Post-Quantum Cryptography in the 5G Core

Thomas Attema*† , Bor de Kock† , Sandesh Manganahalli Jayaprakash†,
Dimitrios Schoinianakis‡ , Thom Sijpesteijn†, and Rintse van de Vlasakker†
*CWI, Amsterdam, The Netherlands
†TNO, The Hague, The Netherlands
‡Nokia Bell Labs, Athens, Greece

***Abstract*—In this work, the conventional cryptographic algorithms used in the 5G Core are replaced with post-quantum alternatives and the practical impact of this transition is evaluated. Using a simulation environment, we model the registration and deregistration of varying numbers of user equipments (UEs) and measure the resulting effects on bandwidth consumption and latency. Our results show that the deployment of post-quantum cryptographic algorithms has a measurable effect on performance, but that this effect is small, and perhaps more crucially, that the extra overhead needed in terms of computation and bandwidth does not have any substantial impact on the usability of the network and the efficiency of its network functions. Overall the experimental results in this work corroborate earlier research: the 5G Core is technically able to support post-quantum cryptography without any inherent issues connected to the increased computational overhead or larger message size.**

I. Introduction

Quantum computers will have a profound impact on the world as we know it: they will be able to perform computations that have so far been infeasible, thus realizing various breakthroughs in fields like chemistry and biology. Unfortunately, the emergence of quantum computing has introduced unprecedented risks to modern cryptographic frameworks — the foundation of our digital security and economy — necessitating urgent reconsideration of security protocols across digital infrastructures. Shor's quantum algorithm threatens to compromise widely deployed public-key cryptographic systems by solving some mathematical problems, such as integer factorization and discrete logarithms, in polynomial time — tasks that remain computationally infeasible for classical computers. As the mathematical foundation of many cryptographic algorithms is based on the assumption that these problems are impossible to solve, this is a problem — and this vulnerability extends to the cryptographic foundations of 5G networks, which rely heavily on these conventional protocols to secure data transmission, user authentication, and data integrity.

As 5G networks become the backbone of global connectivity, their long operational lifecycle raises concerns about future-proofing against quantum threats. Current encryption methods securing 5G communications will be broken once quantum computers achieve sufficient scale, exposing sensitive data to retroactive decryption attacks. This "harvest now, decrypt later" risk underscores the critical need to preemptively integrate quantum-resistant cryptographic primitives into the 5G Core (5GC) architecture.

By adopting standards for post-quantum cryptography (PQC), which rely on mathematical problems resistant to both conventional and quantum attacks, the 5G Core can mitigate vulnerabilities while maintaining compliance with evolving regulatory and industry requirements. Various standardization organizations (such as the IETF [1]) and NIST in the United States [2]) as well as policy makers (such as the European Commission [3], BSI in Germany [4] and NCSC in the United Kingdom [5]) have started to encourage transitioning to post-quantum security within the next coming years — or even require it in order for security certifications to be upheld. It is to be expected that mobile network technologies will have to undergo this transition as well, within the coming years.

A. Background

a) Post-Quantum Cryptography (PQC): The development of large-scale quantum computers will have a large impact on the security of commonly used conventional cryptographic algorithms. Shor's algorithm from 1994 [6] can be used to mount devastating attacks on the public key algorithms that currently secure most internet communications, including RSA [7] and Diffie-Hellman [8]. This means the development of new algorithms for key establishment and digital signatures is a requirement. To address this need, the United States National Institute

Author list in alphabetical order.
Document date: December 23, 2025.

of Standards and Technology (NIST) initiated a multi-year standardization effort to find new algorithms for key encapsulation (KEM) and digital signature algorithms (DSA), a process that at the time of writing has lead to its first published standards. This Post-Quantum Cryptography standardization process was highly transparent and in collaboration with the cryptographic research community at large [9]. In contrast, the impact of quantum computing on symmetric cryptography is far more limited: although there has been a discussion on whether Grover's algorithm is able to brute-force 128-bit symmetric keys, NIST recently clarified that 128-bit keys for AES remain quantum-safe for decades to come [10].

In this work, our experiments rely on KEMs and digital signature algorithms from this NIST competition: for KEMs, we evaluate the code-based BIKE algorithm [11] as well as the lattice-based FrodoKEM [12]. For digital signatures, our experiments include algorithms based on Module Lattices (ML), Stateless Hash functions (SLH), and Fast Fourier Transforms over NTRU lattices (FN). Specifically, ML-DSA is the standardized algorithm previously known as *Dilithium* [13], and SLH-DSA corresponds to the hash-based scheme formerly referred to as *SPHINCS+* [14]. The lattice-based scheme *Falcon* [15] has also been selected for standardization, with its final standards document still under development [16]; upon publication, *Falcon* is expected to be renamed FN-DSA. We also evaluate the performance of elliptic curve (`secp2561`) and RSA-signatures to, to compare their performance with their PQC equivalents. For a thorough overview on post-quantum cryptography in general and the various 'families' of algorithms, we refer the reader to e.g. [17], [18], [19].

On a final note, we use the term *conventional cryptography* to refer to cryptography from before the post-quantum transition, i.e. cryptography that was not built with resistance against quantum adversaries in mind.

b) Hybridization of conventional and post-quantum cryptography: The term *hybrid cryptography* can refer to several concepts, but in this work we refer to the combination of a conventional and a post-quantum algorithm into one scheme that has (some of) the benefits of both. There are several reasons that justify the use of hybrid cryptographic schemes. First, at the beginning of the post-quantum standardization process by NIST, there was some uncertainty whether these new protocols would indeed turn out to be secure in the longer run; adding a layer of conventional cryptography as well, meant that the security of protocols would at the very least not decrease below the original level.

Another reason a combination of conventional and post-quantum can make sense is the attacker model for *current* deployments of post-quantum cryptography. A common frame of reference are so-called *harvest-now, decrypt-later* attacks, in which we assume that a nation-state adversary stores large amounts of encrypted data now, so that attacks can be mounted whenever quantum computers are indeed available to perform them. Under this assumption we require post-quantum secrecy, but not yet post-quantum authentication: if an attacker stores messages now they can later try and break the encryption, but will not achieve anything by breaking the authentication.

A downside is that the combination of two schemes will always add computational overhead and can also increase the message size of the key — although the latter can be mitigated by e.g. `xor`'ing the two protocols' keys instead of sending both [20].

Using hybrid schemes is promoted by several standardization bodies,[21], [22] and is natively supported in various applications including the TLS implementation we use in our experiments. Because of this — and as we do not expect the added computational overhead to be problematic for our use case — we opt to use hybridized versions of post-quantum algorithms instead of standalone post-quantum algorithms in this work.

c) Transport-Layer Security (TLS): TLS is a security protocol used for a variety of internet applications, most visibly `https` web traffic. Due to its versatility in terms of modes and ciphersuites, variations of TLS are used in a range of protocols, including industrial applications and IoT home appliances. Although variants using a pre-shared key exist, most commonly TLS starts with a handshake between client and server, where among other things the cryptographic primitives and key lengths are negotiated depending on the capabilities of both parties. Newer TLS versions offer high flexibility in terms of ciphersuites, making it easy to exchange insecure protocols for post-quantum protocols such as the ones mentioned in the previous paragraph. In recent years much has been published about how to achieve full post-quantum security in TLS, either by replacing the classical signatures with a post-quantum alternative [23] or by changing the approach to authentication altogether. In KEMTLS, for example, signatures in the handshake are replaced with instantiations of KEMs from the NIST competition [24]. An overview of the various strategies to migrate TLS to a post-quantum version can be found in [25].

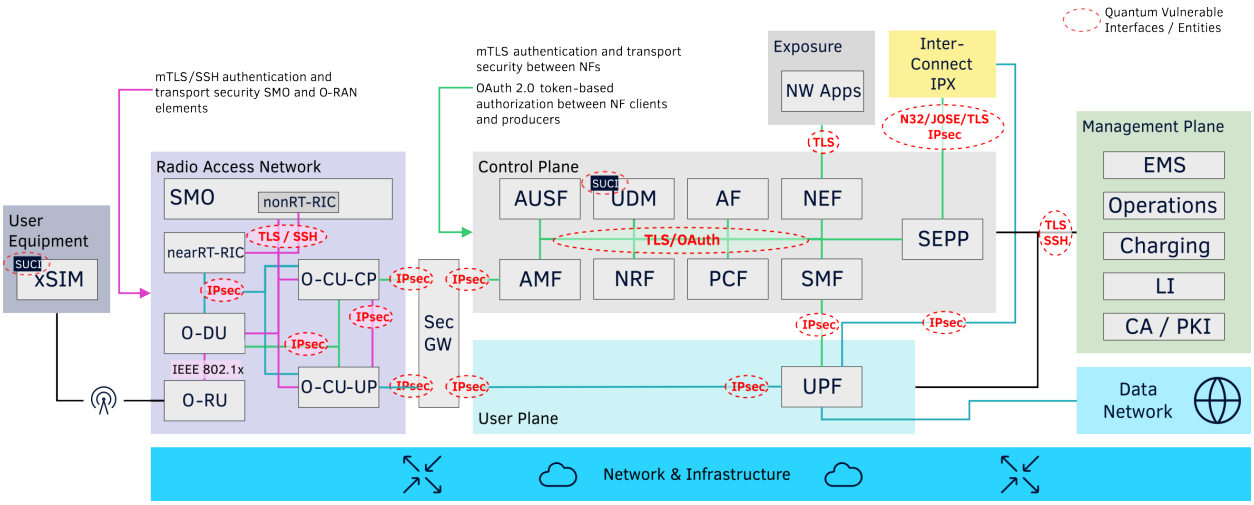

Fig. 1. Overview of vulnerable interfaces in a 5G network [26].

d) The 5G core network (5GC): The security architecture of 5G networks represents a marked departure from previous generations, reflecting fundamental changes in the design and deployment of authentication, authorization, and encryption mechanisms. Earlier generations of mobile networks relied predominantly on symmetric-key cryptography: the Subscriber Identity Module (SIM) stored a long-term shared secret that enabled mutual authentication between the user equipment (UE) and the network [27]. While effective in earlier deployment contexts, this model offered limited flexibility and did not readily accommodate the scale and heterogeneity of emerging services.

In contrast, 5G adopts a cloud-native, microservice-oriented core architecture and makes extensive use of Internet protocols and standards—most notably Transport Layer Security (TLS) and OAuth 2.0—to secure service-to-service communication [27]. This architectural transition is accompanied by a shift in the trust model: rather than relying primarily on long-term symmetric secrets, 5G core security increasingly depends on a Public Key Infrastructure (PKI)-based framework to support dynamic authentication and scalable key management [27]. Although this change improves operational agility, it also expands the attack surface with respect to quantum-capable adversaries, since public-key primitives are precisely the class of mechanisms threatened by Shor-type attacks [27], [28].

More broadly, the 5G security architecture spans multiple domains, including access-network security, core-network security, and service-based architecture (SBA) security, each with distinct constraints that influence the integration of post-quantum cryptography (PQC) [28], [29]. The core network is of particular relevance in this context: its virtualized network functions (VNFs) and service-based interfaces both enable comparatively agile software updates and create practical opportunities for cryptographic migration [28]. At the same time, virtualization and increased software complexity introduce additional risks (e.g., misconfiguration, expanded trust relationships, and interface exposure), underscoring the need to integrate PQC within a comprehensive and systematically engineered security framework [28], [29].

e) Current Vulnerabilities and Security Requirements: Despite its advanced security features, the 5G architecture contains inherent vulnerabilities that quantum computing may exploit. The transition to software-based network functions increases the attack surface and potential for exploitation through software vulnerabilities [28]. Additionally, the reliance on PKI for authentication and authorization makes 5G networks particularly susceptible to quantum attacks that can break the underlying mathematical problems of current public key cryptosystems [27], [28].

The security requirements for 5G networks are demanding and multifaceted, encompassing data confidentiality, integrity, authenticity, privacy, and availability [29]. These requirements are further complicated by the diverse use cases 5G supports, from enhanced mobile broadband (eMBB) to ultra-reliable low-latency communications (URLLC) and massive Internet of Things deployments [28]. Each use case presents unique security

challenges and performance constraints that must be considered when implementing post-quantum cryptography [30].

5G networks must also contend with the challenge of ensuring end-to-end security across a heterogeneous ecosystem of devices, networks, and service providers [31]. This complexity is amplified by the need to maintain interoperability with legacy systems while introducing quantum-resistant security measures [27]. The security architecture must therefore be flexible enough to accommodate different security profiles and cryptographic capabilities while ensuring a consistent security posture across the network [29], [30].

In Figure 1 a high-level overview of a 5G system is provided, highlighting the various interfaces and components that are vulnerable to quantum attacks. The figure emphasizes the need for a comprehensive security strategy that encompasses all aspects of the 5G architecture, from the radio access network (RAN) to the core network and service-based architecture [26]. The RAN provides connectivity between user equipment and the core, carrying user traffic and enabling access to network services. The core network coordinates interactions among network functions and supports secure transport for both user-plane and control-plane communication.

Figure 1 also shows that asymmetric cryptography and in particular TLS is extensively used to protect all communication between different components of the core network. These components referred to as Network Functions are critical; they carry out all the control plane traffic of all the users on the network. Therefore, it is imperative to develop and share more implementations and performance benchmarks with the community to better understand the effects of post-quantum cryptography on these components. This paper aims to address this need by investigating the challenges associated with migrating the 5G core to post-quantum cryptographic solutions.

B. Related work

Several recent works focus on implementing and benchmarking post-quantum variants of the TLS protocol [32], [33], including optimizations for embedded devices [34], [35], and evaluations specifically targeted at the Android mobile operating system [36]. Notably, the work in [33] reveals encouraging results for PQC adoption. For example, it was shown that HQC and Kyber perform comparably to legacy cryptography, while Dilithium and Falcon signature schemes demonstrate even faster performance. There were also no performance drawbacks observed from implementing hybrid cryptographic approaches. At higher NIST security levels, PQC algorithms actually outperformed currently deployed algorithms, although PQC might pose certain challenges when it comes to bandwidth-constrained applications [33].

Recent research on post-quantum cryptography (PQC) migration for 5G networks has focused on enhancing authentication protocols to address quantum threats. A notable contribution comes from researchers developing quantum-resistant extensions to the 5G Authentication and Key Agreement (AKA) protocol [37].

There is still a considerable gap when it comes to the evaluation of PQC in actual telecom networks. This is extremely relevant considering also the fact that, the 3GPP, IETF, ITU and O-RAN standardization initiatives for the development of PQC telecommunication standards are still in progress, and so it is crucial to explore the migration challenges of PQC in real-world telecom environments.

C. Our contributions

In this work we replaced the key establishment and digital signature algorithms in 5G with post-quantum alternatives, and tested what impact this has on the network when deployed on a lab setup resembling a real-world 5G core network, where only the radio part of the network is simulated.

The work was done concurrently with [28] and is similar in idea and execution. Since the approach was slightly different we decided to make our experiment public. It should be seen as a confirmation of known/existing results rather than as a novel contribution.

The main difference is that the authors of [28] implemented a custom open-source PQC-equipped `free5GCore` system to evaluate the initial handshake latency between VNFs. Their results suggest a negligible increase in UE connection setup duration and a small increase in connection setup data requirements. In contrast, in this work we considered a hybrid approach (described in Section I-A0b), and included a migration of the signature algorithms to a post-quantum variant. We also provide a more thorough analysis of the impact on the network at varying numbers of devices.

II. Experiments

A. Set-up of the 5G core.

The following experiments were performed in the 5G-lab at TNO, where we have access to an existing 5G core setup. An overview of the complete setup can be seen in Figure 2. In our core setup we use an Intel Next Unit of Computing-machine with an i7-8559U processor

(4 cores, hyperthreaded), to run a set of 10 network functions: NRF, AMF, UPF, UDR, UDM, AUSF, NSSF, BSF, PCF, and SMF. When starting the core network, the required signature and KEM algorithms are configured on each of the network functions, and the necessary TLS certificates are generated and loaded depending on this specification.

To make this possible, the following steps were first performed:

1) `openssl` was compiled against `liboqs` [38] to enable the `oqsprovider`, granting access to PQ-TLS algorithms.
2) `libcurl` was compiled against the `oqsprovider`-enabled `openssl`.
3) `libngthttp2` was compiled against the `oqsprovider`-enabled `openssl`.
4) `open5gs` was compiled against these custom versions of `libcurl` and `libngthttp2`.
5) Changes were made to `open5gs`'s interface to `libcurl` and `libngthttp2` to be able to set KEM and signature algorithms as a parameter in the NFs.
6) For each signature algorithm in the `oqsprovider`-enabled `openssl`, a set of PKI certificates was generated.

Now we are able to start the 5G core with any selection of PQ-algorithms.

B. Simulating radio connections.

The user equipment (UE) and the Radio Access Network (RAN) were simulated using the open source tool `ueransim` [39] on a separate Intel machine with the same specs as above. The two machines are connected over a 1 Gbit/s LAN connection over which the traffic between the radio access node and a core network is routed. `ueransim` enables us to create a large number of UEs using our experiment script.

At regular intervals, the simulated UEs send out a registration request (step (1) in Figure 3) followed by a PDU session creation request (step (2) in Figure 3) to the core network. For new UEs, this request then triggers setting up a secure connection between various network functions in the core network.

C. Choice of post-quantum algorithms.

Table I shows the algoritms chosen for our experiments. For BIKE, FrodoKEM, Falcon and ML-DSA a combination was made with a (conventional) ECC implementation, to achieve hybrid variants as described in Section I-A0b.

D. Experimental setup.

We run an experiment where we vary the number of active UEs. Each UE de-registers every t seconds, after which it immediately re-registers and requests a PDU session. An attempt is made to space out the re-registrations in time by starting the initial registrations for each UE t/n seconds apart, where t is the re-registration interval in seconds (usually $t = 10$) and n is the number of UEs.

The setup is built to measure both the latency and bandwidth impact of using these new algorithms, particularly focusing on the registration and PDU session establishment procedures. For latency the values indicate the total latency between the moment the `registration` request-message is sent and the moment the `registration accept-message` is received. For bandwidth we measure the total amount of data in bytes sent from/to each network function's SBI interface. These measurements are performed using `bpftrace`.

E. Results.

Both conventional and post-quantum algorithms are tested. We first analyze the duration of device registration and session creation during setup for various algorithm choices. In Figure 4 we use RSA for signatures and vary the KEM used for each experiment. In Figure 5 we use conventional (elliptic curve-based) Diffie-Hellman for key agreement, but vary the signature scheme. In the KEM-experiment we observe a small difference in registration time for the various KEMs; in the Signature-experiment the difference is larger and SPHINCS is the faster algorithm.

As described in the above, we mainly experimented with the effect the number of UEs has on network peformance. In Figure 6 we can observe a distinct jump in the timings for the 95th percentile, first visible at 40 UEs. The jump is roughly 200ms, and is most likely caused by a queue batching mechanism in the system, but we have not been able to determine which mechanism specifically causes this.[1] Analyzing these results with the assumption that there is indeed an unidentified batching mechanism in mind, we see a linear increase in the 95th percentiles. We have observed more jumps (up to 400ms, 600ms, etc.) at higher UE counts and higher percentiles, but many of these are the result of the system as a whole failing. Increasing the number of UEs to 130

[1]There are various timers in the `ueransim` software, some of which had a default value of 200ms, but altering the `ueransim` source code to change these timers had no effect on the results.

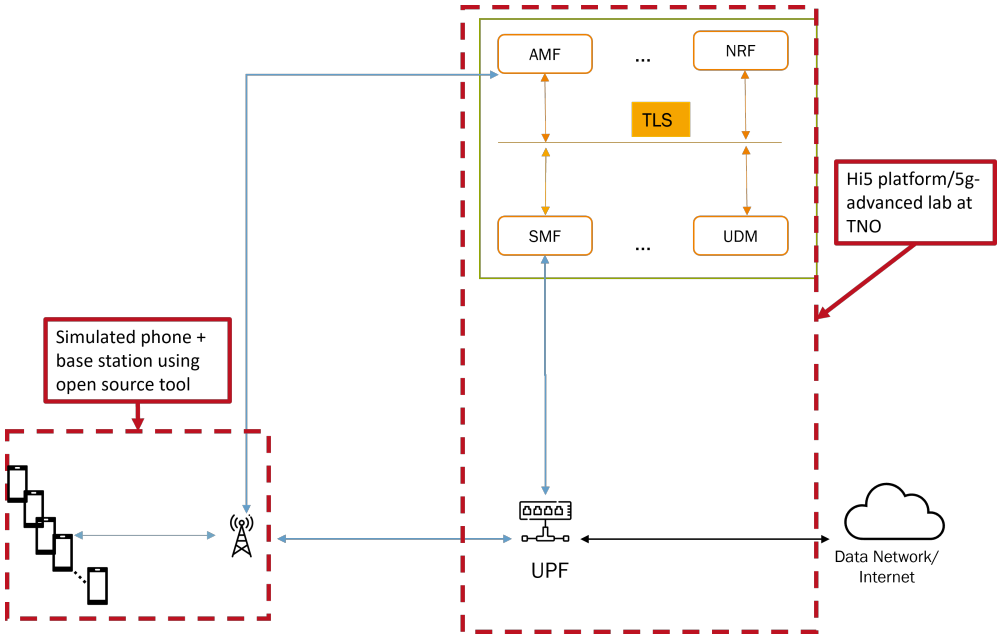

Fig. 2. The setup for the experiments described in this work.

TABLE I
THE KEY ENCAPSULATION MECHANISMS AND DIGITAL SIGNATURE ALGORITHMS USED IN THE EXPERIMENTS. REMARK THAT `rsaEncryption` REFERS TO RSA SIGNATURES.

KEM		DSA	
Plain ECC	`secp256r1`	RSA	`rsaEncryption`
BIKE	`p256_bikel1`	Falcon	`p256_falcon513`
	`p384_bikel3`	ML-DSA	`p384_mldsa66`
FrodoKEM	`p521_frodo1344shake`	SPHINCS+	`sphincssha2129ssimple`

and higher also leads to unpredictable behaviour, such as UE requests being ignored by the core/RAN, errors and warnings being triggered in the core etc. We have therefore chosen to limit our results to 120 UEs.

Under normal operating conditions, there is no clear difference between the conventional and post-quantum algorithms, even when looking at the results for higher percentiles. Considering outliers, however, the results of each algorithm selection diverge significantly, and the usage of post-quantum algorithms would lead to poor experience in such rare cases. This can be seen in Figure 7.

III. CONCLUSION & DISCUSSION

The main conclusion of this work is a positive one: we can update the algorithms used by TLS for key establishment and authentication in the 5G Core to a post-quantum variant without a substantial impact on the usability of the network. For future versions of 5G and its successors, this is good news.

As mentioned in the introduction, between conducting the experiments and preparing this manuscript, [28] performed a very similar experiment. This work further corroborates these earlier results and is consistent with their conclusion.

A. Future work

Several directions for future research were out of scope for the present study and are left as future work.

a) IPsec: The IPsec protocol [40] is used in cellular deployments to protect certain communication channels between the radio access network (RAN) and the 5G Core, including interfaces involving user-plane transport. Versions of IPSec with support for post-quantum cryptography exist, as well as drafts standards for new protocol standards that include it.[41], [42] Post-quantum-capable variants of IKE/IPsec have been proposed, and

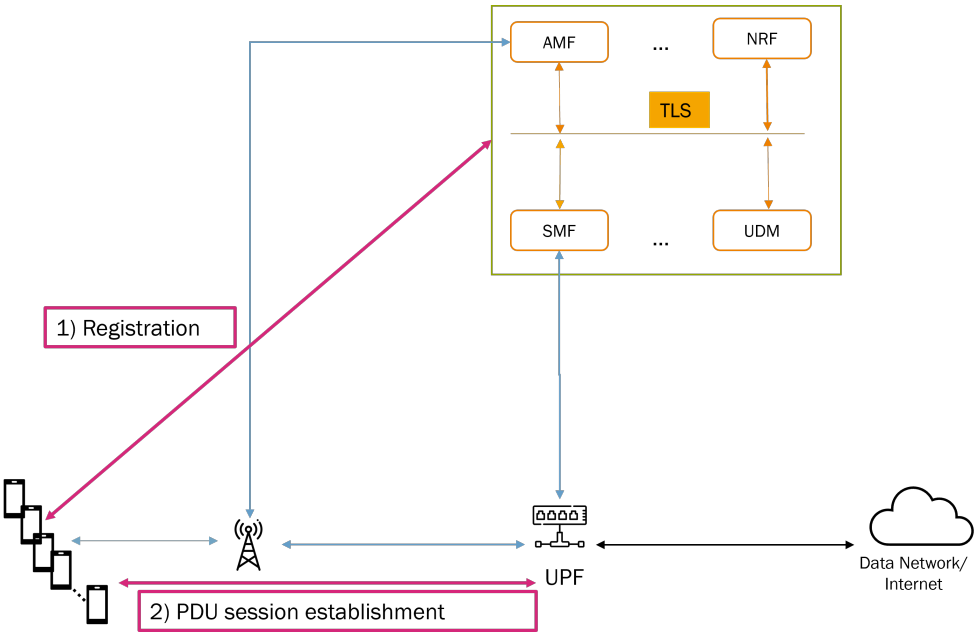

Fig. 3. A new registration request triggers setting up various connections in the core.

TABLE II
SUMMARY RESULTS OF THE PQ-TLS ENABLED OPEN5GS EXPERIMENTS.

Algorithms	UE setup duration Median	99th percentile	SBI data rate
`(secp256r1, rsaEncryption)`	257 ms	505 ms	111.0 KB/s
`(p384_bikel3, p384_mldsa65)`	264 ms	669 ms	114.8 KB/s
`(p384_bikel3, rsaEncryption)`	260 ms	571 ms	112.5 KB/s
`(secp256r1, p384_mldsa65)`	260 ms	507 ms	115.2 KB/s

several Internet-Drafts describe approaches for integrating post-quantum key establishment and authentication into IKEv2 [41], [42]. A natural extension of our work is to evaluate the performance and operational implications of such mechanisms within 5G deployments.

b) KEMTLS: A promising recent line of research explores instantiating TLS without conventionally generated digital signatures by replacing handshake signatures with instantiations of a (post-quantum) key-encapsulation mechanism (KEM). Especially in a post-quantum context this is promising, as the post-quantum signature algorithms from the NIST standardization project (including the ones mentioned in this work) are typically substantially more inefficient than their KEM counterparts, both in terms of computational efficiency and message size.[24], [43] Aditionally, they are typically more convoluted to implement.[25, Ch. 5] It should also be noted that various works on the topic of KEMTLS speficially point out its usability for TLS 1.3 session resumption-like use cases [25, §5.2], of which the 5G core with its known components is an example.

Despite the availability reference implementations of KEMTLS exist, deploying these in the 5G Core is a challenge as the 5G Core is largely written in `C`, including the TLS implementation it uses. Perhaps the most promising implementation of KEMTLS is based on the `rustls` project,[2] [3] and while the `rustls` community has an (ongoing) project to provide FFI-bindings for easy integration with a language such as `C`,[4] the work on `C`-bindings only properly started after the KEMTLS-fork

[2] `rustls`-project: https://github.com/rustls/rustls/. Accessed at commit `bdb3036`.

[3] `rustls`-fork that provides KEMTLS: https://github.com/thomwiggers/rustls/. Accessed at commit `8d3925e`.

[4] `rustls-ffi`-project: https://github.com/rustls/rustls-ffi. Accessed at commit `4d1d5d8`.

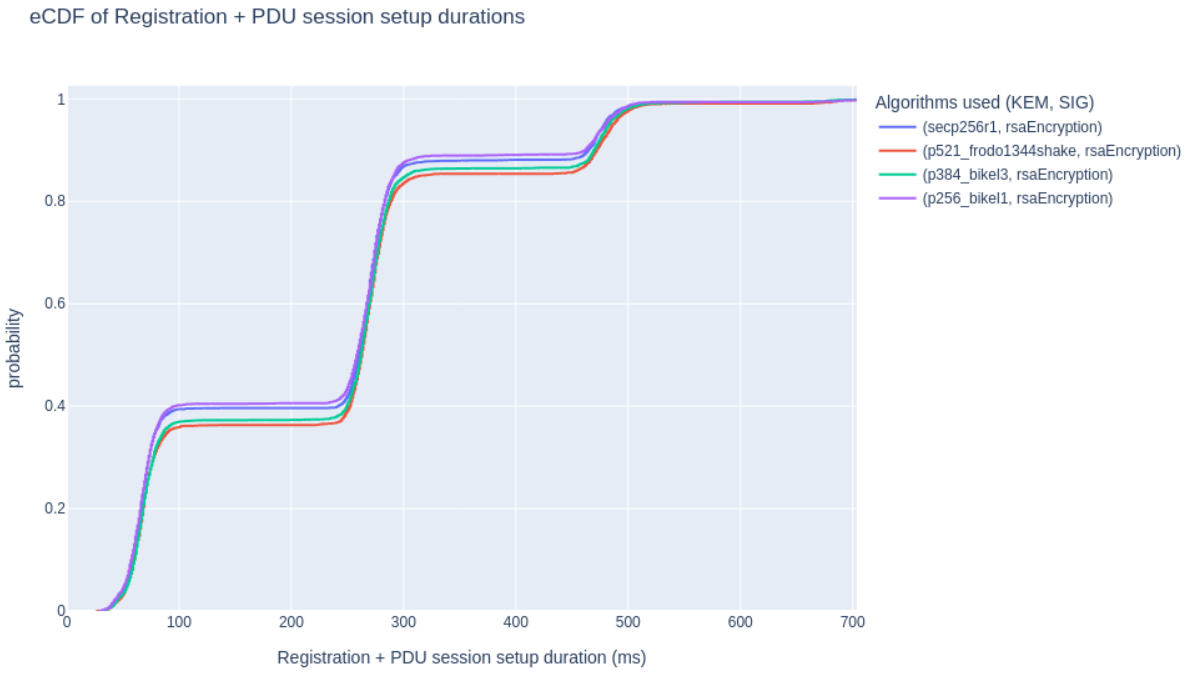

Fig. 4. Histogram showing the setup duration with various KEMs. Remark that `rsaEncryption` refers to the RSA digital signature algorithm.

Fig. 5. Histogram showing the setup duration with various signature algorithms, combined with a conventional (ECC-based) KEM.

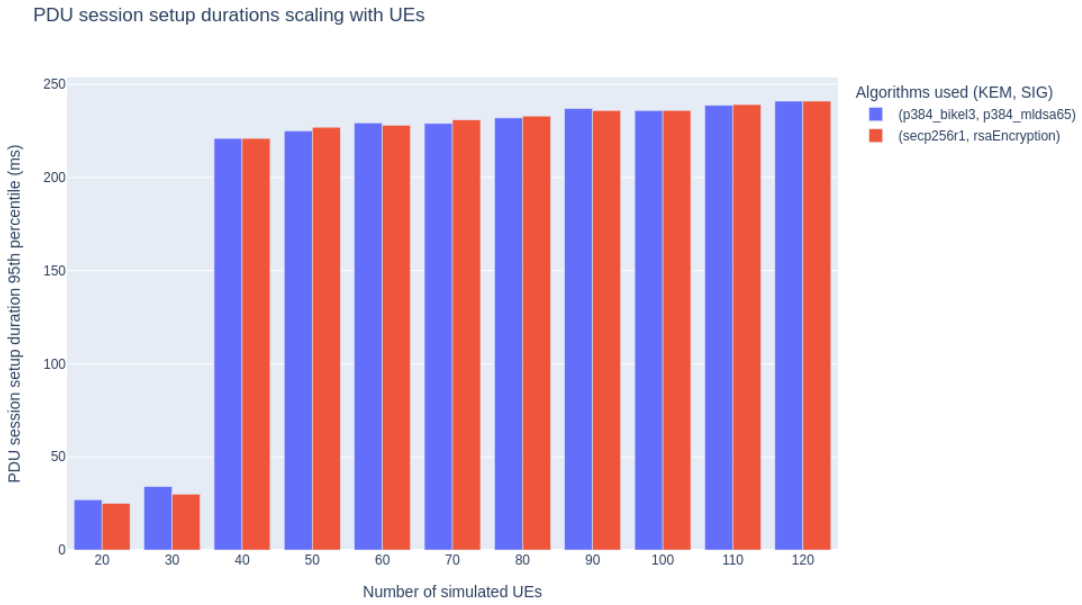

Fig. 6. The duration of the slowest 95th percentile of registrations, for a varying number of UEs.

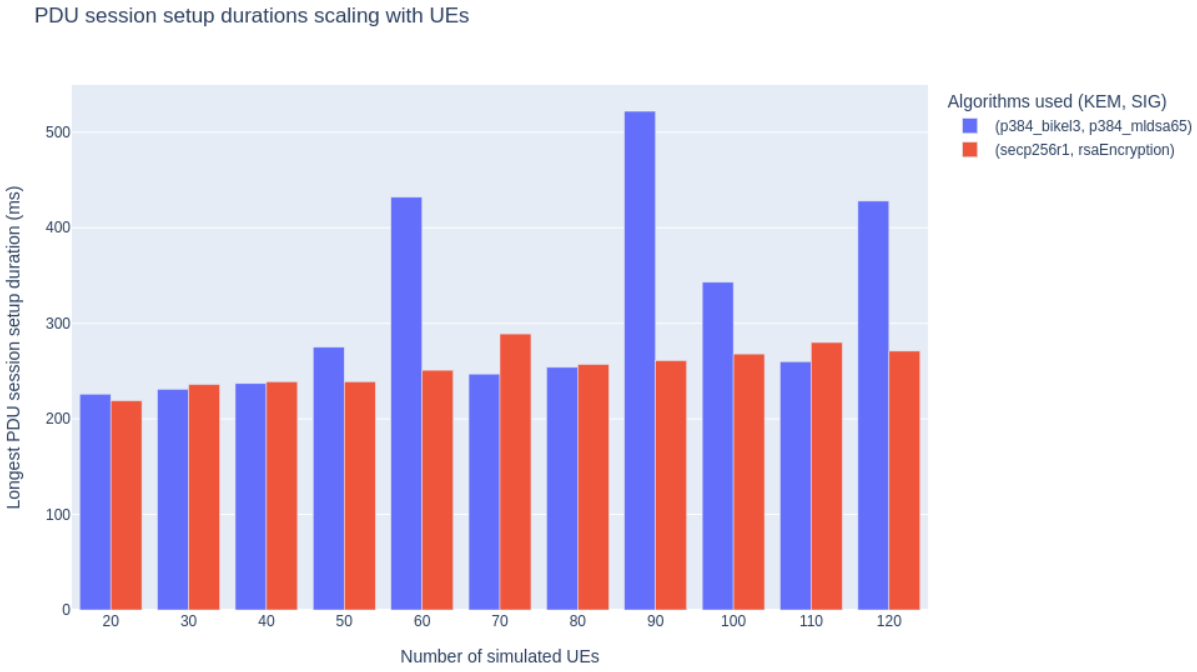

Fig. 7. The duration of the slowest 100th percentile of registrations, for a varying number of UEs.

was split off from the project.[5] This implies getting a `C`-version of KEMTLS working would either requiring manually updating the KEMTLS-fork to be up-to-date with the most recent version of `rustls-ffi` or the other way around — either option is infeasible within the scope of this project.

Another implementation exists in the form of a `botan`-pull request,[6] however there do not seem to be client or server software libraries that use `botan` and that we could easily integrate with the `open5gs` code.[7] We consider experimenting with KEMTLS in the 5G Core an interesting topic for future work.

ACKNOWLEDGMENTS

The research in this work was conducted as part of the CONFIDENTIAL6G project, which has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) as part of the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101096435.

REFERENCES

[1] A. Banerjee, T. Reddy.K, D. Schoinianakis, T. Hollebeek, and M. Ounsworth, "Post-Quantum Cryptography for Engineers," Internet Engineering Task Force, Internet-Draft draft-ietf-pquip-pqc-engineers-09, Feb. 2025, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers/09/

[2] C. Lee, "NIST Special Publication (SP) 1800-38 (Draft), Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography — csrc.nist.gov," https://csrc.nist.gov/pubs/sp/1800/38/iprd-(1), [Accessed April 14, 2025].

[3] E. Commission, "Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography — digital-strategy.ec.europa.eu," https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography, [Accessed April 14, 2025].

[4] B. für Sicherheit in der Informationstechnik, "Quantum Technologies and Quantum-Safe Cryptography — bsi.bund.de," https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-post-quanten-kryptografie_node.html, [Accessed April 7, 2025].

[5] M. Swayne, "UK Sets Timeline, Road Map for Post-Quantum Cryptography Migration — thequantuminsider.com," https://thequantuminsider.com/2025/03/20/uk-sets-timeline-road-map-for-post-quantum-cryptography-migration/, [Accessed April 7, 2025].

[6] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.

[5] As of `rustls-ffi`-commit `58e2b58` (November 20, 2023), the project is no longer compatible with the KEMTLS-fork of `rustls`. Comparing this commit with the current (2025) version of `rustls-ffi`, there have been almost 19 000 updated lines.

[6] See https://github.com/neXenio/botan/pull/20.

[7] See e.g. https://github.com/randombit/botan/issues/1323 for discussion of this issue.

[7] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the Association for Computing Machinery*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[8] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[9] P. Schwabe, "Invited talk: 6 years of NIST PQC – looking back and ahead," https://cryptojedi.org/peter/data/pqcrypto-20220929.pdf, Dec. 2022.

[10] National Institute of Standards and Technology, "Post-Quantum Cryptography, FAQ," https://csrc.nist.gov/projects/post-quantum-cryptography/faqs, accessed: 2025-04-15.

[11] N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, S. Gueron, T. Guneysu, C. Aguilar-Melchor, R. Misoczki, E. Persichetti, N. Sendrier, J.-P. Tillich, G. Zémor, V. Vasseur, S. Ghosh, and J. Richter-Brokmann, "BIKE," National Institute of Standards and Technology, Tech. Rep., 2022, available at https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions.

[12] M. Naehrig, E. Alkim, J. Bos, L. Ducas, K. Easterbrook, B. LaMacchia, P. Longa, I. Mironov, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila, "FrodoKEM," National Institute of Standards and Technology, Tech. Rep., 2020, available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

[13] 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., 2022, available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

[14] A. Hülsing, D. J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L. Gazdag, P. Kampanakis, S. Kölbl, T. Lange, M. M. Lauridsen, F. Mendel, R. Niederhagen, C. Rechberger, J. Rijneveld, P. Schwabe, J.-P. Aumasson, B. Westerbaan, and W. Beullens, "SPHINCS$^+$," National Institute of Standards and Technology, Tech. Rep., 2022, available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

[15] 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., 2022, available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

[16] National Institute of Standards and Technology, "NIST Releases first 3 finalized Post-Quantum encryption standards," https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards, Aug 2024, [Accessed April 7, 2025].

[17] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[18] C. Peikert, "Lattice cryptography for the internet," Cryptology ePrint Archive, Report 2014/070, 2014. [Online]. Available: https://eprint.iacr.org/2014/070

[19] ——, "A decade of lattice cryptography," Cryptology ePrint Archive, Report 2015/939, 2015. [Online]. Available: https://eprint.iacr.org/2015/939

[20] E. Crockett, C. Paquin, and D. Stebila, "Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH," Cryptology ePrint Archive, Report 2019/858, 2019. [Online]. Available: https://eprint.iacr.org/2019/858

[21] D. Connolly, "Hybrid PQ/T Key Encapsulation Mechanisms," Internet Engineering Task Force, Internet-Draft draft-irtf-cfrg-hybrid-kems-03, Feb. 2025, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-cfrg-hybrid-kems/03/

[22] ETSI, "ETSI launches new standard for Quantum-Safe Hybrid Key Exchanges to secure future post-quantum encryption," https:

//www.etsi.org/newsroom/press-releases/2513-etsi-launches-new-standard-for-quantum-safe-hybrid-key-exchanges-to-secure-future-post-quantum-encryption, accessed: 2025-04-15.

[23] D. J. Bernstein, B. B. Brumley, M.-S. Chen, and N. Tuveri, "OpenSSLNTRU: Faster post-quantum TLS key exchange," in *USENIX Security 2022*, K. R. B. Butler and K. Thomas, Eds. USENIX Association, Aug. 2022, pp. 845–862.

[24] P. Schwabe, D. Stebila, and T. Wiggers, "Post-quantum TLS without handshake signatures," in *ACM CCS 2020*, J. Ligatti, X. Ou, J. Katz, and G. Vigna, Eds. ACM Press, Nov. 2020, pp. 1461–1480.

[25] T. Wiggers, "Post-quantum tls," Ph.D. dissertation, Radboud University, Nijmegen, The Netherlands, January 2024. [Online]. Available: https://thomwiggers.nl/publication/thesis/

[26] W. Coomans, D. Schoinianakis, R. Sohn, S. Chenard, A. Banerjee, and M. Charbonneau, "The road to quantum-safe networks," https://www.nokia.com/asset/214685, Nokia Bell Labs, White Paper, April 2025.

[27] T. C. Clancy, R. McGwier, and L. Chen, "Post-quantum cryptography and 5g security: tutorial," *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:160010107

[28] P. Scalise, R. Garcia, M. Boeding, M. Hempel, and H. R. Sharif, "An applied analysis of securing 5g/6g core networks with post-quantum key encapsulation methods," *Electronics*, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:273726082

[29] Y. Hanna, D. Pineda, M. Veksler, M. Paudel, K. Akkaya, M. Anastasova, and R. Azarderakhsh, "Integrating post-quantum tls into the control plane of 5g networks," *2024 IEEE International Performance, Computing, and Communications Conference (IPCCC)*, pp. 1–8, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:275957700

[30] B. Ojetunde, T. Kurihara, K. Yano, T. Sakano, and H. Yokoyama, "A multi-level rule model for selecting post-quantum cryptography in 5g application and beyond," *2024 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–6, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:268046685

[31] D. T. Uysal, P. Yoo, and K. Taha, "Data-driven malware detection for 6g networks: A survey from the perspective of continuous learning and explainability via visualisation," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 61–71, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:253415446

[32] J. Zheng, H. Zhu, Y. Dong, Z. Song, Z. Zhang, Y. Yang, and Y. Zhao, "Faster post-quantum TLS 1.3 based on ML-KEM: Implementation and assessment," in *ESORICS 2024, Part II*, ser. LNCS, J. Garcia-Alfaro, R. Kozik, M. Choraś, and S. Katsikas, Eds., vol. 14983. Springer, Cham, Sep. 2024, pp. 123–143.

[33] M. Sosnowski, F. Wiedner, E. Hauser, L. Steger, D. Schoinianakis, S. Gallenmüller, and G. Carle, "The Performance of Post-Quantum TLS 1.3," in *Companion of the 19th International Conference on Emerging Networking EXperiments and Technologies*. Paris France: ACM, dec 2023, pp. 19–27.

[34] K. Bürstinghaus-Steinbach, C. Krauß, R. Niederhagen, and M. Schneider, "Post-quantum TLS on embedded systems: Integrating and evaluating Kyber and SPHINCS+ with mbed TLS," in *ASIACCS 20*, H.-M. Sun, S.-P. Shieh, G. Gu, and G. Ateniese, Eds. ACM Press, Oct. 2020, pp. 841–852.

[35] G. Tasopoulos, C. Dimopoulos, A. P. Fournaris, R. K. Zhao, A. Sakzad, and R. Steinfeld, "Energy consumption evaluation of post-quantum TLS 1.3 for resource-constrained embedded devices," Cryptology ePrint Archive, Report 2023/506, 2023. [Online]. Available: https://eprint.iacr.org/2023/506

[36] D. Mankowski, T. Wiggers, and V. Moonsamy, "TLS → post-quantum TLS: Inspecting the TLS landscape for PQC adoption on android," Cryptology ePrint Archive, Report 2023/734, 2023. [Online]. Available: https://eprint.iacr.org/2023/734

[37] M. T. Damir and V. Niemi, "On post-quantum identification in 5g," in *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 292–294. [Online]. Available: https://doi.org/10.1145/3507657.3529657

[38] D. Stebila and M. Mosca, "Post-quantum key exchange for the internet and the open quantum safe project," in *International Conference on Selected Areas in Cryptography*. Springer, 2016, pp. 14–37.

[39] A. Güngör, "UERANSIM: Open source 5g ue and ran (gNodeB) implementation," https://github.com/aligungr/UERANSIM.

[40] K. Seo and S. Kent, "Security Architecture for the Internet Protocol," RFC 4301, Dec. 2005. [Online]. Available: https://www.rfc-editor.org/info/rfc4301

[41] G. Wang, "KEM based Authentication for the IKEv2 with Post-quantum Security," Internet Engineering Task Force, Internet-Draft `draft-wang-ipsecme-kem-auth-ikev2-00`, Mar. 2025, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-wang-ipsecme-kem-auth-ikev2/00/

[42] P. Kampanakis and G. Ravago, "Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2)," Internet Engineering Task Force, Internet-Draft `draft-kampanakis-ml-kem-ikev2-09`, Nov. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-kampanakis-ml-kem-ikev2/09/

[43] R. Gonzalez and T. Wiggers, "KEMTLS vs. post-quantum TLS: Performance on embedded systems," Cryptology ePrint Archive, Report 2022/1712, 2022. [Online]. Available: https://eprint.iacr.org/2022/1712