ASIA CCS '25

Zero-Knowledge & Blockchain & Post-Quantum

Kurt Pan @ ZKPunk

September 17, 2025

Contents

1 Zero-Knowledge

1.1 [TNLN25] LogaLookup: Efficient Multivariate Lookup Argument for Accelerated Proof Generation

Zero-Knowledge proof is a cryptographic protocol between two parties called the prover $\mathcal{P}$ and the verifier $\mathcal{V}$, in which $\mathcal{P}$ convinces $\mathcal{V}$ that it knows certain secret information that satisfies a program without revealing the secret. Intended for practicality, a key characteristic of ZK proof is succinctness, allowing the verifier to quickly validate the proof. However, this succinctness usually leads to the trade-off in proof generation time and has constituted the bottleneck in adopting ZK proof into real-world applications.Among the efforts to reduce the prover's time, HyperPlonk - a novel SNARK - suggests migrating from univariate to multivariate polynomials, hence removing the expensive cost in interpolating the polynomials. In addition, a subroutine called lookup argument can be embedded inside a SNARK to speed up the proving process while also supporting circuit gates for complex functions.In this paper, we present LogaLookup, a novel multivariate lookup argument designed for accelerated proof generation using logarithmic derivative. Our scheme is able to support high-degree lookup achieves a faster proving time than Plookup - the multivariate lookup argument scheme proposed alongside HyperPlonk - by eliminating the need for higher-degree intermediate polynomials. Consequently, benchmarking results demonstrate that our scheme achieves proof generation times that are 2.5x faster than those of Plookup, while maintaining minimal impact on verifier performance. We also propose the integration of our lookup argument scheme into HyperPlonk+ to construct a complete lookup-embedded SNARK system.

1.2 [HYOK25] DUPLEX: Scalable Zero-Knowledge Lookup Arguments over RSA Group

Lookup arguments enable a prover to convince a verifier that a committed vector of lookup elements $\vec{f} \in \mathbb{F}^m$ is contained within a predefined table $T \in \mathbb{F}^N$. These arguments are particularly beneficial for enhancing the performance of SNARKs in handling non-arithmetic operations, such as batched range checks or bitwise operations. While existing works have achieved efficient and succinct lookup arguments, challenges remain, particularly when dealing with large vectors of lookup elements in privacy-sensitive applications. In this paper, we introduce DUPLEX , a scalable zero-knowledge lookup argument scheme that offers significant improvements over previous approaches. Notably, we present the first lookup argument designed to operate over the RSA group. Our core technique allows for the transformation of elements into prime numbers to ensure compatibility with the RSA group, all without imposing substantial computational costs on the prover. Given m lookup elements, DUPLEX achieves an asymptotic proving time of $O(m \log m)$, with constant-sized proofs, and constant-time verification. Additionally, DUPLEX ensures the privacy of lookup elements and is robust against dynamic table updates, making it highly suitable for scalable verifiable computation in real world applications. We implemented and empirically evaluated DUPLEX, comparing it with the state-of-the-art zero-knowledge lookup argument Caulk [CCS'22] [ZBKM+22]. Our experimental results demonstrate that DUPLEX significantly outperforms Caulk in proving time for both single and batched lookup arguments, while maintaining practical proof size and verification time.

1.3 [LM25] Fast SNARK-based Non-Interactive Distributed Verifiable Random Function with Ethereum Compatibility

Distributed randomness beacons (DRBs) are fundamental for various decentralised applications, such as consensus protocols, decentralised gaming and lotteries, and collective governance protocols. These applications are heavily used on modern blockchain platforms. This paper presents the so far most efficient direct construction and implementation of a non-interactive distributed verifiable random function (NI-DVRF) that is fully compatible with Ethereum. Our NI-DVRF scheme adopts pairings and combines techniques from secret sharing, SNARKs, and BLS signatures. The security properties of the resulting NI-DVRF scheme are formally modelled and

proven in the random oracle model under standard pairing-based assumptions. To justify the efficiency and cost claims and more generally its adoption potential in practice, the proposed NI-DVRF scheme was implemented in Rust and Solidity. Our implementation is highly optimised and is currently being investigated for deployment on the multichain layer-2 scaling solution provided by Boba Network to power its DRB service zkRand. Our experimental analysis, therefore, also evaluates performance and scalability properties of the proposed NI-DVRF and its implementation.

1.4 [ZC25] VeRange: Verification-efficient Zero-knowledge Range Arguments with Transparent Setup for Blockchain Applications and More

Zero-knowledge range arguments are a fundamental cryptographic primitive that allows a prover to convince a verifier of the knowledge of a secret value lying within a predefined range. They have been utilized in diverse applications, such as confidential transactions. Range arguments with a transparent setup dispense with any trusted setup to eliminate security backdoor and enhance transparency. They are increasingly deployed in diverse decentralized applications on blockchains. One of the major concerns of practical deployment of range arguments on blockchains is the incurred gas cost and high computational overhead associated with blockchain miners. Hence, it is crucial to optimize the verification efficiency in range arguments to alleviate the deployment cost on blockchains and other decentralized platforms. In this paper, we present VeRange with several new zero-knowledge range arguments in the discrete logarithm setting, requiring only $c\sqrt{N/logN}$ group exponentiations for verification, where N is the number of bits to represent a range and c is a small constant, making them concretely efficient for blockchain deployment with a very low gas cost. Furthermore, VeRange is aggregable, allowing a prover to simultaneously prove T range arguments in a single argument, requiring only $O(\sqrt{TN/log(TN)} + T$ group exponentiations for verification. We deployed VeRange on Ethereum, achieving the fastest verification runtime and the lowest gas cost among the discrete-logarithm-based range arguments in practice.

1.5 [JSRC+25] Mining Attack with Zero Knowledge in the Blockchain

Mining attacks remain a serious threat to Proof-of-Work (PoW) blockchain systems, as malicious miners can deviate from standard mining rules to gain

extra rewards. While classic selfish mining tactics conceal entire blocks or release them at once to cause forks, we extend the strategy space by introducing partial block sharing and leveraging zero-knowledge proofs. Specifically, we propose a novel Mining Attack with Zero Knowledge, encompassing two main strategies: Partial Selfish Mining (PSM) and its advanced variant Advanced PSM (A-PSM).By selectively releasing only partial block data, an attacker can attract rational miners to join its private branch without fully revealing the mined block. A zero-knowledge-proof-based mechanism ensures that these rational miners can be convinced of the block's validity without learning its complete content, thereby incentivizing them to collude for higher individual gains. Our theoretical and experimental results show that, under certain conditions on mining power distribution and network latency, PSM can yield higher rewards than both honest and selfish mining, and A-PSM attackers can achieve profits that match or exceed selfish mining and even honest mining. This work highlights a novel zero-knowledge-enabled collusion threat in blockchain mining and calls for broader security measures to protect against such sophisticated strategies.

2 Blockchain

2.1 [ARGM25] Scalable Time-Lock Puzzle

Time-Lock Puzzles (TLPs) enable a client to lock a message such that a server can unlock it only after a specified time. They have diverse applications, such as scheduled payments, secret sharing, and zero-knowledge proofs. In this work, we present a scalable TLP designed for real-world scenarios involving a large number of puzzles, where clients or servers may lack the computational resources to handle high workloads. Our contributions are both theoretical and practical. From a theoretical standpoint, we formally define the concept of a "Delegated Time-Lock Puzzle (D-TLP)", establish its fundamental properties, and introduce an upper bound for TLPs, addressing a previously overlooked aspect. From a practical standpoint, we introduce the "Efficient Delegated Time-Lock Puzzle" (ED-TLP) protocol, which implements the D-TLP concept. This protocol enables both the client and server to securely outsource their resource-intensive tasks to third-party helpers. It enables real-time verification of solutions and guarantees their delivery within predefined time limits by integrating an upper bound and a fair payment algorithm. ED-TLP allows combining puzzles from different clients, enabling a solver to process them sequentially, significantly reducing computational resources, especially for a large number of puzzles or clients.

ED-TLP is the first protocol of its kind. We have implemented ED-TLP and conducted a comprehensive analysis of its performance for up to 10,000 puzzles. The results highlight its significant efficiency in TLP applications, demonstrating that ED-TLP securely delegates 99% of the client's workload and 100% of the server's workload with minimal overhead.

2.2 [DEFL+25] BIP32-Compatible Threshold Wallets

Cryptographic wallets are an essential tool to securely store and maintain users' secret keys and consequently their funds in Blockchain networks. A compelling approach to construct such wallets is to share the user's secret key among several devices, such that an adversary must corrupt multiple machines to extract the entire secret key. Indeed, many leading cryptocurrency companies such as Coinbase, Binance, or ZenGo have started offering such distributed wallets to their customers. An important feature of a cryptographic wallet is its compatibility with the so-called BIP32 specification, the most widely adopted standard for cryptographic wallets. Essentially, BIP32 specifies the notion of a hierarchical deterministic wallet, which allows to create a key hierarchy in a deterministic fashion. Unfortunately, despite significant interest, no practically efficiently solution for a fully distributed wallet scheme, that also follows the BIP32 standard, exists. In this work, we show the first concretely efficient construction of a fully distributed wallet that is compliant with the BIP32 standard. To this end, we first provide a game-based notion of threshold signatures with rerandomizable keys and show an instantiation via the Gennaro and Goldfeder threshold ECDSA scheme (CCS'18). We then observe that one of BIP32's key derivation mechanisms, the so-called hardened derivation, cannot efficiently be translated to the threshold setting. Instead, we devise a novel and efficient hardened derivation mechanism for the threshold setting that satisfies the same properties as the original mechanism as specified by BIP32. As a final contribution, we evaluate our solution with respect to its running time and communication cost.

2.3 [SPVM25] FIRST: FrontrunnIng Resistant Smart ConTracts

Owing to the increasing acceptance of cryptocurrencies, there has been widespread adoption of traditional financial applications such as lending, borrowing, margin trading, and more, into the cryptocurrency realm. In some cases, the inherently transparent and unregulated nature of cryptocur-

rencies exposes users of these applications to attacks. One such attack is frontrunning, where a malicious entity leverages the knowledge of currently unprocessed financial transactions and attempts to get its own transaction(s) executed ahead of the unprocessed ones. The consequences of this can be financial loss, inaccurate transactions, and even exposure to more attacks. We propose FIRST, a framework that prevents frontrunning, and as a secondary effect, also backrunning and sandwich attacks. FIRST is built using cryptographic protocols including verifiable delay functions and aggregate signatures. We formally prove the security of FIRST using the universal composability framework, and experimentally demonstrate its effectiveness using Ethereum and Binance Smart Chain blockchain data. We show that with FIRST, the probability of frontrunning is approximately 0.00004 (or 0.004%) on Ethereum and 0% on Binance Smart Chain, making it effectively near zero.

2.4 [CYXN+25] Infiltrated Selfish Mining: Think Win-Win to Escape Dilemmas

Pooled mining in Bitcoin lets participants share costs and combine computational power, so each miner receives steadier payouts proportional to their contributed work.However, several recent attacks, such as Fork After Withholding (FAW), Power Adjusting Withholding (PAW), and Fork Withholding Attack under a Protection Racket (FWAP), have demonstrated that attackers can exploit open pools to deviate from honest mining and gain more rewards.In this paper, we introduce a novel attack called Infiltrated Selfish Mining (ISM) attack, enabling attackers to earn a higher reward than FAW under certain circumstances, while remaining easier to execute than both PAW and FWAP. By infiltrating a pool and withholding found block, an ISM attacker can generate not only an intentional fork but also a rivalless secret block that stays one block ahead of the public chain. To our best knowledge, ISM is the first pooled mining attack that is capable of avoiding the "miner's dilemma" without suffering a loss in a game when two or more pools attack against each other, and providing the corresponding theoretical winning conditions. Our formal analysis proves that ISM can produce a win-win outcome for all attacking pools in ISM games, in contrast to previous attacks, which operate as pool-size games benefitting only larger pools. The win-win thinking of ISM makes it more attractive to attackers, and therefore more harmful. We also propose a reward approach integrated with a new punishment solution as a potential countermeasure against ISM.

2.5 [QWLC+25] BRC20 Snipping Attack

In this paper, we introduce and implement BRC20 snipping attack. Our attack manipulates the BRC20 token transfers in open markets and disrupts the fairness among bidding participants. The long-standing principle of "highest bidder wins" is rendered ineffective.Typically, open BRC20 token markets rely on Partially Signed Bitcoin Transactions (PSBT) to broadcast selling intents and wait for buying auctions. Our attack targets the BRC20 buying process (i.e., transfer) by injecting a front-running transaction to complete the full signature of the PSBT. At its core, the attack exploits the mempool's fee-based transaction selection mechanism to snipe the victim transaction, replicate metadata, and front-run the legesmate transaction. This attack applies to platforms using PSBT for BRC20 token transfers, including popular Bitcoin exchanges and marketplaces (e.g., Magic Eden, Unisat, Gate.io, and OKX).We implemented and tested the attack on a Bitcoin testnet (regtest), validating its effectiveness through multiple experimental rounds. Results show that the attacker consistently replaces legitimate transactions by submitting higher-fee PSBTs. We have also made responsible disclosures to the mentioned exchanges.

3 Post-Quantum

3.1 [KSKK25] poqeth: Efficient, post-quantum signature verification on Ethereum

This work explores the application and efficient deployment of (standardized) post-quantum (PQ) digital signature algorithms in the blockchain environment. Specifically, we implement and evaluate four PQ signatures in the Ethereum Virtual Machine: W-OTS+, XMSS, SPHINCS+, and MAYO. We focus on optimizing the gas costs of the verification algorithms as that is the signature schemes' only algorithm executed on-chain, thus incurring financial costs (transaction fees) for the users. Hence, the verification algorithm is the signature schemes' main bottleneck for decentralized applications. We examine two methods to verify post-quantum digital signatures on-chain. Our practical performance evaluation shows that full on-chain verification is often prohibitively costly. Naysayer proofs (FC'24) [SGB24] allow a novel optimistic verification mode. We observe that the Naysayer verification mode is generally the cheapest, at the cost of additional trust assumptions. We release our implementation called poqeth as an open-source

library. [1]

3.2 [TMM25] Ring-LWR based Commitments and ZK-PoKs with Application to Verifiable Quantum-Safe Searchable Symmetric Encryption

Prior research on ensuring trust in delegated computation through lattice-based zero-knowledge proofs mostly rely on Learning-With-Errors (LWE) assumption. In this work, we propose a zero-knowledge proof of knowledge using the Ring Learning with Rounding (RLWR) assumption for an interesting and useful class of statements: linear relations on polynomials. We begin by proposing, to the best of our knowledge, the first efficient commitment scheme in literature based on the hardness of RLWR assumption. We establish two properties on RLWR; that aid in the construction of our commitments: 1. closure under addition with double rounding, and 2. closure under multiplication with a short polynomial. Building upon our RLWR ;commitment scheme, we consequently design a RLWR ;based Σ_2 protocol for proving knowledge of a single committed message under linear relations with public polynomials.As an use-case of our proposed Σ_2 protocol, we showcase a construction of a quantum-safe Searchable Symmetric Encryption (SSE) scheme by plugging a prior LWR based SSE scheme from (EuroSP 2023) with our Σ_2 protocol. Concretely, using our Σ_2 protocol for linear relations, we prove the correctness of an encrypted search result in a zero-knowledge manner. We implement our verifiable SSE framework and show that the overhead of an extra verification round is negligible (0.0023 seconds) and retains the asymptotic query execution time complexity of the original SSE scheme.Our work establishes results on zero-knowledge proof systems that can be of independent interest. By shifting the setting from RLWE to RLWR, we gain significant 1. efficiency improvements in terms of communication complexity by O(M) (since some prior works on RLWE require rejection sampling by a factor of M), as well as 2. very short proof size (8.4 KB) and tighter parameters (since RLWR does not explicitly manipulate error polynomials like RLWE).

3.3 [KS25] An Optimized Instantiation of Post-Quantum MQTT protocol on 8-bit AVR Sensor Nodes

Since the selection of the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) standardization algorithms, re-

[1] https://github.com/ruslan-ilesik/poqeth

search on integrating PQC into security protocols such as TLS/SSL, IPSec, and DNSSEC has been actively pursued. However, PQC migration for Internet of Things (IoT) communication protocols remains largely unexplored. Embedded devices in IoT environments have limited computational power and memory, making it crucial to optimize PQC algorithms for efficient computation and minimal memory usage when deploying them on low-spec IoT devices. In this paper, we introduce KEM-MQTT, a lightweight and efficient Key Encapsulation Mechanism (KEM) for the Message Queuing Telemetry Transport (MQTT) protocol, widely used in IoT environments. Our approach applies the NIST KEM algorithm Crystals-Kyber (Kyber) while leveraging MQTT's characteristics and sensor node constraints. To enhance efficiency, we address certificate verification issues and adopt KEMTLS;[72] to eliminate the need for Post-Quantum Digital Signatures Algorithm (PQC-DSA) in mutual authentication. As a result, KEM-MQTT retains its lightweight properties while maintaining the security guarantees of TLS 1.3. We identify inefficiencies in existing Kyber implementations on 8-bit AVR microcontrollers (MCUs), which are highly resource-constrained. To address this, we propose novel implementation techniques that optimize Kyber for AVR, focusing on high-speed execution, reduced memory consumption, and secure implementation, including Signed LookUp-Table (LUT) Reduction. Our optimized Kyber achieves performance gains of 81%,75%, and 85% in the KeyGen, Encaps, and DeCaps processes, respectively, compared to the reference implementation. With approximately 3 KB of stack usage, our Kyber implementation surpasses all state-of-the-art Elliptic Curve Diffie-Hellman (ECDH) implementations. Finally, in KEM-MQTT using Kyber-512, an 8-bit AVR device completes the handshake preparation process in 4.32 seconds, excluding the physical transmission and reception times.

3.4 [RJ25] Quantum-safe Signatureless DNSSEC

We present SL-DNSSEC: a backward-compatible protocol that leverages a quantum-safe KEM and a MAC to perform signature-less SL-DNSSEC validations in a single UDP query/response style. Our experiments targeting NIST level I security for `QTYPE A` query resolution show that SL-DNSSEC is practically equivalent to the presently deployed RSA-2048 in terms of bandwidth usage and resolution speeds. Compared to post-quantum signatures, SL-DNSSEC reduces bandwidth consumption and resolution times by up to (95%) and (60%), respectively. Moreover, with response size $<$ query size $\leq$ 1232 bytes, SL-DNSSEC obviates the long-standing issues of IP

fragmentation, TCP re-transmits and DDoS amplification attacks.

3.5 [Nio25] Practical Deniable Post-Quantum X3DH: A Lightweight Split-KEM for K-Waay

The Signal Protocol, underpinning secure messaging for billions, faces the challenge of migrating to a post-quantum world while preserving critical properties like asynchrony and deniability. While Signal's PQXDH key exchange protocol addresses post-quantum confidentiality, full migration of the X3DH protocol remains elusive. Relying on a split KEM K-Waay ,USENIX'24 [CHNR+24] offers a promising migration path, but it has so far suffered from size limitations compared to concurrent works leveraging ring signatures. This work introduces Sparrow-KEM and Sym-Sparrow-KEM, novel asymmetric and symmetric split KEMs respectively, i.e. for which keys can be used interchangeably for sending and receiving, or only in one direction. They are designed to optimize the K-Waay protocol for size efficiency. Leveraging the MLWE assumption, these constructions reduce by a factor 5.1 $\times$ the communication of prior post-quantum X3DH based on split KEMs, plus provides a 40 $\times$ speedup. Additionally,Sym-Sparrow-KEM is the first symmetric split-KEM to offer deniability, IND-1KCA, and IND-1BatchCCA security, capturing implicit authentication properties. We provide formal security proofs for both schemes, including deniability. Our results demonstrate the feasibility of a compact and deniable post-quantum X3DH protocol based on split KEMs.

3.6 [SBO25] A Quantum-Secure Framework for IoD: Strengthening Authentication and Key-Establishment

The authentication and key establishment (AKE) mechanism is considered one of the promising solutions for securing communication in Internet of Drones (IoD) applications. Nevertheless, existing AKE mechanisms based on traditional cryptographic techniques rely on integer factorization and discrete logarithms, which are no longer safe with the advent of quantum computers. These shortcomings motivate us to design a cutting-edge Quantum Secure Authentication and Key-Establishment mechanism (QSAKE) for the IoD environment. To the best of our knowledge, QSAKE is the pioneered work that uses advanced quantum-safe cryptography, providing a strong defence beyond traditional methods. To further enhance security, it eliminates storing long-term secrets directly in drone memory, reducing the risk of unauthorized access. A Holybro Pixhawk-based microcontroller is

used with a Raspberry Pi connected to a Xilinx Arty A7-100T FPGA board to develop a realistic testbed. Finally, this work stands out as a groundbreaking application of a complete authentication process within a practical IoD testbed, demonstrating its high efficacy and practicality.

References

[ARGM25] Aydin Abadi, Dan Ristea, Artem Grigor, and Steven Murdoch. "Scalable Time-Lock Puzzle". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 839–855. ISBN: 9798400714108 (cit. on p. 5).

[CHNR+24] Daniel Collins, Lois Huguenin-Dumittan, Ngoc Khanh Nguyen, Nicolas Rolin, and Serge Vaudenay. "K-Waay: Fast and Deniable Post-Quantum X3DH without Ring Signatures". In: *33rd USENIX Security Symposium (USENIX Security 24)*. 2024, pp. 433–450 (cit. on p. 11).

[CYXN+25] Xuelian Cao, Zheng Yang, Tao Xiang, Jianting Ning, Yuhan Liu, Zhiming Liu, and Jianying Zhou. "Infiltrated Selfish Mining: Think Win-Win to Escape Dilemmas". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 906–922. ISBN: 9798400714108 (cit. on p. 7).

[DEFL+25] Poulami Das, Andreas Erwig, Sebastian Faust, Philipp-Florens Lehwalder, Julian Loss, Ziyan Qu, and Siavash Riahi. "BIP32-Compatible Threshold Wallets". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 856–872. ISBN: 9798400714108 (cit. on p. 6).

[HYOK25] Semin Han, Geonho Yoon, Hyunok Oh, and Jihye Kim. "DUPLEX: Scalable Zero-Knowledge Lookup Arguments over RSA Group". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 72–86. ISBN: 9798400714108 (cit. on p. 3).

[JSRC+25] Yu Jiaping, Gao Shang, Song Rui, Zhiping Cai, and Xiao Bin. "Mining Attack with Zero Knowledge in the Blockchain". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 890–905. ISBN: 9798400714108 (cit. on p. 4).

[KS25] YoungBeom Kim and Seog Chung Seo. "An Optimized Instantiation of Post-Quantum MQTT protocol on 8-bit AVR Sensor Nodes". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 248–266. ISBN: 9798400714108 (cit. on p. 9).

[KSKK25] Ruslan Kysil, István András Seres, Péter Kutas, and Nándor Kelecsényi. "poqeth: Efficient, post-quantum signature verification on Ethereum". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 327–343. ISBN: 9798400714108 (cit. on p. 8).

[LM25] Jia Liu and Mark Manulis. "Fast SNARK-based Non-Interactive Distributed Verifiable Random Function with Ethereum Compatibility". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 807–822. ISBN: 9798400714108 (cit. on p. 3).

[Nio25] Guilhem Niot. "Practical Deniable Post-Quantum X3DH: A Lightweight Split-KEM for K-Waay". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 298–312. ISBN: 9798400714108 (cit. on p. 11).

[QWLC+25] Minfeng Qi, Qin Wang, Ningran Li, Shiping Chen, and Tianqing Zhu. "BRC20 Snipping Attack". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 923–938. ISBN: 9798400714108 (cit. on p. 8).

[RJ25] Aditya Singh Rawat and Mahabir Prasad Jhanwar. "Quantum-safe Signatureless DNSSEC". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 267–282. ISBN: 9798400714108 (cit. on p. 10).

[SBO25] Salman Shamshad, Sana Belguith, and Alma Oracevic. "A Quantum-Secure Framework for IoD: Strengthening Authentication and Key-Establishment". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 313–326. ISBN: 9798400714108 (cit. on p. 11).

[SGB24] István András Seres, Noemi Glaeser, and Joseph Bonneau. "Naysayer Proofs". In: *International Conference on Financial Cryptography and Data Security*. Springer. 2024, pp. 22–32 (cit. on p. 8).

[SPVM25] Emrah Sariboz, Gaurav Panwar, Roopa Vishwanathan, and Satyajayant Misra. "FIRST: FrontrunnIng Resistant Smart ConTracts". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 873–889. ISBN: 9798400714108 (cit. on p. 6).

[TMM25] Debadrita Talapatra, Nimish Mishra, and Debdeep Mukhopadhyay. "Ring-LWR based Commitments and ZK-PoKs with Application to Verifiable Quantum-Safe Searchable Symmetric Encryption". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 283–297. ISBN: 9798400714108 (cit. on p. 9).

[TNLN25] Dien H. A. Tran, Tam N. B. Nguyen, Nhien-An Le-Khac, and Thuc D. Nguyen. "LogaLookup: Efficient Multivariate Lookup Argument for Accelerated Proof Generation". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 215–230. ISBN: 9798400714108 (cit. on p. 2).

[ZBKM+22] Arantxa Zapico, Vitalik Buterin, Dmitry Khovratovich, Mary Maller, Anca Nitulescu, and Mark Simkin. "Caulk: Lookup arguments in sublinear time". In: *Proceedings of the 2022*

ACM SIGSAC Conference on Computer and Communications Security. 2022, pp. 3121–3134 (cit. on p. 3).

[ZC25] Yue Zhou and Sid Chi-Kin Chau. "VeRange: Verification-efficient Zero-knowledge Range Arguments with Transparent Setup for Blockchain Applications and More". In: *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '25. Association for Computing Machinery, 2025, pp. 823–838. ISBN: 9798400714108 (cit. on p. 4).