-Sheng. Ideas and methods for cryptographic module security evaluation. China Information Security, 2018, (9): 96-99(in Chinese)
(石竑松，李贺鑫，杨永生. 密码模块安全测评的思路和方法. 中国信息安全，2018，(9)：96-99)

[176] Chen Hua, Xi Wei, Fan Li-Min, et al. Side channel analysis and evaluation on cryptographic products. Journal of Electronics & Information Technology, 2020, 42(8): 1836-1845(in Chinese)
(陈华，习伟，范丽敏等. 密码产品的侧信道分析与评估. 电子与信息学报，2020，42(8)：1836-1845)

[177] Ma Yuan, Chen Tian-Yu, Wu Xin-Ying, et al. Design, implementation and testing of random number generators. Journal of Information Security Research, 2019, 5(1): 39-49(in Chinese)
(马原，陈天宇，吴鑫莹等. 随机数发生器的设计与检测. 信息安全研究，2019，5(1)：39-49)

[178] Chen Ting, Li Zi-Hao, Zhu Yu-Xiao, et al. Understanding Ethereum via graph analysis. ACM Transactions on Internet Technology, 2020, 20(2): 1-32

[179] Li Lang, Jiao Ge, Li Ren-Fa, et al. Research of ECC algorithm resistant to power analysis attacks. Microelectronics & Computer, 2011, 28(1): 27-30(in Chinese)
(李浪，焦铬，李仁发等. 一种 ECC 加密芯片抗功耗攻击研究. 微电学与计算机，2011，28(1)：27-30)

[180] Chen Yi, Shen Yan-Tian, Yu Hong-Bo. Analysis and improvements of deep learning-based key recovery attack. Journal of Cryptologic Research, 2023, 10(1): 168-180(in Chinese)
(陈怡，申焱天，于红波. 对基于深度学习的密钥恢复攻击的分析与改进. 密码学报，2023，10(1)：168-180)

[181] Huang Liang-Tao, Zhao Zhi-Cheng, Zhao Ya-Qun. A two-stage cryptosystem recognition scheme based on random forest. Chinese Journal of Computers, 2018, 41(2): 382-399(in Chinese)
(黄良韬，赵志诚，赵亚群. 基于随机森林的密码体制分层识别方案. 计算机学报，2018，41(2)：382-399)

[182] Zhang Huan-Guo, Wu Fu-Sheng, Wang Hou-Zhen, et al. A survey: Security verification analysis of cryptographic protocols implementations on real code. Chinese Journal of Computers, 2018, 41(2): 288-308(in Chinese)
(张焕国，吴福生，王后珍等. 密码协议代码执行的安全验证分析综述. 计算机学报，2018，41(2)：288-308)

[183] Ou Hai-Wen, Wang Yu-Xiao, Ouyang Chen, et al. SM2-based digital certificate parsing and validity verification. Journal of Computer Applications, 2016, 36(S1): 46-48(in Chinese)
(欧海文，王誉晓，欧阳琛等. 基于 SM2 算法的数字证书解析及有效性验证. 计算机应用，2016，36(S1)：46-48)

[184] Wang Feng-Feng, Zhang Tao, Xu Wei-Guang, et al. Overview of control-flow hijacking attack and defense techniques for process. Chinese Journal of Network and Information Security, 2019, 5(6): 10-20(in Chinese)
(王丰峰，张涛，徐伟光等. 进程控制流劫持攻击与防御技术综述. 网络与信息安全学报，2019，5(6)：10-20)

[185] Zhang Fang-Yu, Lin Jing-Qiang, Wei Rong, et al. Research progresses on security applications of cryptography and discussions on validation of software cryptographic modules. Journal of Cryptologic Research, 2020, 7(3): 290-310(in Chinese)
(郑昉昱, 林璟锵, 魏荣等. 密码应用安全技术研究及软件密码模块检测的讨论. 密码学报, 2020, 7(3): 290-310)

[186] Hu Jing-Xiu, Yang Yang, Xiong Lu, et al. Guomi algorithm analysis and software performance research analysis. Netinfo Security, 2021, 21(10): 8-16(in Chinese)
(胡景秀, 杨阳, 熊璐等. 国密算法分析与软件性能研究. 信息网络安全, 2021, 21(10): 8-16)

HUANG Ke, Ph. D., associate professor. His research interests are applied cryptography and blockchain.

LI Xiong, Ph. D., professor. His research interests focus on applied cryptography.

YUAN Sheng, M. S. candidate. His research interests include Satellite Internet and applied cryptography.

LIU Xing-Yu, M. S. candidate. His research interests include software security and applied cryptography.

ZHANG Xiao-Song, Ph. D., professor, His research interests are blockchain security, AI security, etc.

Background

The success of cryptocurrencies has attracted researchers worldwide to study blockchain. Understanding the underlying cryptographic algorithms is crucial for advancements in both cryptography and cryptocurrencies. The concept of Public-Key Algorithms (PKC) introduced by Diffie and Hellman in 1976 has inspired research in digital signatures, encryption, and other primitives. However, validating PKC schemes can be challenging for beginners due to the interdisciplinary nature and high entry level.

Blockchain technology is evolving towards versatile applications, where PKC plays a vital role in addressing security and privacy concerns. Blockchain imposes strict requirements on the performance and security of PKC algorithms. Formalizing and validating blockchain-based PKC is crucial for the feasibility of successful cryptocurrencies. However, this task is non-trivial as it involves algorithmic design, defining achievable security goals, concrete implementation, and efficient security reductions. These challenges are magnified in the decentralized and trustless nature of blockchains. This work aims to address the challenges in designing and analyzing practical PKC for blockchain. Unlike existing surveys, we focus on the formalization and validation of PKC. By presenting 8 cryptographic schemes and 2 generic methods, we provide necessary techniques and experiences for implementing blockchain-based PKC. This article also delves into security evaluation concepts and research to support the implementation and application of blockchain-based cryptographic technology in compliance with national technical standards. Finally, we conclude the paper and highlight future challenges. Our ultimate goal is to inspire rigorous and long-term research in cryptography and blockchain.

This work was supported in part by the National Natural Science Foundation of China under Grant Nos. 62002048, 62332018, U19A2066, 62072078, U22B2029, the Basic Program of Sichuan Province Science Foundation under Grant No. 2022-NSFSC0876, the Science and Technology Project of State Grid Corporation of China under Grant No. 5700-202355311A-1-1-ZN and the Chengdu Jiaozi Financial Holding Group Company Ltd.