2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) | 979-8-3503-2385-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/TPS-ISA58951.2023.00041

Beyond Basic Trust: Envisioning the Future of NextGen Networked Systems and Digital Signatures

Attila A. Yavuz
Computer Science & Engineering
University of South Florida
Tampa, FL, USA
attilaayavuz@usf.edu

Kiarash Sedghighadikolaei
Computer Science & Engineering
University of South Florida
Tampa, FL, USA
kiarashs@usf.edu

Saleh Darzi
Computer Science & Engineering
University of South Florida
Tampa, FL, USA
salehdarzi@usf.edu

Saif E. Nouma
Computer Science & Engineering
University of South Florida
Tampa, FL, USA
saifeddinenouma@usf.edu

***Abstract*—Authentication and integrity are foundational security services for trustworthy systems and the prerequisite of privacy preservation. At the heart of these services lies digital signatures, widely deployed in real-life applications and supported by various standards. Yet, newly emerging next-generation (NextG) networked systems are vastly distributed, include many resource-limited components, and demand advanced features such as privacy, anonymity, and post-quantum (PQ) security. However, the current signature standards and specialized signatures only meet some of these important requirements in isolation. Hence, there is a significant gap in the state-of-the-art in identifying the needs of emerging networked systems and synergizing them with the features of advanced signatures.**

In this work, we strive to mitigate this gap by uniting burgeoning ubiquitous systems with advancements in digital signatures and then envisioning the trust via signatures with extended feature for NextG networked systems. We investigate the current signature standardizations and advanced constructions for their potentials and drawbacks in three essential aspects of NextG networks - decentralized, privacy-preserving, and resource-constraint settings. We first analyze threshold cryptography efforts proffered by NIST, both from secure multi-party computation and custom design constructions, with applications on distributed systems like blockchains, federated cloud, and NextG Public Key Infrastructures (PKIs) in mind. We then investigate the intersections of distributed signatures and privacy-preservation techniques for privacy-sensitive NextG applications (e.g., medical, cryptocurrency). We also focus on research gaps for resource and time-limited systems and identify suitable signatures to remedy this gap for security-critical applications (e.g., vehicular networks, smart grids). Finally, we discuss potential directions for these ubiquitous NextG systems and advanced signatures in the PQ era. We expect that our vision contributes to the narrowing of the gap in NextG networked applications and emerging digital signatures, thereby aiding practitioners and field experts to lay the foundations of authentication services for NextG systems.

***Index Terms*—Next generation networks; digital signatures; distributed systems; post-quantum cryptography; authentication.**

I. Introduction

Digital signature underpins the foundation of trust in information technologies by permitting data integrity, authentication, and non-repudiation properties. Therefore, they found utility in diverse domains, such as PKIs, communication protocols (e.g., TLS, VPNs), smart contracts and blockchains, supply chain integrity, healthcare, and electronic voting. To set frameworks for general-purpose (GP) digital signatures, the National Institute of Standards and Technology (NIST) offers comprehensive guidance [1] encompassing a range of algorithms and suggested curves [2] to facilitate the development of standardized digital signatures (e.g., ECDSA [3], EdDSA [4], RSA [5]). Despite their merits, these standards cannot meet the requirements of emerging NextG networked systems and applications. Below, we elaborate on some of the most critical challenges of NextG networked systems that need novel digital signatures to mitigate these challenges.

Most existing networked systems and applications rely on centralized approaches, wherein entities centrally manage both the storage and executions of cryptographic schemes. However, this approach is susceptible to single-point of failures (e.g., system compromises) and breaches (e.g., root certificate breaches in PKI). In pursuit of heightened security and resiliency, there is an effort to shift from centralized to distributed architectures such as federated cloud, ubiquitous IoTs, and blockchains. Yet, the standard signatures are not designed for distributed computation, leading to a critical weakness in emerging NextG networked applications. Threshold cryptography permits confidential and distributed execution of cryptographic operations among multiple parties and therefore is an ideal approach to mitigate these weaknesses. A recent attempt at NIST's Multi-Party Threshold Cryptography (MPTC) project [6] underscores the importance of this research direction [6]. Yet, there is a significant gap in the state-of-the-art needs, properties, and integration of threshold digital signatures into emerging NextG systems and applications such as distributed PKIs, vehicular/autonomous networks, and other critical cyber-infrastructures (e.g., federated cloud).

Privacy preservation is necessary for various NextG networked applications (e.g., blockchains, e-voting), but GP signatures are not designed with privacy in mind. Privacy-preserving authentication has been an active research area for decades, yet deployment of privacy-enhanced signatures (e.g., group [7], ring [8], and blind signatures [9]) are lacking at best in current systems. The consideration of privacy and anonymity for digital signatures also has been discussed in NIST's MPTC project [6], and balancing between performance, robustness, and privacy are mentioned as major challenges. Hence, there

979-8-3503-2385-6/23/$31.00 ©2023 IEEE
DOI 10.1109/TPS-ISA58951.2023.00041

is a critical need for identifying the requirements, features, and potential integration means of privacy-preserving signatures into NextG applications.

Another critical challenge of NextG networks from a digital signature perspective is the high-performance demands of low-end and/or mobile components of IoT systems and applications. Given the limited resources (e.g., computation, bandwidth), the principal factors for instilling trust via digital signatures revolve around various cost metrics, implementation efficiency, and execution flexibility. Hence, it is necessary to investigate lightweight and fast solutions that can address the needs of low-end (embedded) IoT devices and delay-aware NextG networked systems (e.g., vehicular, smart-grid).

The expected emergence of quantum computers poses a severe threat to the existing public key cryptography standards that rely on conventional-secure intractability assumptions such as Integer Factorization (IF) and Discrete Logarithm Problem (DLP) [10]. NIST has taken the lead in developing Post-quantum Cryptography (PQC) standards [11] to mitigate such quantum computing threats. However, akin to their conventional-secure counterparts, new PQC standards also do not consider the aforementioned advanced features that are solely needed by NextG networked systems such as distributed security, privacy enhancement, and lightweight/fast performance. Moreover, they are significantly costlier than their classical counterparts, compounding the challenges of designing and integrating them with advanced features into NextG networked applications.

A. Our Contribution

In this work, we systematically investigate current and emerging digital signature standardization efforts along with advanced signature constructions through lenses of distributed authentication, privacy preservation, lightweight performance, and PQ security for NextG networked systems. We identify potential research directions and layout visions toward synergizing suitable digital signature solutions and NextG networked applications to address the aforementioned limitations. We further outline our contributions below.

- *Envisioning the Foundational Trust in Distributed NextG Networks and Applications*: It is of significant importance to identify gaps and potential solutions for integrating distributed signatures with decentralized NextG networked systems. Hence, we first concisely examine the existing threshold signature landscape by capturing both generic (secure Multi-Party Computation (MPC) [12]) and custom threshold signatures. We identify the shortcomings of these approaches for decentralized NextG settings such as their computational/communication complexities versus performance needs of target applications (e.g., PKIs, IoT, and healthcare systems), and threat models of applications versus security features of different threshold signatures. We then map out potential visions and research directions that might remedy some of these gaps. Among important research directions, we emphasize synergizing NIST's MPTC [6] and NIST's PQC [13] projects, efficient transparent thresholding of Elliptic Curve (EC)DLP schemes (e.g., [14]) for standard compliance, and custom thresholding of selected signatures (e.g., Schnorr-based [15], Attribute-based [16]) for high-performance deployments.

- *Towards Privacy and Anonymity Preserving Authentication for NextG Networked Systems*: Considering the essential need to integrate privacy-preserving authentication into NextG networked systems, we first provide a concise analysis of state-of-the-art privacy-enhancing digital signatures [17]. We identify important gaps such as consideration of privacy features in isolation, lack of thorough feasibility for specific applications, and limited employment in privacy-critical domains (e.g., healthcare, federated learning). In light of these insights, we present a forward-looking course outlining the forthcoming signatures suitable for NextG networked systems. This analysis lay out Group [7], Ring [8], and Blind signatures [9] in terms of efficiency and outlines potential synergies among them. Further, it highlights the need for constructing PQ secure privacy-preserving signatures and the need for distributed constructions as recommended by the NIST's MPTC project.

- *Analysis of Lightweight and Delay-aware Signatures for Performance Demanding NextG Networks*: Various NextG networks harbor a vast number of resource-limited IoT devices yet still demand energy-efficiency (e.g., wearables, medical devices) with minimum delay to ensure application safety (e.g., for vehicular networks). We first examine key criteria and approaches to achieve time-critical, computation-aware, and efficient signatures for such applications. We then explore advanced constructions aiming for lighter communication, optimum tag/key sizes, and higher security levels, identifying computational gaps in current signatures. We scrutinize aggregate [18], certificateless [19], and forward-secure signatures [20] in this context, and then present potential future work for lightweight PQ-secure signatures.

- *Envisioning Practical Signatures with Advanced Features in the Post-quantum Era*: We present potential PQ signatures for NextG networks through current and in-progress NIST standardization efforts by assessing their applicability in real-world settings (e.g., pre versus post-quantum performance). Exploring the recent additional PQC signature competition [11], we discuss advanced designs such as MPC-based techniques [21]. These form the foundation for GP signatures using symmetric key-based primitives [22] or combined PQC approaches, as well as thresholding PQ signatures. We delve into advanced signature constructions tailored for distributed systems and privacy-enhancing technologies, highlighting their inherent characteristics. Considering factors like omitted properties, security gaps, and vulnerabilities, we discuss potential combinations of security solutions, along with projections for applications.

- *Taxonomy and Organization*: Fig. 1 illustrates the paper's taxonomy, methodology, and prospective trust framework, including identified gaps, possible trajectories, and potential visions. The paper comprises Section 2 on trust evaluation in distributed systems, Section 3 on signatures with advanced properties in privacy-enhancing technologies, Section 4 on

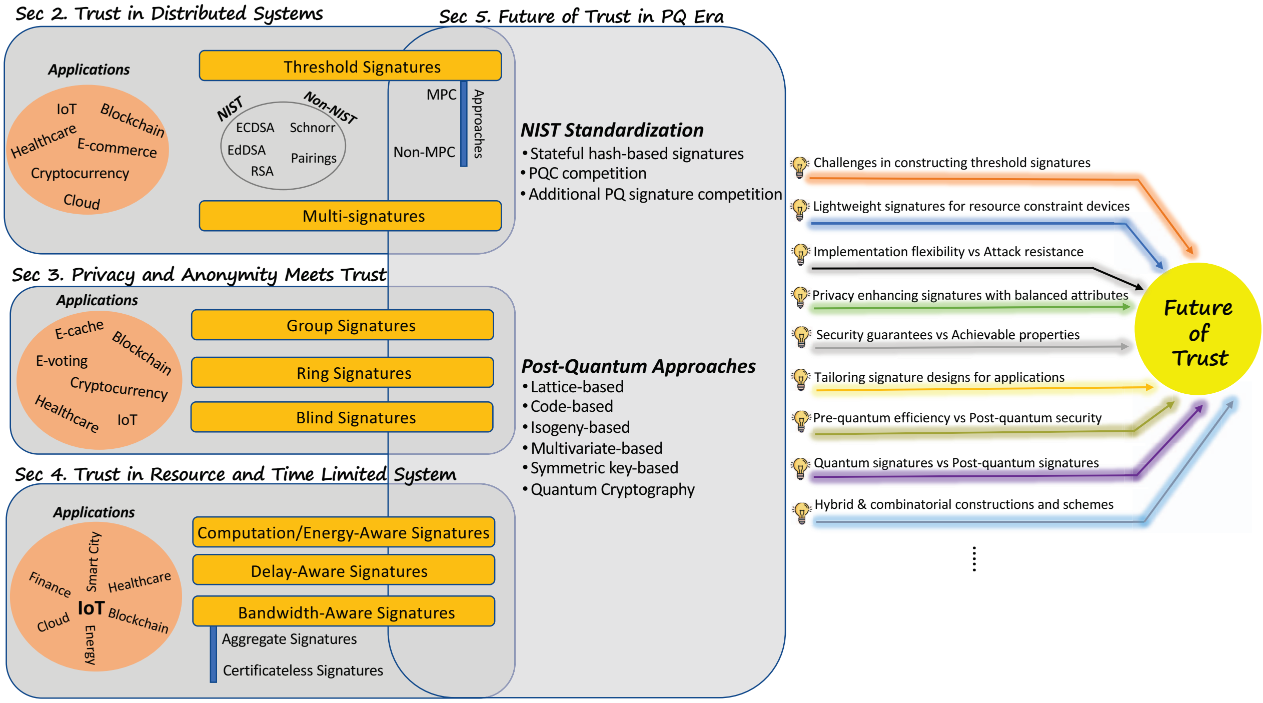
Sec 2. Trust in Distributed Systems
Sec 5. Future of Trust in PQ Era
Applications
IoT
Blockchain
Healthcare
E-commerce
Cryptocurrency
Cloud
Threshold Signatures
NIST
Non-NIST
ECDSA
Schnorr
EdDSA
Pairings
RSA
MPC
Non-MPC
Approaches
Multi-signatures
NIST Standardization
• Stateful hash-based signatures
• PQC competition
• Additional PQ signature competition
Sec 3. Privacy and Anonymity Meets Trust
Applications
E-cache
Blockchain
E-voting
Cryptocurrency
Healthcare
IoT
Group Signatures
Ring Signatures
Blind Signatures
Post-Quantum Approaches
• Lattice-based
• Code-based
• Isogeny-based
• Multivariate-based
• Symmetric key-based
• Quantum Cryptography
Sec 4. Trust in Resource and Time Limited System
Applications
Smart City
Finance
Healthcare
IoT
Cloud
Blockchain
Energy
Computation/Energy-Aware Signatures
Delay-Aware Signatures
Bandwidth-Aware Signatures
Aggregate Signatures
Certificateless Signatures
Challenges in constructing threshold signatures
Lightweight signatures for resource constraint devices
Implementation flexibility vs Attack resistance
Privacy enhancing signatures with balanced attributes
Security guarantees vs Achievable properties
Tailoring signature designs for applications
Pre-quantum efficiency vs Post-quantum security
Quantum signatures vs Post-quantum signatures
Hybrid & combinatorial constructions and schemes
Future of Trust
⋮

Fig. 1: Taxonomy and Relation of Critical NextG Networked Systems and Applications through the Lenses of Emerging Digital Signatures

resource and time-limited systems, and Section 5 on analysis, vision, and projections in the post-quantum era. The paper concludes with Section 6.

II. Future of Trust in Distributed Systems

Most cryptographic schemes rely on a single party to carry out cryptographic operations and store confidential information, making them vulnerable to potential compromises or malicious actions. Threshold cryptography enhances security, resilience, and robustness by distributing secrets and computations among multiple parties, necessitating collaborative efforts from enough of them to conduct cryptographic operations. These advantages have prompted NIST to solicit proposals [6] of multi-party threshold schemes for cryptographic primitives, encompassing both NIST-standardized and non-standardized signature schemes with succinct and verifiably-deterministic signatures. This call aims to identify effective approaches, best practices, and reusable components for future guidelines.

(t, n) threshold digital signature ($\mathcal{TS}$) is a scheme where the confidential values are distributed secretly among n parties such that collaboration of at least t parties is required to generate a signature on a message. A $\mathcal{TS}$ is achievable through two methods: Utilizing secure MPC [12] as the generic approach or adopting custom approaches.

1) Generic approaches: MPC allows a group of mutually distrustful parties to jointly compute a function using their private inputs, guaranteeing that no further information apart from the function's output is disclosed during the computation. Hence, NIST considers MPC [23] as an ideal tool for implementing transparent thresholding in which the properties of the underlying signature remain unchanged, even when parties' inputs are not shares of secrets. This is extremely useful from the standardization point of view since the threshold versions of NIST standards, whether conventional-secure or PQC, will retain their provable security arguments.

This has the capacity to lead to prime adoption of threshold versions in some industrial settings where standard compliance is a critical requirement. In this line, there are various generic thresholding efforts of prominent signature schemes with MPC such as Schnorr [24], ECDSA [25], and EdDSA [14].

2) Custom approaches: Despite its merits, transparent thresholding can be costly for some applications due to MPC's significant communication and computational overhead. While ongoing research like NIST's Circuit Complexity project [26] aims to improve MPC protocols, custom thresholding approaches are essential for constructing efficient schemes for performance-aware NextG networked systems.

The Schnorr signature [27], and its elliptic curve variants, is a seminal construction that not only inspires ECDSA [3] and EdDSA [4], but also amenable to custom thresholding. Starting with the notable work of FROST [15], which introduced a round-optimized Schnorr $\mathcal{TS}$, multiple endeavors have been made to enhance existing schemes. These encompass proposals for concurrent signing sessions, parallel signing, independent signing w.r.t parties, generating stateless signatures, and utilizing an offline party when the signing party is unavailable.

Since the prominent work [28], subsequent research enhanced threshold ECDSA schemes with a focus on bandwidth efficiency via multi-round preprocessing and non-interactive signing techniques. Additionally, there are efforts to enhance resilience by involving an offline party when the signing participant is unavailable. Thresholding EdDSA also received attention by reducing MPC operations during the signing and bolstering resilience by incorporating an offline signing.

There are also threshold signatures that rely on IF and cryptographic pairing [29], [30]. The notable example of pairing-based signatures is BLS [31] with its threshold variants (e.g., [32]). Subsequent work enhanced it by offering features like constant-size signatures, non-interactive signing, and proactive and forward security. Furthermore, there are also RSA-based threshold schemes (e.g., [33]), which are later improved by reducing the required number of participants, eliminating trusted parties, and enabling dynamic groups.

Multi-Signatures: Multi-Signatures (MSs) [34] enable cooperative generation of signatures involving a group of participants. Each member holds a set of private and public keys, and the verifier can verify the participation of all the members. MSs resemble (n, n) TSs, but they differ from the constraint on the participant count n. In the context of MS, they offer the flexibility to form groups, enabling the participation of any number of participants without being restricted by a predetermined setup with a fixed n. Significant enhancements have been made to augment the efficacy of current schemes. These include eliminating the requirement for prior subgroup composition before signature computation, facilitating concurrent signing processes, and introducing order-independent signature aggregation techniques. Additionally, methods have been developed to guarantee constant-time signing and verification operations. Prominent works [35]–[37] have contributed to constructing Schnorr MS with improvements via enabling key aggregation, having a deterministic signing with constant size signature, and providing constant time signing operation.

Vision: Previous TS constructions have pursued either a full private approach to protect signers' identities or an accountable approach to enable signer identification. Achieving a balance between privacy and accountability holds significance across applications such as Blockchain. This pursuit has led to the development of a new signature scheme called Threshold, Accountable, and Private Signatures (TAPS) [38]. The lack of research on TAPS presents a notable opportunity to develop TAPS implementations using standard assumptions. These implementations could offer shorter public keys and signatures, enabling complete tracing and efficient verification procedures.

Standard EC-based signatures are favored over RSA-based ones due to their faster signing and smaller keys. ECDSA is favored for multi-party environments like Blockchain due to lesser use of hash computations, simplifying its threshold implementation in such scenarios. Conversely, multi-party EdDSA requires fewer message exchanges among participants than threshold ECDSA. Hence, constructing and deploying threshold constructions of these signatures is application-dependent. Extensive research on threshold ECDSA highlights various distinctions. These differences include the utilization of the Paillier cryptosystem [39] for securely sharing the private key and facilitating the addition of encrypted shares without requiring prior decryption. Furthermore, the validation of operations through Zero Knowledge Proof (ZKP) and the application of Oblivious Transfer (OT) for generating and distributing random values and exchanging partial signatures are part of the differences. Despite efforts to enhance efficiency like having online-offline signing phases, using ElGamal commitments [40] instead of Paillier, and replacing Paillier with OT, a lasting trade-off exists between performance benchmarks of computation, communication, and storage. The trade-off challenges stem from incorporated techniques like Paillier encryption, ZKP, and OT.

In contrast to standard EC-based signatures, the (EC) Schnorr signature offers several advantages in thresholding, including security, effectiveness, malleability resistance, linearity, batch verification, and multi-signature functionality. These advantages suggest the Schnorr signature's capability to substitute current signatures, as evidenced by the shift from ECDSA to Schnorr by Bitcoin [41] and various other systems. Given this trajectory and prominent works of FROST [15] for Schnorr TSs and Musig2 [36] for Schnorr MSs, it is advisable to improve and create distributed Schnorr signatures for future systems. These constructions should incorporate properties like unlinkability, resilience, adaptive security, and strong unforgeability.

Federated clouds influenced the rise of distributed electronic healthcare systems and the expansion of IoT networks. Some of them use Attribute-Based Signatures (ABSs) with pairings, whose inefficiency impedes the effectiveness of data sharing in such healthcare applications. Constructing ABSs designed for the IoT-Cloud continuum, where the utilization of heterogeneous signatures [42] is feasible, may mitigate the performance challenges in existing applications by offloading resource-intensive computations to capable devices.

NIST's MPTC project offers researchers a plethora of opportunities in developing multi-party threshold constructions, covering both standardized and non-standardized signatures. Moreover, given the NIST's current PQC standards and its recent call for additional PQC signatures, thresholding such constructions holds equal importance to their conventional-secure alternatives. We will discuss threshold PQ-secure schemes in Section V.

III. Privacy and Anonymity Meets Trust

Besides security, resilience, and robustness offered by TS, alternative special-purpose signatures offer distinctive characteristics, primarily focused on enhancing privacy and anonymity via Group, Ring, and Blind Signatures.

Group Signatures: Group signatures (GSs) [7] enable a group of parties, each possessing a private signing key, to individually generate digital signatures on behalf of the group such that it can be further verified by any member using the group's single public key. A trusted party, the group manager, carries out the group administration, empowered to trace the signer's identity during a dispute (*i.e.*, anonymity revocation), consequently facilitating traceability. Numerous endeavors have been undertaken to develop GSs relying on IF or DLP improving previous schemes by allowing for dynamic group formation, multi/verifier-local revocation, concurrent signing, constant sizes (public key and signature), etc. Moreover, additional security notions have been incorporated into GSs, like full anonymity and full traceability, that encompass security notions of unlinkability, exculpability, and non-frameability.

Ring Signatures: Ring signatures (RSs) [8] stand apart from GSs for not requiring setup procedures, group managers, and revocation mechanisms. When signing a message, each participant, possessing a private and public key set, selects a subset of other participants' public keys, including their own, to form an anonymous group known as a ring. Considerable efforts have been made to develop RSs based on IF and (EC)DLP with undeniable and ID-based signatures. Further improvements encompass trustless ad hoc group formation, maintaining constant sizes signatures and keys, and presenting hierarchical security definitions for anonymity and unforgeability.

Blind Signatures: Blind signatures (BSs) [9] allow a user to receive a signature from the signer without revealing information about the signed (blinded) message. There are different BS schemes permitting fairness and removal of anonymity and unlinkability through a trusted entity when a fraud is suspected. Partial BSs enables signers to include agreed-upon common information in the signature. Some BSs allow the recovery of partial or full messages, while others contribute to the realization of stateless signatures with less computation overhead.

Vision: The existing GSs and RSs focus on either anonymity or traceability, but not both with a balanced performance. This gap matters in scenarios where revoking anonymity is necessary such as fraud detection, electronic auctions, and private blockchains. Specifically, the tracing mechanism used in existing methods is centralized and lacks identifying malicious tracers. Moreover, in specific applications like software attestation, solutions like Intel's Enhanced Privacy ID (EPID) use GS but with costly revocation, limiting their scalability. Therefore, a possible avenue of research involves designing signatures that incorporate efficient revocation with integrated anonymity and decentralized traceability, while also detecting malicious tracers.

Linkable ring signatures (LRSs) [43] offer valuable assurance in recognizing signatures from the same signer, particularly used in electronic voting and cryptocurrency applications. Notable research directions are investigating biometric cryptosystems alongside existing methods to establish link tags in LRSs. Other focus areas might be better scalability by reducing signature sizes while improving security against third-party pressure for denying the signatures.

The integration of BSs with pairings to create ID-based and non-interactive BSs has posed challenges to their practicality due to the pairings' heavy computations. Although non-interactive BSs are inefficient without pairings, due to the general-purpose use of proof systems, enhancing existing schemes by either creating pairing-free alternatives or refining the underlying pairings is vital. Moreover, current BSs face challenges in executing effectively in parallel. Additionally, there has been no introduction of a round-optimal ID-based BS with message recovery. Future constructions could address these efficiency gaps in BS schemes.

Another vital aspect of privacy-preserving signatures is their potential integration into NextG networked applications that involve sensitive data to be collected and analyzed such as electronic healthcare and Internet of Medical Things (IoMT) applications [44]. For example, consider data-driven learning in medical contexts like Federated Learning (FL) [45]. The information exchange among participants must be protected with signatures, but this may also make FL applications vulnerable to Source Inference Attacks (SIAs) [46], which can disclose the participants' identities through inferences made between the training dataset and FL nodes. Practical integration of privacy-preserving signatures into such AI tools, especially for medical systems, is expected to be a prominent research direction. The other important application is Tor-like technologies to usher anonymous networks that can aid users in protecting their communication and privacy. However, its focus on anonymity and lack of identity verification pose challenges [47]. Allowing the computing nodes to join and leave voluntarily leads to the presence of unreliable nodes in the network. Additionally, the absence of traceability mechanisms contributes to the vulnerability of nodes to denial-of-service (DoS) attacks. Thus, there is an interest in researching digital signatures to maintain anonymity while introducing traceability in Tor-like networks so that these illegal activities and DoS attacks can be mitigated. Finally, PQ-secure versions of privacy-preserving signatures will be a vital research direction, which will be discussed in more details in Section V.

IV. Trust in Resource and Time Limited Systems

IoT is comprised of an array of low-end devices ranging from medical devices (e.g., implants), personal gadgets (e.g., smart-watch), and military equipment (e.g., aerial drones). Hence, there is a need to develop efficient cryptographic algorithms that can meet the stringent requirements of IoT applications. As a result, the battery life of these IoT devices lasts longer, providing more flexibility to execute their core application-specific operations. Herein, our primary focus centers on lightweight authentication tools, specifically digital signatures.

Computation/Energy-Aware Signatures: Low-end IoT devices require lightweight computations and low bandwidth overhead. There exist numerous digital signatures offering fast signature generation, small signatures, and compact keys. For instance, there are digital signatures that rely on third-parties (e.g., secure hardware-supported server [48], non-colluding distributed servers [49]) in order to remove the burden of public-key supply and their certification from the resource-constrained signers. In a similar line, Certificateless digital signatures (e.g., [19], [50]) remove the certification overhead from the signer side by introducing a public-key generator (PKG) (e.g., cloud server). This latter also enhances the security guarantees at the signer side by computing the private keys on demand with partial private input from PKG.

Delay-Aware Signatures: Delay-aware digital signatures are different from energy-aware variants in the way that they can compromise the signer's energy usage to reduce end-to-end delay. This is of paramount importance for time-critical and real-time applications. There exist digital signatures (e.g., CEDA [51], SCRA [52]) that precompute a table of messages and their corresponding signatures during the key generation to allow an efficient signature generation. There is also other lightweight digital signatures offering aggregation and anonymous signing (e.g., [53]) that are designed for resource-constrained devices. Despite their merits, they are based on seminal signature algorithms (i.e., BLS) which have expensive signing operations [54].

Bandwidth-Aware Signatures: Bandwidth-aware digital signatures are mainly aggregate and certificateless signatures having a compact and small-size signature and public key sizes, respectively. Aggregate signature (AS) schemes attempt to reduce the cryptographic payload by combining multiple and distinct signatures into a constant-size signature. A constant-size signature translates into a significantly lower bandwidth usage. The primary AS schemes can be classified into pairing-based (e.g., BLS [31]) which have the highest compression ratios across multiple signers but with expensive signing operations. Factorization-based: (e.g., C-RSA [55]) have an efficient batch verification but with a costly signature generation and large key sizes. EC-based: (e.g., BAF [20], [42], [56]) has the best balance between signing efficiency and key sizes. It is important to note that such lightweight signatures can also play an important role in projecting cognitive wireless network services and their surrounding data structures (e.g., [57]–[59]).

Vision: Lightweight digital signatures find applications in various real-world scenarios, notably in IoT networks and digital twin frameworks. The digital twins involve replicating physical systems ranging from living (e.g., human) or non-living (e.g., smart city) beings. These systems are empowered by low-end IoT devices that actively monitor and transmit authenticated and/or encrypted data streams to remote cloud servers for long-term storage and analytical purposes. Thus, it is critical to devise cryptographic solutions that are highly efficient, yet still offering long-term security with exotic security features such as signature aggregation.

Delving into long-term security, PQ-secure lightweight signature is still an open issue. For instance, the selected NIST PQC signature standards (*e.g.*, Dilithium [60]) remain impractical for deployment in IoT devices due to the costly computations and large key sizes. Note that PQC standards do not offer essential security features namely aggregation which is suitable in bandwidth- or storage-limited applications, such as wireless sensor networks and medical devices. However, PQ signature schemes that do allow aggregation often suffer from processing slowdown, low compression ratios, and interactive signing. Currently, utilizing lattice-based hard problems, we can attain ASs with provable security in the Quantum Random Oracle Model (QROM), logarithmic growth in signature size, and additional features like identity-based capabilities or sequential aggregation [18]. This sequential aggregation results in reduced data transmission and makes the scheme more practical for applications like routing protocols, certification chains, and blockchains.

The security challenges for low-end IoTs extend beyond quantum attacks, encompassing the vulnerability to physical malware attacks, such as side-channel and timing attacks [61]. To mitigate these risks, forward-security [20] is a feature that periodically evolves the private key, thus preventing the recovery of past key iterations. Although NIST recommends XMSS$^{\text{MT}}$ [62] as a stateful signature scheme, it is more computationally expensive compared to PQC standards with similar large keys and unsuitable for lightweight IoT networks.

There are only a few signature schemes that provide PQ security with the above-listed evaluation metrics. For example, ANT [63] relies on a set of distributed third-party servers to construct one-time keys and commitments. However, it assumes non-colluding distributed servers and is susceptible to network delays. Similarly, HASES [48] exploits the availability of secure enclaves on cloud servers to delegate the construction of one-time keys from low-end IoTs to the resourceful clouds. However, it relies on the central root of trust which is against the future orientation towards distributed systems.

The future direction of the cryptosystems is going towards distributed settings, [64] proposed to harness the quantum networks among distributed cloud servers, alongside hardware acceleration (e.g., GPUs) to reduce computational and communication overhead. Therefore, we anticipate that future lightweight signatures will incorporate these emerging technologies to achieve secure and efficient distributed solutions.

V. Future of Signatures in Post-Quantum Era

Post-quantum security is one of the most crucial factors to ensure long-term security for NextG networked systems. In this section, we will investigate the current and potential future quantum-safe digital signatures through the lenses of such systems.

A. Current NIST-PQC Signature Standardization Efforts

NIST has conducted two competitions concerning post-quantum GP signatures. The first competition focused on stateful hash-based signatures, and it concluded with the IETF publishing RFCs related to the winning signatures. These victorious signatures, known as XMSS$^{\text{MT}}$ [62] and LMS [65], along with their multi-tree variants, provide robust security guarantees while minimizing reliance on strong assumptions. On another front, NIST has also organized a competition for GP Key Encapsulation Mechanisms (KEM) and Digital Signature schemes. This competition has progressed to its final round, with three signature schemes selected: CRYSTALS-Dilithium

[60], FALCON [66], and SPHINCS+ [67], where Dilithium stands out as the primary scheme to be implemented [13].

It is important to highlight that, apart from SPHINCS+, the digital signatures considered as finalists, primarily relied on the hardness of structured lattices. To encourage diversity in the standardization of PQC algorithms, NIST initiated an additional competition specifically focused on GP digital signatures [11]. The call for submissions emphasized the need for non-lattice algorithms suitable for various applications, such as certificate transparency. The primary requirement for submissions was to provide solutions with "quick verification and concise signature" properties. Although accepting signature proposals based on structured lattices, they must ensure security against *EUF-CMA* and demonstrate substantial superiority over Dilithium and FALCON. On the other hand, non-lattice proposals must demonstrate significant performance benefits compared to SPHINCS+. Notably, NIST has recently revealed the initial-round schemes in this competition.

B. Future of NIST-PQC Efforts for Signature Standards

Lattice-based cryptography has been broadly used in signature schemes, boasting the highest number of overall winner candidates in PQC competitions. The lattice-based schemes announced in the additional PQ-secure signature competition are either based on unstructured lattices with improved performance or structured lattices with shorter signatures, faster operations, and side-channel-resistant construction. For instance, HAETAE [68], which was also part of the Korean PQC competition, is chosen for its improved complexity and compact signature, fitting within a single TCP/UDP datagram.

All initial code-based proposals in the PQC competitions have been compromised, leaving the pursuit of a reliable signature scheme based on error-correcting codes challenging. Moreover, a substantial portion of code-based signatures presented in the additional signature competition are established through integration with other PQC techniques (e.g., MPC in the Head paradigm)). Despite their security assurances, the efficiency of code-based signatures still remains a concern.

The Unbalanced Oil and Vinegar signature [69], initially rejected alongside other multivariate-based signatures in the initial PQC competition, has become the foundation for most of the chosen signatures in NIST's additional signature competition. Multivariate schemes can be effectively combined with other PQC approaches, allow various parameter sets, and offer comparable performance, particularly on low-cost devices. The isogeny-based approach inherently lacks support for certain features and cryptographic primitives, such as signature protocols. Despite significant cryptanalysis and the discovery of vulnerabilities in the SIDH (Supersingular Isogeny Diffie-Hellman) problem, which affects a substantial portion of isogeny-based constructions, SQIsign [70] is the only signature scheme that remained unaffected, and was selected in NIST's additional signature competition.

Hash-based signatures provide security without relying on any number-theoretic assumptions. Therefore, in the case of attacks, one can just replace the underlying hash function. Additionally, hash-based signatures can provide forward security, enhancing their resilience against key compromises.

Although the only symmetric-key-based signature constructed on the MPCitH (MPC in the Head) paradigm in the PQC competition was broken, this approach has been widely adopted in NIST's additional signature competition. Many selected schemes are based solely on this method or through a combination with other PQC approaches like multivariate, code, and isogeny. For instance, MIRA [22] is a combination of MPCitH and MinRank coding problem. Primarily, by developing a non-interactive ZKP using MPC techniques in a black-box manner, it becomes possible to transform into a robust symmetric key-based signature scheme. The security of this scheme relies on the challenge of the chosen symmetric primitive for key generation and the selected MPC protocol. The prominent advantage of constructing signatures from symmetric primitives like schemes based on hash functions or MPCitH paradigm lies in the absence of structured assumptions, efficient implementation, and the ability to customize parameter sets to suit various applications.

C. Potential Future of PQC Signatures with Advanced Features

While GP signatures fulfill essential security criteria, they fall short for some use cases, particularly, in the context of emerging distributed and privacy-enhancing technologies. In this section, we consider signatures with advanced properties in the PQ era.

Threshold Signatures: In thresholding NIST's lattice-based schemes, a challenge is with rejection sampling, which necessitates keeping intermediate values undisclosed until the sampling is finished. To address this, a combination of MPC techniques of *Linear Shamir's secret sharing (LSSS)*-based MPC for linear operations and Garbled circuit (GC)-based MPC for non-linear operations. While applying these methods, there could arise a need for transitions between them. This transition is facilitated by the utilization of daBits [71], which are double-shared authenticated bits designed to operate within two distinct secret sharing schemes. Moreover, the secrets are shared linearly among the parties in threshold constructions. Furthermore, heavy reliance on cryptographic hash functions has a detrimental impact on the complexity of thresholding. The analysis by [21] conducted a comprehensive study of signature thresholding in the competition's second round, revealing the computational complexities of applying the MPC techniques. Their findings highlight that with the utilization of optimized garbled circuit implementations, constructing threshold PQ-secure signatures is inefficient regarding signing time for practical use. Despite current inefficient schemes, these ongoing efforts show potential in creating effective approaches and reusable components to facilitate the thresholding of future PQ-secure signatures with comparable structures.

Multi-Signatures: Lattice-based MSs continue to face the open problem of striking a tradeoff between efficiency and security. Constructing efficient schemes based on non-standard lattice problems or achieving provable security assurance with smaller signature sizes and lower costs remains a challenge.

While there is a lattice-based MS based on Dilithium that provides provable security in the QROM, the parameter set for these schemes is still not compact enough, making them impractical for real-world scenarios. MSs based on coding theory are not only formed on top of code-based signatures which have been rendered insecure but also their designs have been subjected to cryptanalysis and have not met the security requirements expected of MS schemes. Besides lattice-based approach, only multivariate cryptography offers robust MS schemes that feature relatively smaller signatures. However, note that multivariate-based schemes are built on Hidden Field Equation, which has been subjected to various cryptanalysis.

Group Signatures: Given that the majority of PQ-secure GSs are constructed using non-interactive ZKPs, a prospective goal, particularly in the context of lattice-based methods, is to develop an efficient GS scheme with provable security in standard or QROM models [72]. Also, when employing the revocation mechanism in a lattice-based approach, complete anonymity is not supported. Recently, independent signatures and key sizes have been achieved with respect to group size. Nevertheless, the ultimate goal of achieving lattice-based GSs with constant sizes while providing full anonymity, traceability, and dynamic features requires further investigation. In contrast to other improved signatures, code-based GSs have achieved full dynamism and logarithmic growth.

On the other hand, isogeny-based methods produce GSs with logarithmic size growth w.r.t the group size. However, these methods rely on lower security assurances and remain impractical for real-world applications. There are a limited number of hash-based GSs that rely on an information-theoretically secure structure. However, these schemes face difficulties in converting a one-time scheme to a multi-time and longer signature generation times, primarily caused by the height of their tree structure. While achieving a fully dynamic GS is possible through various PQC approaches, it often necessitates placing significant trust in different authorities or assuming an honest key generation process. However, this level of trust is not always feasible in some real-world applications.

Ring Signatures: The vast majority of PQ-secure RSs have been constructed using non-interactive ZKPs. Apart from security considerations and the substantial communication and computation requirements, the primary direction is reducing the key and signature size for the number of users in the ring [73].

The lattice-based RS offers computational/unconditional anonymity, linkability, and privacy preservation, making it the most efficient for achieving (poly)logarithmic signature sizes. Moreover, lattice-based methods enable traceable RS schemes with a balance between GSs with traceability and RSs with anonymity. This versatility makes lattice-based methods applicable to e-voting, e-cash, and cryptocurrencies, preventing non-reusability and double-spending attacks.

Isogeny-based and hash-based RSs both achieve a logarithmic signature scale and utilize the Merkle tree for efficient key management. However, isogeny schemes suffer from slow signature generation, while hash-based schemes are faster with a simple design. However, despite offering traceability to control anonymity guarantees and prevent malicious signer abuse, hash-based schemes are limited to one-time use or face key management issues. Despite supporting traceability, code-based methods suffer from a slow signing process, which remain impractical for real-world applications with large rings. In contrast, multivariate RSs stand out by providing smaller signatures while maintaining provable security, a rare achievement within the realm of PQC.

One potential future direction involves combining RSs with ASs, which provides support for integrity, communication efficiency, and anonymity, making it valuable for privacy-preserving applications. Another direction is to blend threshold and RSs, resulting in perfect anonymity that is applicable to decentralized applications. Also, in contrast to RSs, ring signcryption offers unconditional anonymity and privacy without the need for ring administrators, making it applicable to electronic finance and decentralized platforms.

Blind Signatures: In contrast to classical schemes, the state of PQ-secure BS is unsatisfactory. Specifically, lattice-based approach still lacks a practical and secure BS with key and signature sizes applicable to real-world scenarios. Some lattice-based schemes attempt to achieve blindness by utilizing fully homomorphic encryption, which leads to increased complexity. While providing provable security in ROM based on standard lattice problems, these schemes are limited to linear growth in the size of the maximum number of signatures and are only applicable to certain scenarios. On the other hand, code-based approach offers only a limited number of BS schemes and currently impractical for real-world applications. Also note that the signature size of BSs remains a significant issue in the code-based approach. Multivariate BSs are derived from schemes that were unsuccessful in the NIST PQC competition. Isogeny-based BSs encounter security issues in their design and often necessitate large parameter sets. Moreover, in certain cases, the resulting signatures lack transferability, effectively making them designated verifier signatures.

VI. Conclusion

Digital signatures play a crucial role in ensuring trustworthy systems, offering authentication, integrity, and non-repudiation across a wide range of applications. Emerging NextG networked systems are characterized by high distribution, the inclusion of resource-limited components, and the demand for advanced properties such as privacy, anonymity, and post-quantum security. However, the current digital signatures have only partially tackled this array of requirements concurrently, revealing an existing gap in the state-of-the-art. This gap pertains to effectively meeting the requisites of emerging systems and synergizing the features of standard and advanced signatures. This study aims to bridge gaps within NextG networked applications by integrating them with emerging digital signatures, thereby envisioning trust enhancement through signatures with extended functionalities tailored for NextG systems. This effort is underpinned by assessing potentials and limitations across three essential aspects:

distribution, privacy preservation, and resource limitation. Therefore, this research starts by first examining NIST's threshold cryptography endeavors, spanning secure MPC and custom design constructions, and considering their emerging applications. Next, we explore the significance of privacy-preserving authentication systems within privacy-sensitive and distributed NextG applications such as medical and cryptocurrency contexts. We then identify the gap in resource and time-limited systems and explore suitable signature solutions to fill these gaps. Finally, the study provides a forward-looking perspective that envisions integrating ubiquitous NextG systems and advanced signatures within the framework of the post-quantum era.

ACKNOWLEDGMENT

This research is supported by the unrestricted gift from the Cisco Research Award (220159), and the NSF CAREER Award CNS-1917627.

REFERENCES

[1] L. Chen, D. Moody, A. Regenscheid, and A. Robinson, "Digital signature standard (dss)," 2023.

[2] L. Chen, D. Moody, A. Regenscheid *et al.*, "Recommendations for discrete logarithm-based cryptography: Elliptic curve domain parameters," 2019.

[3] ANSI, "Accredited standards committee x9 (2005) public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ecdsa). american national standard for financial services (ans) x9.62-2005," Tech. Rep., 2005.

[4] D. J. Bernstein, N. Duif, T. Lange *et al.*, "High-speed high-security signatures," *Journal of cryptographic engineering*, vol. 2, no. 2, 2012.

[5] K. Moriarty, B. Kaliski, J. Jonsson, and A. Rusch, "Pkcs# 1: Rsa cryptography specifications version 2.2," Tech. Rep., 2016.

[6] L. Brandao and R. Peralta, "Nist first call for multi-party threshold schemes," 2023.

[7] D. Chaum and E. Van Heyst, "Group signatures," in *Advances in Cryptology—EUROCRYPT'91: Workshop on the Theory and Application of Cryptographic Techniques, Proceedings 10*. Springer, 1991.

[8] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology—ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, Proceedings 7*. Springer, 2001.

[9] J. Vora, P. DevMurari, S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, "Blind signatures based secured e-healthcare system," in *2018 International conference on computer, information and telecommunication systems (CITS)*. IEEE, 2018.

[10] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 1994, pp. 124–134.

[11] "Round 1 additional signatures," https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures, accessed: Aug, 2023.

[12] A. C. Yao, "Protocols for secure computations," in *23rd annual symposium on foundations of computer science (sfcs 1982)*. IEEE, 1982.

[13] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang *et al.*, "Status report on the third round of the nist post-quantum cryptography standardization process," *US Department of Commerce, NIST*, 2022.

[14] C. Bonte, N. P. Smart, and T. Tanguy, "Thresholdizing hasheddsa: Mpc to the rescue," *International Journal of Info. Security*, vol. 20, no. 6, 2021.

[15] C. Komlo and I. Goldberg, "Frost: flexible round-optimized schnorr threshold signatures," in *Selected Areas in Cryptography: 27th International Conference, Halifax, NS, Canada (Virtual Event), October 21-23, 2020, Revised Selected Papers 27*. Springer, 2021.

[16] W. Susilo, G. Yang, F. Guo, and Q. Huang, "Constant-size ciphertexts in threshold attribute-based encryption without dummy attributes," *Information Sciences*, vol. 429, pp. 349–360, 2018.

[17] A. Chator, M. Green, and P. R. Tiwari, "Sok: Privacy-preserving signatures," *Cryptology ePrint Archive*, 2023.

[18] D. Boneh and S. Kim, "One-time and interactive aggregate signatures from lattices," *preprint*, 2020.

[19] R. Behnia, A. A. Yavuz, M. O. Ozmen, and T. H. Yuen, "Compatible certificateless and identity-based cryptosystems for heterogeneous iot," in *Information Security Conference (ISC)*. Springer, 2020.

[20] A. A. Yavuz, P. Ning, and M. K. Reiter, "BAF and FI-BAF: Efficient and publicly verifiable cryptographic schemes for secure logging in resource-constrained systems," *ACM Trans on Info. Sys. Sec.*, vol. 15, no. 2, 2012.

[21] D. Cozzo and N. P. Smart, "Sharing the luov: threshold post-quantum signatures," in *IMA International Conference on Cryptography and Coding*. Springer, 2019.

[22] N. Aragon, L. Bidoux, J.-J. Chi-Domínguez, T. Feneuil, P. Gaborit, R. Neveu, and M. Rivain, "Mira: a digital signature scheme based on the minrank problem and the mpc-in-the-head paradigm," *arXiv preprint arXiv:2307.08575*, 2023.

[23] L. T. Brandão, N. Mouha, and A. Vassilev, "Threshold schemes for cryptographic primitives: challenges and opportunities in standardization and validation of threshold cryptography," 2018.

[24] Y. Lindell, "Simple three-round multiparty schnorr signing with full simulatability," *Cryptology ePrint Archive*, 2022.

[25] A. Dalskov, C. Orlandi, M. Keller, K. Shrishak, and H. Shulman, "Securing dnssec keys via threshold ecdsa from generic mpc," in *Computer Security–ESORICS 2020: 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14–18, 2020, Proceedings, Part II 25*. Springer, 2020.

[26] NIST, "Circuit Complexity, csrc.nist.gov," https://csrc.nist.gov/Projects/circuit-complexity, 2023, [Accessed 17-08-2023].

[27] C.-P. Schnorr, "Efficient identification and signatures for smart cards," in *Advances in Cryptology—CRYPTO'89 Proceedings 9*. Springer, 1990.

[28] R. Gennaro, S. Goldfeder, and A. Narayanan, "Threshold-optimal dsa/ecdsa signatures and an application to bitcoin wallet security," in *Applied Cryptography and Network Security: 14th International Conference, ACNS, Guildford, UK, Proceedings 14*. Springer, 2016.

[29] V. S. Miller, "The weil pairing, and its efficient calculation," *Journal of cryptology*, vol. 17, no. 4, pp. 235–261, 2004.

[30] G. Frey, M. Muller, and H.-G. Ruck, "The tate pairing and the discrete logarithm applied to elliptic curve cryptosystems," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1717–1719, 1999.

[31] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *Journal of cryptology*, vol. 17, 2004.

[32] A. Boldyreva, "Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme," in *International Workshop on Public Key Cryptography*. Springer, 2002.

[33] V. Shoup, "Practical threshold signatures," in *Advances in Cryptology—EUROCRYPT: International Conference on the Theory and Application of Cryptographic Techniques*. Springer, 2000.

[34] K. Itakura, "A public-key cryptosystem suitable for digital multisignature," *NEC research and development*, vol. 71, 1983.

[35] J. Nick, T. Ruffing, Y. Seurin, and P. Wuille, "Musig-dn: Schnorr multi-signatures with verifiably deterministic nonces," in *Proceedings of the ACM SIGSAC Conf. on Computer and Communications Security*, 2020.

[36] J. Nick, T. Ruffing, and Y. Seurin, "Musig2: simple two-round schnorr multi-signatures," in *Annual International Crypto. Conf.* Springer, 2021.

[37] G. Maxwell, A. Poelstra, Y. Seurin, and P. Wuille, "Simple schnorr multi-signatures with applications to bitcoin," *Designs, Codes and Cryptography*, vol. 87, no. 9, 2019.

[38] D. Boneh and C. Komlo, "Threshold signatures with private accountability," in *Annual International Cryptology Conference*. Springer, 2022, pp. 551–581.

[39] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International conference on the theory and applications of cryptographic techniques*. Springer, 1999, pp. 223–238.

[40] Y. Lindell and A. Nof, "Fast secure multiparty ecdsa with practical distributed key generation and applications to cryptocurrency custody," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018.

[41] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, vol. 4, no. 2, p. 15, 2008.

[42] A. A. Yavuz, "ETA: Efficient and tiny and authentication for heterogeneous wireless systems," in *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, ser. WiSec '13, April 2013, pp. 67–72.

[43] W. Li, Z. Lin, Q. Chen *et al.*, "A hybrid design of linkable ring signature scheme with stealth addresses," *Security and Communication Networks*, vol. 2022, 2022.

[44] K. Chatterjee, A. Singh, Neha, and K. Yu, "A multifactor ring signature based authentication scheme for quality assessment of iomt environment in covid-19 scenario," *ACM Journal of Data and Information Quality*, vol. 15, no. 2, pp. 1–24, 2023.

[45] G. A. Kaissis, M. R. Makowski, D. Rückert, and R. F. Braren, "Secure, privacy-preserving and federated machine learning in medical imaging," *Nature Machine Intelligence*, vol. 2, no. 6, pp. 305–311, 2020.

[46] H. Hu, Z. Salcic, L. Sun, G. Dobbie, and X. Zhang, "Source inference attacks in federated learning," in *2021 IEEE International Conference on Data Mining (ICDM)*. IEEE, 2021, pp. 1102–1107.

[47] Q. Tan, X. Wang, W. Shi, J. Tang, and Z. Tian, "An anonymity vulnerability in tor," *IEEE/ACM Transactions on Networking*, vol. 30, no. 6, pp. 2574–2587, 2022.

[48] S. E. Nouma, , and A. A. Yavuz, "Post-quantum forward-secure signatures with hardware-support for internet of things," ser. IEEE International Conference on Communications (ICC). IEEE, 2023, p. 1–6.

[49] M. O. Ozmen, R. Behnia, and A. A. Yavuz, "Energy-aware digital signatures for embedded medical devices," in *7th IEEE Conference on Communications and Network Security (CNS)*, 2019.

[50] S.-H. Seo, J. Won, and E. Bertino, "Pclsc-tkem: a pairing-free certificateless signcryption-tag key encapsulation mechanism for a privacy-preserving iot." *Trans. Data Priv.*, vol. 9, no. 2, 2016.

[51] M. O. Ozmen, R. Behnia, and A. A. Yavuz, "Compact energy and delay-aware authentication," in *2018 IEEE Conference on Communications and Network Security (CNS)*, 2018, pp. 1–9.

[52] A. A. Yavuz, A. Mudgerikar, A. Singla, I. Papapanagiotou, and E. Bertino, "Real-time digital signatures for time-critical networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, 2017.

[53] T. Li, H. Wang, D. He, and J. Yu, "Permissioned blockchain-based anonymous and traceable aggregate signature scheme for industrial internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 10, 2020.

[54] S. E. Nouma and A. A. Yavuz, "Practical cryptographic forensic tools for lightweight internet of things and cold storage systems," in *Proceedings of the 8th ACM/IEEE Conf. on IoT Design and Implementation*, 2023.

[55] A. A. Yavuz, "Immutable authentication and integrity schemes for outsourced databases," *IEEE Trans. Dependable Sec. Comput.*, vol. 15, no. 1, pp. 69–82, 2018.

[56] R. Behnia, M. O. Ozmen, and A. A. Yavuz, "ARIS: Authentication for real-time IoT systems," in *53rd IEEE International Conference on Communications (ICC), Shanghai, China*, May 2019.

[57] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "Cuckoo filter-based location-privacy preservation in database-driven cognitive radio networks," in *Computer Networks and Information Security (WSCNIS), 2015 World Symposium on*, Sept 2015, pp. 1–7.

[58] M. Grissa, A. Yavuz, and B. Hamdaoui, "An efficient technique for protecting location privacy of cooperative spectrum sensing users," in *IEEE Infocom Green and Sustainable Networking and Computing Workshop, 2016 (GSNC '16).*, April 2016.

[59] N. Adem, B. Hamdaoui, and A. Yavuz, "Pseudorandom time-hopping anti-jamming technique for mobile cognitive users," in *2015 IEEE Globecom Workshops (GC Wkshps)*, Dec 2015, pp. 1–6.

[60] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, and P. Schwabe, "Crystals-dilithium: A lattice-based digital signature scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018.

[61] E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, "Recent advances in post-quantum cryptography for networks: A survey," in *Seventh International Conference On Mobile And Secure Services (MobiSecServ)*. IEEE, 2022.

[62] A. Huelsing, D. Butin, S.-L. Gazdag, J. Rijneveld, and A. Mohaisen, "XMSS: eXtended Merkle Signature Scheme," RFC 8391, May 2018. [Online]. Available: https://rfc-editor.org/rfc/rfc8391.txt

[63] R. Behnia and A. A. Yavuz, "Towards practical post-quantum signatures for resource-limited internet of things," in *Annual Computer Security Applications Conference*, 2021.

[64] A. A. Yavuz, S. E. Nouma, T. Hoang, D. Earl, and S. Packard, "Distributed cyber-infrastructures and artificial intelligence in hybrid post-quantum era," in *IEEE 4th International Conf. on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*. IEEE, 2022.

[65] D. McGrew, M. Curcio, and S. Fluhrer, "Leighton-micali hash-based signatures," Tech. Rep., 2019.

[66] P. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, Z. Zhang *et al.*, "Fast-fourier lattice-based compact signatures over ntru," 2019.

[67] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, "The sphincs+ signature framework," in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 2129–2146.

[68] J. H. Cheon, H. Choe, J. Devevey, T. Güneysu, D. Hong, M. Krausz, G. Land, M. Möller, D. Stehlé, and M. Yi, "Haetae: Shorter lattice-based fiat-shamir signatures," *Cryptology ePrint Archive*, 2023.

[69] "Unbalanced oil and vinegar," https://www.uovsig.org/, accessed: Aug, 2023.

[70] "Sqisign," https://sqisign.org/.

[71] D. Rotaru and T. Wood, "Marbled circuits: Mixing arithmetic and boolean circuits with active security," in *International Conference on Cryptology in India*. Springer, 2019.

[72] M. S. Şahin and S. Akleylek, "A survey of quantum secure group signature schemes: Lattice-based approach," *Journal of Information Security and Applications*, vol. 73, p. 103432, 2023.

[73] M. Buser, R. Dowsley, M. Esgin, C. Gritti, S. Kasra Kermanshahi, V. Kuchta, J. Legrow, J. Liu, R. Phan, A. Sakzad *et al.*, "A survey on exotic signatures for post-quantum blockchain: Challenges and research directions," *ACM Computing Surveys*, vol. 55, no. 12, 2023.