

Getting Ready for the Future (or Now): Towards a Cybersecurity Fabric for Future Integrated Satellite-Terrestrial Networks

Gürkan Gür* and Attila Altay Yavuz†

*Zurich University of Applied Sciences (ZHAW), Winterthur, Switzerland

†University of South Florida (USF), Tampa, Florida, USA

gueu@zhaw.ch, attilaayavuz@usf.edu

Abstract—In this paper, we outline a fast and lightweight network security fabric and identify the research gaps for developing such a fabric that respects the needs of trustworthy NextG SATIN for the post-quantum era. To achieve these objectives, we identify in which research directions more innovations are needed, namely algorithmic (NIST-PQC, distributed computing, time-disclosed cryptography), architectural (decentralized SATIN, distributed key management), and evaluation aspects.

I. INTRODUCTION

The emerging satellite networks will play a vital role in next-generation (NextG) networked systems and applications such as mobile networks (e.g., 6G [1]) and the Internet of Things (IoT) [2]. They will create a multi-layered ubiquitous connectivity substrate for facilitating the Internet of Everything (IoE) vision, integrating with terrestrial and aerial networks [3] for seamless applications. It is critical to ensure the reliability and safety of these satellite-enabled systems and services. Although generic network security protocols exist, the unique characteristics of emerging satellite systems and their interplay with hybrid network architectures pose significant performance/reliability challenges. Satellite systems' delay-aware and error-prone nature and the complex software/network stack of space-aerial-terrestrial integrated networks (SATIN) [4] require efficient and lightweight network security protocols [5]. Moreover, the energy consumption of any communication-computation system, let alone SATINs, is important due to the global goal of net-zero operation while meeting security requirements as needed and when needed. These challenges are compounded when the security threats of emerging quantum computers are considered [6]. It is well-known that post-quantum cryptography (PQC) standards [7] are costly for mobile networks [8]. Therefore, it is an open research problem to devise network security protocols that respect the performance and reliability needs of the new SATIN. Moreover, there is a need for systematic performance evaluation of such network security protocols when they are coupled with SATIN.

In this paper, we elaborate on these research gaps towards developing a fast and lightweight network security fabric that respects the needs of trustworthy NextG SATIN for the post-quantum era. To achieve these objectives, we delineate the

innovations on multiple fronts, including algorithmic (NIST-PQC, distributed computing, time-disclosed cryptography), architectural (decentralized SATIN, distributed key management), and evaluation aspects of SATIN.

II. RESEARCH GAPS, REQUIREMENTS, AND OPEN PROBLEMS

For a PQC-compliant cybersecurity fabric, the following open research gaps and questions are crucial:

- 1) **Lack of performance and impact profiling of emerging PQC technologies for NextG SATINs:** A key question is "What is the performance profile of forthcoming NIST-PQC standards in SATIN settings?". Currently, the impact of PQC standards only has been investigated in basic protocols (e.g., [9], [10]). Due to their dynamic, large-scale, and heterogeneous nature, it is a challenging research problem to profile the impacts of PQC in SATIN-enabled applications.
- 2) **Lack of delay-awareness in PQC standards:** NIST-PQC schemes are not designed with real-time systems in mind, and are costly for delay-aware SATINs (e.g., satellite-vehicular/drones) [11], [12]. How can we achieve delay awareness for NIST-PQC while keeping an eye on standard compliance? What are speed-storage-compliance trade-offs for varying degrees of standard deviation in exchange for efficiency/complexity?
- 3) **Critical gap in unleashing architectural potential of SATIN for PQ era:** The federated cloud and parallel computing enabled breakthroughs in fields like federated learning. Along the same line, what are the awaiting opportunities in synergizing unique features of SATINs like decentralized terrestrial computing layer and hyper-connectivity with PQC to make them practical? How can we bridge the interdisciplinary gap between SATINs and PQ-safe network security protocols?
- 4) **Lack of lightweight and energy-aware PQC for SATIN:** NIST-PQC signatures [7] are significantly costlier than their conventional-secure counterparts [13], and are not practical for low-end IoE devices [14]). Can we achieve lightweight signing for PQC signatures, with a full and secure deployment potential on low-end

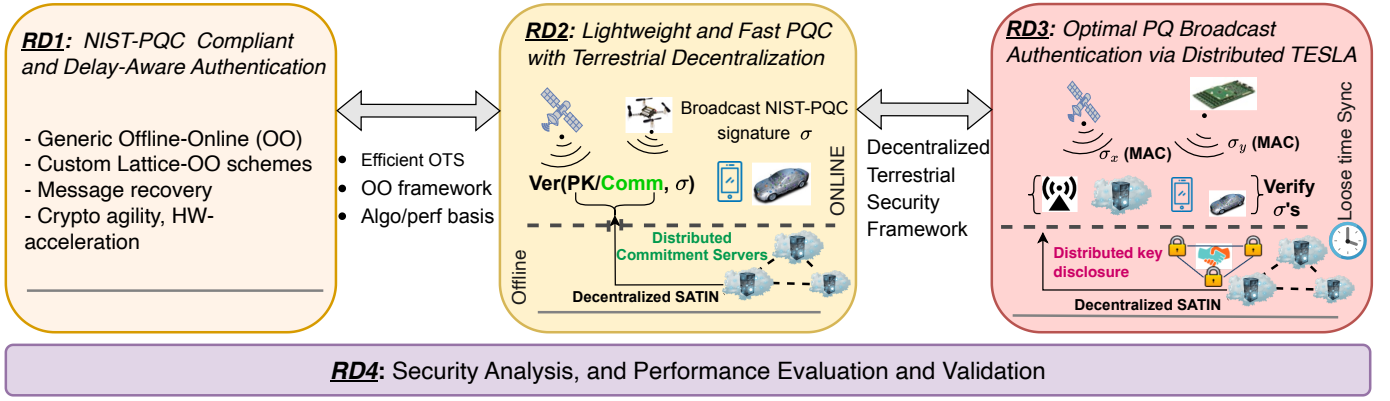


Fig. 1. Research directions for a NextG SATIN security fabric.

(e.g., 8-bit) devices? How can we exploit the distributed computing of the decentralized layer in SATIN to attain energy-aware signing that otherwise might not be possible?

- 5) **Dilemma of near-optimal PQ-security and broadcast authentication for SATIN:** Symmetric-key-based authentication offers near-optimal efficiency and PQ-security, yet it lacks public verifiability and scalability sorely needed by SATINs. Can we achieve “the best of both worlds” by raising near-optimal PQ-safe broadcast authentication by enhancing time-factor-based protocols (e.g., TESLA [15], [16])? Is it possible to mitigate the limitations of such protocols by developing decentralized key management strategies via SATIN architectures?

III. RESEARCH DIRECTIONS

We propose a novel cybersecurity fabric through the following four research directions (Figure 1) toward addressing the aforementioned open research problems in the SATIN domain. The mapping of research gaps to research directions are depicted in Figure 2.

A. RD-1: Offline-Online Strategies for PQ-Standard Compliant and Delay-Aware Authentication

A fast and NIST-PQC compliant authentication framework that respects the delay needs of SATINs is an important research direction. Due to their sheer importance in NextG networks, mitigating the delay of NIST-PQC schemes is important. Generic offline-online (OO) techniques [17] for NIST-PQC signatures [7] to minimize their signing cost is one research topic. Efficient algebraic one-time signatures (OTS), which is independent of interest, to support OOs and schemes in RD-3 are also necessary. Custom OO techniques (e.g., [18]) for a NIST-PQC signature [19] with varying degrees of departure from the standard in exchange for better efficiency. Such OO framework can be extended by enabling message recovery (MR) [20], [21] to reduce transmission overhead, hybrid constructions [22] to offer cryptographic agility [23], and hardware acceleration [24] to push the computational performance to the edge. The outcome of this research direction

can lead to a new delay-aware OO framework that offers an algorithmic and performance baseline for RD-2 and 3.

B. RD-2: Lightweight and Fast PQC with Terrestrial Decentralization

A set of lightweight and delay-aware network security mechanisms based on the assets from RD-1 can be developed. One of the main limitations of OO approaches is the need for linear storage and regeneration of expensive cryptographic tokens (e.g., a commitment value per message) on the signer. While OO can reduce the delay, its linear overhead is not feasible for low-end devices comprising a vital portion of SATIN-enabled IoE. Addressing this fundamental limitation requires bringing novelty in both algorithmic and architectural fronts: The transformation of OO-Dilithium in RD-1 such that the storage/generation of commitments is shifted from the signer to the verifier is another research topic. This goal can be achieved via a new “commitment separation strategy” that takes into account special features of lattice-based signatures (e.g., rejecting sampling [19]).

Harnessing terrestrial decentralization and distributed verification via the envisaged SATIN fabric can lift the cap on the number of signatures to be computed. Distributed computational servers can jointly supply verifiers with necessary commitments, considering both semi-honest [25] and malicious settings (via trusted execution environments [26]). This RD can facilitate lightweight PQC signatures that is suitable for low-end IoE devices while offering a low end-to-end delay.

C. RD-3: Near-Optimal PQ Broadcast Authentication with Distributed Time-Factor

The solutions in RD-1 and RD-2 innovate on NIST-PQC standards, and are based on public-key cryptography. However, symmetric-key-based schemes offer a near-optimally efficient PQ-safe authentication but without scalability and public verifiability. In this research direction, a promising solution is to resolve this conflict by unlocking the potential of time-factor-based solutions via decentralized SATINs. Timed Efficient Stream Loss-tolerant Authentication (TESLA) [15], which permits public verification of Message Authentication

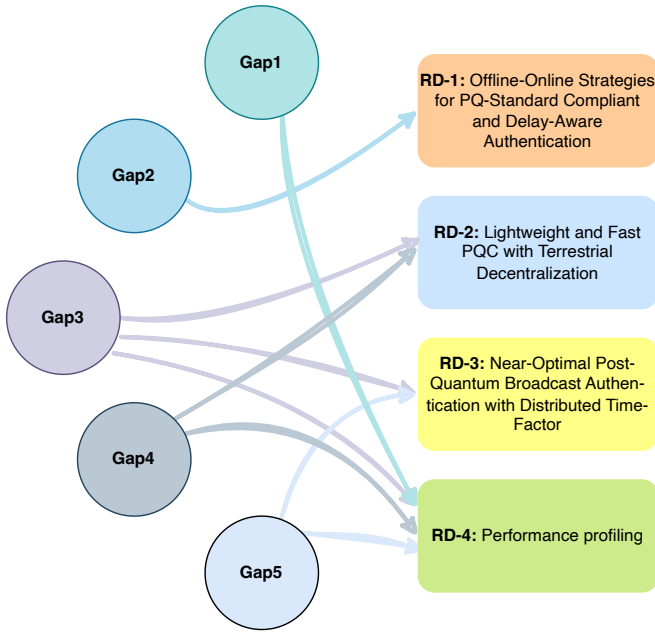


Fig. 2. Mapping of research gaps to research directions for a NextG SATIN cybersecurity fabric.

Codes (MAC) [27] via partially synchronized delayed-key disclosure, is a potential solution. TESLA can be improved via Universal MACs [28] to enable OO and MAC aggregation, thereby reducing buffering storage/delay. However, a detailed assessment of factors impacting TESLA for NextG networks for modern SATIN architectures (e.g., packet loss, delay) is crucial. Additionally, the packet loss and synchronization issues are two main weaknesses of TESLA. A unique strategy is to exploit the decentralized SATIN framework in RD-2 to enable a distributed disclosure of keying materials at the terrestrial layer. This unique strategy is expected to shield ground receivers from the sender's network conditions, thereby opening a path for unlocking the sheer potential of TESLA-type protocols to attain near-optimal PQ security for SATINs.

D. RD-4: Performance Evaluation and Validation

A comprehensive performance evaluation of a cybersecurity framework via theoretical analysis, full-fledged implementations, and large-scale network simulations (e.g., NS3 [29]) encapsulating various types of devices (e.g., from 8-bit devices to GPU-enabled clusters), networking environments, and protocols is needed. Such evaluation will fill the critical gap in profiling conventional-secure and PQ-secure NIST standards in the SATIN context by capturing intricacies like complex topologies, different network protocols, and parameters (e.g., packet loss, fragmentation, latency). A threat model and security analysis to complement provable security arguments need to be developed for any cryptographic schemes contained in the cybersecurity fabric. The outcome of this research direction can lead to a comprehensive cybersecurity evaluation fabric for fast and lightweight PQC in SATINs that will serve as a testbed for future research endeavors.

IV. CURRENT STATE OF RESEARCH

The proposed fabric aims to achieve lightweight, fast, and standard-compliant post-quantum secure broadcast authentication for SATINs, leading to outcomes with a transition-to-practice potential. Therefore, we focus on two classes of techniques in the literature from the lenses of their practicality and scalability in SATINs. That is, we first focus on NIST-PQC digital signatures for scalable and standard-compliant PQ-safe broadcast authentication for SATINs. We then focus on symmetric-key-based broadcast authentication via time factor. We will outline the limitations of related work in these broad categories here.

A. Current and Emerging NIST-PQC Standards

NIST has selected PQC standards [7] in June 2022, and they are expected to be crucial for NextG networks. The NIST-PQC standards harbor lattice-based signatures CRYSTALS-Dilithium [19], Falcon [30], CRYSTALS-Kyber (key-establishment) and a hash-based signature SPHINCS+ [31]. Moreover, NIST created a new addendum to their PQC standardization efforts [32] with a call for additional signature candidates (July 2023). However, the evaluation and analysis of this new round will likely last several years [32].

The performance of NIST-PQC schemes has been investigated for basic communication protocols such as PQ-TLS [6], [10], [33]–[36]. The lattice-based schemes show the best performance in terms of balanced key sizes and signing/verification delay. The overall results show an increased overhead compared to the conventional counterparts, but only tolerable for basic use cases involving a small static number of participants, and especially when it is feasible to fall-back symmetric key (one-to-one) cryptography via key encapsulation. It is, however, known that NIST-PQC standards are not designed for highly dynamic, large-scale, heterogeneous, delay-aware, and lightweight networked systems.

B. Delay-Aware and Lightweight Broadcast Authentication - Challenges of PQC and SATIN

The cryptographic delay introduced by the conventional-secure NIST standards (e.g., ECDSA [37]) can disrupt the delay-aware applications (e.g., vehicular [38], aerial drones [3], [24]). The conventional-secure signatures suffer from performance hurdles for vehicular protocols (e.g., IEEE WAVE [39]), wherein a large number of basic safety messages are broadcast per second. These challenges grow for connected vehicles' Security Credential Management System (SCMS) [40] protocol with several short-term pseudonym certificates.

Yet, NIST-PQC standards are significantly costlier than conventional secure counterparts, and therefore their integration into real-time and/or lightweight networks will vastly exacerbate the impacts of cryptographic overhead over such applications. There is a currently limited number of studies on this subject, and they confirm the significant performance challenges of PQC solutions for dynamic mobile networks (e.g., vehicular [11], [41], [42] and 6G [12], [43]). A similar

research gap also applies to lightweight regimes, as NIST-PQC signatures are currently not practical for resource-limited IoE components [14], [26]. These problems will become more severe in SATINs, since some satellite applications require broadcast authentication with high rates of bulk data transmission (e.g., image, GPS signals, and ISR data), and therefore require high cryptographic throughput [44]. Furthermore, PQ certificate chains are larger than their conventional counterparts, with higher depths due to the large geographical areas covered, increasing verification delays. Finally, SATIN systems will be integrated into various IoE applications, and demand to operate with lightweight IoT settings. Therefore, there is a vital need for lightweight and fast PQ-secure signatures that mitigate the cryptographic overhead of NIST-PQC standards for SATIN applications.

Another important concept is hybrid PQC-conventional techniques that combine both classical and post-quantum schemes [45] so that as long as at least one of the algorithms used remains secure, the hybrid will remain secure [22]. This concept promotes cryptographic agility [23], which is another important research topic.

C. PQ Broadcast Authentication with Time-Factor

The basic symmetric-key cryptography offers near-optimal performance with PQ-safety, but unfortunately is not scalable for dynamic broadcast environments. However, Perrig et al's TESLA (Timed Efficient Stream Loss-tolerant Authentication) [15] achieves a public verification of Message Authentication Codes (MACs) [27], albeit by leveraging time-factor and loose time synchronization. There is some recent work on TESLA's integration into various use cases (e.g., biometric [46], vehicular [47], others [16]). However, they do not aim to mitigate the fundamental limitations of TESLA in terms of large-scale key management, disclosure, and synchronization hurdles, nor do they consider complex SATIN cases. One research direction is to develop strategies by harnessing SATIN's unique features to unleash the sheer potential of TESLA for near-optimal PQ-safe broadcast authentication.

D. Comprehensive Evaluation of PQC in SATIN

One of the most critical gaps in the state of the art lies in a comprehensive evaluation of PQC in complex SATIN settings. For example, there is a lack of protocol-level performance analysis for SATIN such as satellite to drone to terrestrial scenarios. These systems use a variety of protocols such as DVB-X, delay-tolerant protocols, and Mavlink [48]. It is not clear how the delay of PQC, packet fragmentation due to extra packets, and packet loss impact the overall efficiency in these heterogeneous systems. There is a lack of holistic global performance analysis with simulations, e.g., for various multi-tiered satellite systems with multiple terrestrial connections and high dynamicity. This is more challenging when a multitude of IoT components in the IoE paradigm are integrated. Given millions of objects, how the protocol level differences for conventional versus NIST-PQC versus the proposed cybersecurity fabric will manifest themselves needs

to be investigated. Moreover, the trade-offs between distributed computing/offloading and PQC optimization deserve more attention.

V. CONCLUSION

Enabling efficient and secure broadcast functionalities by innovating on emerging PQC standards [7] via new offline-online transformations, distributed execution strategies, and algorithmic improvements is crucial for a novel cybersecurity SATIN fabric. The architectural capabilities of the terrestrial segment to mitigate the PQ commitment (and/or private/public keys) generation and distribution burden while enabling resilient key management for SATIN protocols are an important research topic. Any such fabric should be accompanied by a comprehensive performance evaluation framework with simulations and tests (e.g., over NSF FABRIC [49]) for novel network security assets that encapsulate several satellite-enabled applications and software-defined network architectures. Overall, these proposed research efforts are expected to make a significant impact by enabling trustworthy NextG satellite-terrestrial networks.

ACKNOWLEDGMENT

This work has received co-funding from the NSF and SNSF, in the framework of the SATUQ project under **SNSF (Grant No 10000409)** and **NSF (ECCS 2444615)**.

REFERENCES

- [1] P. Porambage, G. Gür, D. P. M. Osorio, M. Livanage, and M. Ylianttila, "6G security challenges and potential solutions," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 2021, pp. 622–627.
- [2] X. Zhu and C. Jiang, "Integrated satellite-terrestrial networks toward 6G: Architectures, applications, and challenges," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 437–461, 2022.
- [3] M. O. Ozmen and A. A. Yavuz, "Dronecrypt - An Efficient Cryptographic Framework for Small Aerial Drones," in *2018 IEEE Military Communications Conference (MILCOM 2018)*, 2018, pp. 1–6.
- [4] F. Rinaldi, H.-L. Maattanen, J. Torsner, S. Pizzi, S. Andreev, A. Iera, Y. Koucheryavy, and G. Araniti, "Non-terrestrial networks in 5G & beyond: A survey," *IEEE Access*, vol. 8, pp. 165 178–165 200, 2020.
- [5] S. B. R. Tirmizi, Y. Chen, S. Lakshminarayana, W. Feng, and A. A. Khuwaja, "Hybrid satellite-terrestrial networks toward 6G: Key technologies and open issues," *Sensors*, vol. 22, no. 21, 2022.
- [6] P. Schwabe, D. Stebila, and T. Wiggers, "Post-Quantum TLS Without Handshake Signatures," in *2020 ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, 2020, pp. 1461–1480.
- [7] NIST, "PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates," Available at <https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4>, 2022.
- [8] R. G. L. D'Oliveira, A. Cohen, J. Robinson, T. Stahlbuhk, and M. Médard, "Post-quantum security for ultra-reliable low-latency heterogeneous networks," in *MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM)*. IEEE Press, 2021, p. 933–938.
- [9] D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, "Post-Quantum Authentication in TLS 1.3: A Performance Study," in *27th Annual Network and Distributed System Security Symposium (NDSS 2020)*. The Internet Society, 2020.
- [10] M. Schöffel, F. Lauer, C. C. Rheinländer, and N. Wehn, "Secure IoT in the era of quantum computers—where are the bottlenecks?" *Sensors*, vol. 22, no. 7, p. 2484, 2022.

- [11] N. Bindel, S. McCarthy, H. Rahbari, and G. Twardokus, "Suitability of 3rd Round Signature Candidates for Vehicle-to-Vehicle Communication –Extended Abstract," National Institute of Standards and Technology, Extended Abstract, 2021, available at <https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/bindel-suitability-abstract-pqc2021.pdf>.
- [12] M. A. Lopez, G. N. N. Barbosa, and D. M. F. Mattos, "New barriers on 6G networking: An exploratory study on the security, privacy and opportunities for aerial networks," in *2022 1st International Conference on 6G Networking (6GNet)*, 2022, pp. 1–6.
- [13] National Institute of Standards and Technology, "Digital Signature Standard (DSS)," FIPS PUB 186-5 (Draft), October 2019, available at <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5-draft.pdf>.
- [14] R. Behnia and A. A. Yavuz, "Towards practical post-quantum signatures for resource-limited Internet of Things," in *Annual Computer Security Applications Conference (ACSAC)*, 2021, p. 119–130.
- [15] A. Perrig and J. Tygar, "Tesla broadcast authentication," *Secure Broadcast Communication: In Wired and Wireless Networks*, pp. 29–53, 2003.
- [16] K. Eledlebi, A. A. Alzubaidi, C. Y. Yeun, E. Damiani, V. Mateu, and Y. Al-Hammadi, "Enhanced Inf-TESLA protocol: A continuous connectivity and low overhead authentication protocol via IoT devices," *IEEE Access*, vol. 10, pp. 54912–54921, 2022.
- [17] S. Even, O. Goldreich, and S. Micali, "On-line/off-line digital signatures," in *Advances in Cryptology — CRYPTO' 89 Proceedings*, G. Brassard, Ed. New York, NY: Springer New York, 1990, pp. 263–275.
- [18] P. Zhang, H. Yang, L. Zhu, Y. Zhang, H. Wang, and Q. Xu, "A new lattice-based online/offline signatures framework for low-power devices," *Theoretical Computer Science*, vol. 962, p. 113942, 2023.
- [19] V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, D. Stehlé, and S. Bai, "CRYSTALS-DILITHIUM," National Institute of Standards and Technology, Tech. Rep., 2020, available at <https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions>.
- [20] A. A. Yavuz, F. Alagoz, and E. Anarim, "A new satellite multicast security protocol based on elliptic curve signatures," in *2006 2nd International Conference on Information Communication Technologies*, vol. 2, April 2006, pp. 2512–2517.
- [21] R. del Pino, V. Lyubashevsky, and D. Pointcheval, "The whole is less than the sum of its parts: Constructing more efficient lattice-based akes," in *Security and Cryptography for Networks*, V. Zikas and R. De Prisco, Eds. Cham: Springer International Publishing, 2016, pp. 273–291.
- [22] N. Bindel, U. Herath, M. McKague, and D. Stebila, "Transitioning to a quantum-resistant public key infrastructure," in *Post-Quantum Cryptography: 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings 8*. Springer, 2017, pp. 384–405.
- [23] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, 2022.
- [24] 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, pp. 2627–2639, 2017.
- [25] 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.
- [26] S. E. Nouma and A. A. Yavuz, "Post-quantum forward-secure signatures with hardware- support for Internet of Things," in *International Conference on Communications (ICC)*. IEEE, May 2023.
- [27] J. M. Turner, "The keyed-hash message authentication code (hmac)," *Federal Information Processing Standards Publication*, vol. 198, no. 1, pp. 1–13, 2008.
- [28] S. Ghosh and P. Sarkar, "Variants of Wegman-Carter message authentication code supporting variable tag lengths," *Des. Codes Cryptogr.*, vol. 89, no. 4, pp. 709–736, 2021.
- [29] NS3, "Network Simulator," <https://www.nsnam.org/>, 2022.
- [30] T. Prest, P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang, "FALCON," National Institute of Standards and Technology, Tech. Rep., 2020, available at <https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions>.
- [31] A. Hulsing, D. J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L. Gazdag, P. Kampanakis, S. Kolbl, T. Lange, M. M. Lauridsen, F. Mendel, R. Niederhagen, C. Rechberger, J. Rijneveld, and P. Schwabe, "Sphincs+," Submission to the NIST's post-quantum cryptography standardization process, 2018, https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/SPHINCS_Plus.zip.
- [32] National Institute of Standards and Technology, "NIST Announces Additional Digital Signature Candidates for the PQC Standardization Process," July 2023, <https://csrc.nist.gov/news/2023/additional-pqc-digital-signature-candidates>.
- [33] A. A. Yavuz, D. Earl, S. Packard, and S. E. Nouma, "Hybrid low-cost quantum-safe key distribution," in *Quantum 2.0 Conference and Exhibition*. Optica Publishing Group, 2022.
- [34] C. Paquin, D. Stebila, and G. Tamvada, "Benchmarking post-quantum cryptography in TLS," in *11th International Conference on Post-Quantum Cryptography (PQCrypto 2020)*. Springer, 2020, pp. 72–91.
- [35] A. Abdulrahman, V. Hwang, M. J. Kannwischer, and A. Sprenkels, "Faster kyber and dilithium on the Cortex-M4," in *Applied Cryptography and Network Security*, G. Ateniese and D. Venturi, Eds. Cham: Springer International Publishing, 2022, pp. 853–871.
- [36] M. L. Manna, P. Perazzo, L. Treccozzi, and G. Dini, "Assessing the cost of quantum security for automotive over-the-air updates," in *2021 IEEE Symposium on Computers and Communications (ISCC)*, 2021, pp. 1–6.
- [37] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, Aug 2001.
- [38] 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)*, May 2018, pp. 1–9.
- [39] IEEE, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities," *IEEE Std 1609.2.1-2022 (Revision of IEEE Std 1609.2.1-2020)*, pp. 1–261, 2022.
- [40] US Department of Transportation, "Connected Vehicle Deployment Technical Assistance Security Credential Management System (SCMS) Technical Primer," Available at <https://rosap.ntl.bts.gov/view/dot/43635>, 2022.
- [41] N. Bindel and S. McCarthy, "The need for being explicit: Failed attempts to construct implicit certificates from lattices," *The Computer Journal*, 10 2022.
- [42] N. Bindel, S. McCarthy, G. Twardokus, and H. Rahbari, "Drive (quantum) safe! – towards post-quantum security for V2V communications," *IACR Cryptol. ePrint Arch.*, p. 483, 2022. [Online]. Available: <https://eprint.iacr.org/2022/483>
- [43] T. C. Clancy, R. W. McGwier, and L. Chen, "Tutorial: Post-Quantum Cryptography and 5G Security," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 285–285.
- [44] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," *Computer Networks*, vol. 216, p. 109246, 2022.
- [45] E. Barker, L. Chen, and R. Davis, "Recommendation for key-derivation methods in key-establishment schemes," *NIST Special Publication*, vol. 800, p. 56C, 2018.
- [46] K. Eledlebi, C. Y. Yeun, E. Damiani, and Y. Al-Hammadi, "Empirical studies of TESLA protocol: Properties, implementations, and replacement of public cryptography using biometric authentication," *IEEE Access*, vol. 10, pp. 21941–21954, 2022.
- [47] C. Lyu, A. Pande, Y. Zhang, D. Gu, and P. Mohapatra, "Enabling fast and privacy-preserving broadcast authentication with efficient revocation for inter-vehicle connections," *IEEE Transactions on Mobile Computing*, pp. 1–18, 2023.
- [48] DroneCode Foundation, "MAVLINK 2 protocol," <https://github.com/mavlink/mavlink>.
- [49] I. Baldin, A. Nikolich, J. Griffioen, I. I. S. Monga, K.-C. Wang, T. Lehman, and P. Ruth, "FABRIC: A national-scale programmable experimental network infrastructure," *IEEE Internet Computing*, vol. 23, no. 6, pp. 38–47, 2019.