科学技术与教育 2025年第2期
ISSN: 3079-4455

区块链密码学的隐私保护技术综述

胡薇，撒靓瑶*
昭通学院数学与统计学院，云南昭通，中国
*通讯作者

【摘要】随着区块链技术在金融、供应链、医疗等领域的深入应用，隐私保护问题日益凸显。传统的区块链系统因其透明性和不可篡改性，难以满足对隐私保护的高要求。为此，密码学技术成为解决区块链隐私保护问题的关键。本文综述了当前区块链密码学中的主流隐私保护技术，包括零知识证明、同态加密、安全多方计算和后量子密码学，分析了它们的技术原理、研究进展及面临的挑战。

【关键词】区块链；密码学；隐私保护技术

1.引言

2008 年，Nakamoto 发表论文《Bitcoin: A peer-to-peer electronic cash system》，标志着比特币的诞生[1].比特币是第一个也是至今最为流行的加密货币，相较于其他货币而言，比特币最大的优势在于能够在没有中央管理机制并且参与者不可信的环境下进行可信交易[2]。2009 年，在序号为 0 和 1 的比特币区块相继出现后，序号为 1 的区块出现并于序号为 0 的区块相连接形成了链，标志着区块链的诞生[3]。区块链实际上是去中心化的巨大的账本数据库，在区块链网络中，交易基于密码学原理，所以区块链的隐私保护问题就极为重要。

区块链系统是由数据层、网络层、共识层、激励层、合约层和应用层几个部分组成。在数据层，零知识证明、多方安全计算等技术可以在数据存储和传输过程中保护数据的隐私；在共识层，同态加密技术可以在数据加密的情况下进行计算和验证，确保数据在处理过程中不被泄露。本文根据区块链密码学的隐私保护技术发展，从零知识证明、同态加密、安全多方计算和后量子密码学展开叙述。

2.零知识证明

零知识证明（Zero-Knowledge Proof, ZKP）[4]是一种加密协议，它允许一方（证明者）向另一方（验证者）证明某个陈述为真，而证明过程中无需透露任何关于该陈述的具体信息。其核心目标是在保护隐私的同时实现有效验证。零知识证明具有三种基本属性：完备性，即若陈述为真，证明者能够说服验证者接受证明；可靠性，即若陈述为假，证明者无法欺骗验证者（除非验证者接受极低概率的错误）；零知识性，即验证者除“陈述为真”外，无法获取任何额外信息。

现代零知识证明体系最早来源于 Goldwasser、Micali 和 Rackoff 于 1989 年合作提出并发表了《The Knowledge Complexity of Interactive Proof Systems》[5]，其中阐释了在一个交互系统中为证明某个陈述为真，需要经过多少轮交互，交换多少知识，如果需要交换的知识为零，则称之为零知识证明。

一开始，零知识证明系统在效率以及可用性方面都较为欠缺，仅停留在理论层面。直到近 20 年才得到迅速发展。2010 年，Groth 在《Short Pairing-based Non-interactive Zero-Knowledge Arguments》[6]中提出了目前零知识证明的关键性理论，并实现了基于椭圆曲线密码算法的 ZKP，也是简洁非交互式零知识证明（Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, zk-SNARKs）的理论先驱。

2015 年，Zcash 使用的零知识证明系统，实现了对交易及金额隐私的保护，这是零知识证明在应用上的重要进展。后来发展到 zk-SNARKs 和智能合约相结合，ZKP 技术进入了更为广泛的应用场景。

零知识证明技术中，zk-SNARKs、zk-STARKs（Zero-Knowledge Scalable Transparent Argument of Knowledge）[7] 和 Bulletproofs[8]是三种主流算法，它们在隐私保护、性能和应用场景上各有特点。

2.1 Zk-SNARKs

Zk-SNARKs 由三个算法构成：可信设置、证明生成、验证。通过简洁的非交互式证明，实现交易金额与发送方地址的完全隐藏。其核心优势在于证明长度短，验证时间快，但依赖

可信设置。

2.2 Zk-STARKs

zk-STARKs 是 zk-SNARKs 的技术演变而来，解决了 zk-SNARKs 依赖可信设置的弱点。zk-STARKs 在区块链验证中使用了更加精密的算法，其基于抗碰撞 Hash 函数，而不需要使用椭圆曲线、配对等知识，能够抵抗量子攻击，但相应的代价是 zk-STARK 证明大小达到了 zk-SNARKs 的数千倍，验证成本较高。

2.3 Bulletproofs

Bulletproofs 兼顾了 zk-STARKs 和 zk-SNARKs 的优点，无需可信设置，且证明大小从超过 10kB 缩小到不到 1kB，同时降低 80%的交易费用。但是 Bulletproofs 的证明和验证时间比 zk-STARKs 和 zk-SNARKs 更长。

表 1 为 zk-SNARKs 、 zk-STARKs 、 Bulletproofs 三种算法在算法构成、开销、应用场景等方面的比较。

表 1.三种零知识证明主流算法的比较

类别	zk-SNARKs	zk-STARKs	Bulletproofs
可信设置	需要	不需要	不需要
证明大小	极短	较长	较短
验证时间	极快	对数级增长	较快
抗量子性	不抗量子攻击	抗量子攻击	不抗量子攻击
应用场景	小规模隐私交易	大规模计算、范围证明、链下扩容	隐私交易

近年来，零知识证明技术在区块链领域有重大突破。例如，zk-SNARKs 与智能合约的结合，使得在保护隐私的同时实现复杂的业务逻辑成为可能。同时，针对 zk-STARKs 的优化研究也在不断深入，旨在提高证明效率和降低证明体积。

3.同态加密

同态加密（Homomorphic Encryption, HE）是一种加密技术，它允许在密文上直接进行计算，且计算结果在解密后与明文的计算结果一致。这一特性使数据在加密状态下仍可被处理，无需暴露原始信息，且计算结果以加密的形式输出，仅在需要时由授权方解密。同态加密中有三种同态运算：加法同态、乘法同态、全同态。其中，支持加密数据间进行加法运算为加法同态，支持加密数据间进行乘法运算为乘法同态，同时支持加法和乘法或任意复杂运算为全同态。同态加密由于其特性，成为了区块链隐私保护的核心技术。

1978 年，Rivest、Adleman 和 Dertouzos 在《On Data Banks and Privacy Homomorphisms》[9]中首次提出“隐私同态”概念，设想对加密数据进行直接操作以保护隐私，虽然仅停留在理论层面，但为后续研究奠定了理论基础。随后的近三十年内，同态加密技术得到一定的发展。其中，1999 年提出的 Paillier 加密方案[10]基于合数剩余类问题，实现加法同态，支持无限次加法及有限次明文-密文乘法，是最常用的加法同态方案之一。

2009 年，全同态加密理论得到突破。Gentry 在《Fully Homomorphic Encryption Using Ideal Lattices》[11]中提出首个全同态加密（FHE）方案，基于理想格理论实现任意函数的密文计算，通过“自举技术”（Bootstrapping）实现无限次加法与乘法运算。这一突破性成果标志着同态加密从理论走向实践，但因密文膨胀、计算开销巨大等问题，仍难以直接应用于区块链等实际场景。2011-2013 年，Brakerski 、Gentry 和 Vaikuntanathan（BGV）提出了基于 LWE（Learning With Errors）的层次化同态加密（Leveled FHE）[12]，Brakerski 提出 BFV 方案[13]，并在此基础上发展出了更实用的 RLWE 形式，成为后续方案的基础。2017 年，Cheon 等人提出 CKKS 方案[14]，适用于机器学习等场景，为区块链隐私计算提供了新工具。

应用于区块链的同态加密算法主要为半同态加密的 Paillier、ElGamal[15]以及全同态加密（FHE）的 BGV、BFV、CKKS 方案。

3.1 Paillier

Paillier 由三个算法构成：密钥生成、加密、解密，其安全性基于复合剩余类问题，参数选择合理时，算法是安全的。Paillier 的优势在于其加密和解密操作仅涉及模幂运算，计算复杂度较低；但由于其无法直接支持乘法同态，限制了其在复杂计算中的应用，且密文大小由 $n = pq$ 决定（p, q 为密钥生成算法中选取的大素数），随着 n 增大，开销也会增大。

3.2 ElGamal

ElGamal 是一种基于离散对数问题的公钥加密算法，和 Paillier 类似，由三个算法构成：密钥生成、加密、解密。ElGamal 安全性基于离散对数问题：给定大素数 p，生成元 G，仅由 $G^x \bmod p$ 难以算出 x。在加密过程中，由

于私钥 x 的选择是随机的，可使得每次加密结果不同，模幂运算的计算复杂度较高，可以增加密码的安全性。ElGamal 因其安全性高、灵活性强等优势，在密码学领域得到广泛应用。

3.3 BGV、BFV、CKKS 方案

BGV、BFV、CKKS 方案是三种全同态加密（FHE）方案，允许在密文上直接进行加法、乘法运算，它们基于不同的数学问题和优化策略。

BGV 是第二代 FHE 的代表性方案之一，基于带误差学习（LWE）或环带误差学习（RLWE）问题，通过模数切换技术实现密文同态运算中的噪声管理，无需自举操作即可支持有限深度的电路评估。BGV 通过模数切换技术控制噪声增长，运算效率高，但计算开销较大。主要应用于整数运算的场景，具有一定的局限性。

表 2.五种同态加密算法的比较

类别	Paillier	ElGamal	BGV	BFV	CKKS
算法类型	半同态加密	半同态加密	全同态加密	全同态加密	全同态加密
同态特性	加法同态	乘法同态	加法、乘法同态	加法、乘法同态	加法、乘法同态
计算效率	高效	中等	较低	中等	较低
安全性	合数剩余类问题	离散对数问题	RLWE 问题	RLWE 问题	RLWE 问题
应用场景	隐私保护数据聚合、安全电子投票	数字签名、密钥交换	安全外包计算、隐私保护机器学习、整数运算	安全数据库查询、隐私保护机器学习、整数运算	隐私保护机器学习、金融风险评估

BFV 是第二代 FHE 的另一重要方案，基于 RLWE 问题，通过重线性化技术管理噪声，结合“自举技术”可以实现无限次加法与乘法运算，支持任意深度的同态运算。但自举操作复杂且计算代价高，且需进行谨慎的参数选择。

CKKS 是第三代 FHE 方案，专注于浮点数同态加密，通过近似计算和噪声管理技术，实现对实数域的高效处理。其采用近似计算和优化技术，计算较为高效，且具备广泛兼容性。但近似计算使得精度存在误差，且同样依赖参数的选择。目前常用于机器学习、数据分析等场景。

表 2 为 Paillier、ElGamal 以及 BGV、BFV、CKKS 在算法类型、同态特性、计算效率等方面的比较。

近年来，同态加密技术在性能优化和标准化方面取得了显著进展。例如，针对 CKKS 方案的优化研究，旨在提高计算效率和降低通信开销。同时，同态加密的标准化工作也在不断推进。

4.安全多方计算

安全多方计算（Secure Multi-Party Computation, SMPC）[16]是一种密码学技术，允许多个参与方在不泄露各自原始数据的情况下，共同完成计算任务。其核心目标是“数据可用不可见”[17]，即数据在计算过程中保持隐私性，仅输出最终结果。

SMPC 的核心技术为秘密共享、混淆电路、同态加密结合。秘密共享指在多方协作交易过程中，将数据拆分为多个份额（Shares），分给不同的参与方，在计算时通过份额重组恢复结果。如果仅是部分参与方，则无法恢复数据，需全部参与方共同计算，这就保证了多方协作过程中的数据安全性。混淆电路指不同参与方通过加密电路完成交互，交互过程需参与方通过安全协议完成计算，以保证计算过程中数据不被泄露。同态加密结合指在 SMPC 中引入同态加密，以进一步增强交易的安全性和隐私性。SMPC 因需进行多次交互，存在计算复杂度高、开销大的问题，可通过分层架构等减少通信开销。由于参与方较多，可能存在恶意操作，可结合零知识证明验证参与方行为。

多方安全计算在区块链领域具有广泛应用，如隐私保护的数据分析、安全多方计算协议等。例如，多个医疗机构可以利用多方安全计算技术，在不泄露患者隐私的情况下，共同完成疾病研究和分析。

5.基于后量子密码学的隐私保护技术

随着大数据时代下技术的不断更迭，量子计算机飞速发展，现代密码学体系很有可能在未来被快速攻破。基于后量子密码学（Post-Quantum Cryptography, PQC）的隐私保护技术是应对量子计算对现有密码体系威胁的关键解决方案，其核心在于开发能够抵御量子计算机攻击的加密算法和协议，以保障数据在量子时代的隐私性和安全性。

PQC 主要包括格密码、多变量多项式密码、同源加密等。其中，格密码是基于格问题的加密算法，常见的格问题有最短向量问题（SVP, Shortest Vector Problem）、最近向量问题（CVP, Closest Vector Problem）、带误差学习问题（LWE, Learning With Errors）。多变量多项式密码基于多变量多项式方程组求解难题，多变量多项式常定义在有限域上，进一步增加了问题的复杂性。同源加密基于椭圆曲线上的同源映射问题，椭圆曲线是定义在有限域上的曲线，同源映射是两个椭圆曲线间的特殊映射，需保持曲线上的加法，找到这样的映射在计算上是困难的。PQC 的三种密码学算法均基于计算上困难的数学问题，以抵抗量子攻击，保障数据安全。

PQC 中一些算法的密钥和签名庞大，且并未能高效地在硬件上实现，还需待算法实现进一步优化，以投入到实际应用中。PQC 在量子通信、量子网络安全等领域的研究也在不断深入，展现出广阔的应用前景。

6.总结

尽管区块链密码学的隐私保护技术取得了显著进展，但仍面临一些技术挑战。例如，零知识证明和同态加密的计算效率仍需提高，多方安全计算的通信开销仍需降低，后量子密码学的安全性和实用性仍需进一步验证。

随着量子计算技术的快速发展和区块链技术的广泛应用，区块链密码学的隐私保护技术将面临更多的机遇和挑战。一方面，需要不断优化现有技术，提高计算效率、降低通信开销、增强安全性和实用性；另一方面，需要探索新的技术方向，如结合人工智能、大数据等技术，开发更加高效、安全、实用的隐私保护方案。同时，还需要加强标准化工作，推动区块链密码学隐私保护技术的实际应用和产业发展。

参考文献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[M]. 2009.
[2] Fujimura S, Watanabe H, Nakadaira A, et al., 2015. Bright: A concept for a de-centralized rights management system based on blockchain[C]//2015 IEEE 5th International Conference on Consumer Electronics - Berlin (ICCE-Berlin). 345–346. DOI: 10.1109/ICCE-Berlin.2015.7391275.
[3] 沈鑫，裴庆祺，刘雪峰.区块链技术综述[J]. 网络与信息安全学报，2016，2（11）：10.
[4] Chor B, Goldwasser S, Micali S, et al. Verifiable secret sharing and achieving simultaneity in the presence of faults[C]//Proceedings of 26th Annual Symposium on Foundations of Computer Science (sfcs 1985). 1985: 383-395.
[5] Goldwasser S, Micali S, Rackoff C. The Knowledge Complexity of Interactive Proof Systems[J]. SIAM Journal on Computing, 1989.DOI:10.1137/0218012.
[6] Groth J. Short Pairing-Based Non-interactive Zero-Knowledge Arguments[J]. Springer, Berlin, Heidelberg, 2010.DOI:10.1007/978-3-642-17373-8_19.
[7] Ben-Sasson E, Bentov I, Horesh Y, et al. Scalable, transparent, and post-quantum secure computational integrity[J]. IACR Cryptol ePrint Arch. 2018, 2018: 46-129.
[8] Bünz B, Bootle J, Boneh D, et al. Bulletproofs: short proofs for confidential transactions and more[C]//2018 IEEE Symposium on Security and Privacy (SP). 2018: 315-334.
[9] Rivest R L, Adleman L M, Dertouzos M L. On Data Banks and Privacy Homomorphisms[J]. Foundations of Secure Compuation, 1978.
[10]Paillier P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes[J]. Springer, Berlin, Heidelberg, 1999.DOI:10.1007/3-540-48910-X_16.
[11]Gentry,Craig.Fully homomorphic encryption using ideal lattices[J]. Stoc, 2009: 169-178. DOI:10.1145/1536414.1536440.
[12]Zvika, Brakerski, Craig, et al. (Leveled) Fully Homomorphic Encryption without Bootstrapping[J]. ACM Transactions on Computation Theory (TOCT) - Special issue on innovations in theoretical computer science 2012 - Part II, 2014, 6(3): 1-36. DOI:10.1145/2633600.
[13]Brakerski Z. Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP[J]. Springer Berlin Heidelberg, 2012.DOI:10.1007/978-3-642-32009-5_50.
[14]Cheon J H, Kim A, Kim M, et al. Homomorphic Encryption for Arithmetic of Approximate Numbers[J]. Springer, Cham, 2017. DOI:10.1007/978-3-319-70694-8_15.

[15]Gamal T E. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31: 469-472.
[16]Goldreich O. Secure multi-party computation[J]. Manuscript. Preliminary version, 1998, 78(110): 1-108.
[17]张舒黎，邓春华，胡松等.安全多方计算体系架构及应用思考[J].通信技术，2021，54（09）：2182-2189.