# Theoretical and Practical Aspects in Identifying Gaps and Preparing for Post-Quantum Cryptography

Jörn-Marc Schmidt
*IU International University of Applied Science*
Erfurt, Thüringen, Germany
joern-marc.schmidt@iu.org

Alexander Lawall
*IU International University of Applied Science*
Erfurt, Thüringen, Germany
alexander.lawall@iu.org

***Abstract*—In cryptographic security, quantum computing poses a significant challenge to traditional cryptographic protocols. This study investigates the landscape of Post-Quantum Cryptography (PQC), focusing on the transition from theoretical underpinnings, over standardization efforts to practical implementations. The primary research question that guides this contribution is: What mechanisms can be implemented to safeguard applications? This question is answered by the current state of standards supporting PQC and the ongoing preparation efforts. Thereby, not only the standards for the cryptographic algorithms, but also the protocols relying on them are considered. Furthermore, the status of (open-source) implementations is considered. This study contributes to the ongoing efforts to strengthen cryptographic systems against the challenges posed by quantum computing and provides insights into the available possibilities.**

***Keywords*-Post Quantum Cryptography (PQC); PQC Standards; PQC Implementations.**

## I. Introduction

Quantum computers will influence many fields. They will improve biological and chemical simulations, can be applied for risk modeling, and improve solving of optimization problems. In addition to those constructive improvements, they have the potential to impact the security of cryptographic algorithms. Especially, asymmetric algorithms that rely on the hardness factorization or the discrete logarithm problem cannot be considered secure when a Cryptographic Relevant Quantum Computer (CRQC) is available. Hence, use cases relying on such algorithms will be impacted by CRQCs. Moreover, even data transmitted today can be endangered by attackers recording the transmission and decrypting it as soon as CRQCs are available. This is referred to as harvest now and decrypt later attack.

This challenge, i.e. Post-Quantum (PQ) security, is already picked up by security researchers, developers, several government agencies, and companies. In order to drive the readiness of post-quantum cryptographic algorithms and their adoption in standard applications forward, many activities are underway. They include various working groups, like the Internet Engineering Task Force (IETF) working group *Post-Quantum Use In Protocols* [1], and the European Telecommunications Standards Institute (ETSI) *Quantum-Safe Cryptography (QSC)* working group [2]. Further activities are driven by various companies like Google [3], IBM [4], and Microsoft [5], and Utimaco [6].

This paper provides an overview of those activities. Its scope includes enterprise use cases, not the implementations that are provided to end-users directly. Thereby, its focus is on use cases for asymmetric cryptography due to the expected high impact of CRQC on this type of algorithm. The paper highlights the status of standardization processes and the production-readiness of implementations. As such, it gives guidance on what can be done today to protect applications and data.

The paper is structured as follows. Section II discusses the general preparation process and security protocols. Section III summarizes the status of the standardization of new cryptographic algorithms, while Section IV looks into the status of protocol standards. Libraries that support PQC algorithms, as a foundation for implementations, are presented in Section V. Finally, conclusions are drawn in Section VI.

## II. Building Blocks

The transition to post-quantum cryptography, given the widespread use of the algorithms, is a huge undertaking. As a first step, it is important to understand where susceptible algorithms are employed and how valuable the protected data is. Hence, for a company to prepare, a risk assessment of its application portfolio is required. The first step in such an endeavor is creating a cryptographic inventory, providing insights on where which algorithms, protocols and related parameters are used. Various tools can help creating an inventory [7].

Afterwards, a sound risk model that integrates into the company's risk management procedures is required. For the financial industry, the Financial Services Information Sharing and Analysis Center (FS-ISAC) provides a white paper on modeling the risk [8]. This helps to create a profound strategy and to decide where the highest risks and the biggest benefits are expected. Finally, a maturity index helps judging and comparing where a company is on its journey to post-quantum security [9] [10].

### A. Data Protection

Generally speaking, data requires protection at rest, in transit, and in use.

Data at rest commonly relies on symmetric cryptography, where limited impact of quantum computers is expected. Solutions that employ asymmetric cryptography can make

Copyright (c) IARIA, 2024. ISBN: 978-1-68558-206-7

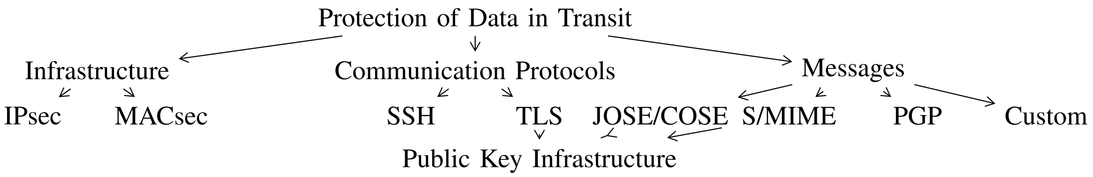

Figure 1. Overview of protocols used in different scenarios to protect data in transit.

use of Key Encapsulation Mechanisms (KEMs) discussed in Section III.

Encryption of data in use is not yet widely used. An available possibility is to rely on processor extensions like Intel Software Guard Extensions (SGX) [11] / Trust Domain Extensions (TDX) [12] or AMD Secure Encrypted Virtualization (SEV) [13]. Especially the attestation, i.e., proving that the protected environment is in a trustworthy state, relies on asymmetric cryptography. Solutions are discussed in [14].

In particular, when focusing on harvest now and decrypt later attack scenarios, security of encryption in transit against attacks with quantum computers is the most pressing scenario. In order to protect data in transit, it is possible to

- protect the underlying infrastructure by ensuring that the communication is PQ-secure. While this has large impact, it is restricted to endpoints that are in direct control; protecting the connections to end-users might not be possible. Commonly, protocols like IPsec and MACsec are employed in such scenarios.
- ensure that the communication protocols are PQ-secure. Common protocols are Transport Layer Security (TLS) and Secure Shell (SSH). Both protocols allow to negotiate the used ciphers with a handshake. This enables using PQC whenever both parties support it without preventing non-PQC-secure communication in case one endpoint is not able to use such a cipher.
- encrypt the transferred message in a quantum-secure way. By using a method that ensures that the data is encapsulated with post-quantum cryptography, a sound protection against adversaries can be achieved. This can be achieved either via standards suitable to the application, like Secure/Multipurpose Internet Mail Extensions (S/MIME) for emails/web-pages, Javascript Object Signing and Encryption (JOSE)/Concise Binary Object Representation (CBOR) Object Signing and Encryption (COSE) for JSON-based messages and Pretty Good Privacy (PGP) for encrypting arbitrary data including files. Another option is to rely on self-defined, custom protocols, e.g. by employing implementations discussed in Section V directly.

The different options that are discussed in the following sections are given in Figure 1.

### *B. Public Key Infrastructure (PKI) and Certificates*

Methods for authentication and ensuring the authenticity of data are required as soon as a CRQC is available. Collecting data today, as in the harvest and decrypt scenario, does not represent a current threat. However, a lack of being ready in time will have devastating consequences as well, as an adversary can impersonate every identity that is not protected and forge any non-PQC signature. A foundation for many protocols and signatures is a valid certificate. Hence, a PQ-secure Public Key Infrastructure (PKI) is required. It can be the foundation for TLS authentication, for re-signing documents, like contracts, and for secure authentication of devices.

## III. The Quest for new Cryptographic Algorithms

The basis of all protocols and building blocks is quantum-secure algorithms. Hence, it is essential to develop and standardize new (asymmetric) cryptographic algorithms to replace the current ones.

A key activity in this regard was launched by National Institute of Standards and Technology (NIST) end of 2016. The NIST issued a call for papers for new post-quantum cryptographic algorithms [15]. Out of 69 initial submissions, three were selected to become Federal Information Processing Standards (FIPS). The following documents have recently (at the time writing this paper) been finalized:

- FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM), based on Cryptographic Suite for Algebraic Lattices (CRYSTALS)-Kyber [16]
- FIPS 204, Module-Lattice-Based Digital Signature Standard (ML-DSA), based on CRYSTALS-Dilithium [17]
- FIPS 205, Stateless Hash-Based Digital Signature Standard (SLH-DSA), based on SPHINCS+ (for practical stateless hash-based signatures) [18]

Moreover, the process is continuing with a fourth round. Remaining candidates are the Key-Encapsulation Mechanisms (KEMs) Bit Flipping Key Encapsulation (BIKE), Classic McEliece, Hamming Quasi-Cyclic (HQC), and Supersingular Isogeny Key Encapsulation (SIKE). As there is no algorithm for digital signatures left from the initial submissions, NIST launched another Call-for-Proposals on *Post-Quantum Cryptography: Digital Signature Schemes*, which is currently in the first round. Hence, despite there are NIST standards already finalized, further algorithms are under consideration.

Naturally, the NIST process and its contributions from researchers all over the world are closely followed by government agencies from other nations.

The British National Cyber Security Center (NCSC) published a white paper recommending the use of the NIST standards or the hash-based signatures Leighton-Micali Hash-Based Signatures (LMS) or eXtended Merkle Signature Scheme (XMSS) [19].

In terms of post-quantum algorithms, the German Bundesamt für Sicherheit in der Informationstechnik (BSI) recommends in its technical policy TR-02102-1 Version 2024-01 using FrodoKEM or Classic McElice as a post-quantum cryptographic algorithm for encryption/key-agreement [20]. It recommends FrodoKEM as a more conservative choice compared to the ML-KEM that is standardized by NIST. While FrodoKEM is not planned to be part of a NIST standard, its specification was submitted to International Organization for Standardization (ISO) for standardization [21]. However, the policy states that ML-KEM will be included in a future version based on the publication of the related NIST standard.

For digital signatures, the policy recommends (among non-PQC-algorithms) Merkle-Signatures, in detail XMSS or LMS, including Multi-Tree-Variants as described in [22]. In addition, it mentions the intent to include SLH-DSA (SPHINCS+) and ML-DSA (CRYSTALS-Dilithium) in future versions.

In general, the policy recommends combining a PQC approach and a classical one. The combination needs to ensure to stay secure, as long as one of the used schemes is secure. Hash-based signatures are an exception in case they are properly implemented, i.e., the do not require a hybrid approach.

In contrast to the German BSI, the French Cybersecurity Agency (ANSSI) states in their PQC position paper, that the *ANSSI traditionally does not provide any closed list of recommended algorithms in order to avoid proscribing innovative state-of-the-art algorithms that could be well-suited for some particular use cases* [23]. However, a list of post-quantum algorithms together with recommendations is given. For KEM, they include ML-KEM and FrodoKEM. The list of digital signature algorithms contains ML-DSA, Falcon (FN-DSA), XMSS/LMS and SLH-DSA. In terms of combining PQC and classical algorithms, the ANSSI states their alignment with the position of the BSI recommending a hybrid approach.

Overall, the process of standardization results in the publication of various recommendations and draft standards. The analysis, including research on secure implementations, is still ongoing, leading to new attacks, cf. [24]. While the NIST is driving the most prominent competition, the government bodies of UK, Germany, and France are basically in line with the recommendations and have not announced any plans for running another competition.

Concluding, the current state, especially in a hybrid setting with a classic algorithm, provides a solid foundation for building and implementing protocols and further post-quantum secure solutions.

## IV. Protocols

In addition to developing and standardizing quantum-secure algorithms, protocol standards need to be adopted.

### A. Infrastructure

Common communication protocols to connect hosts to networks in a secure fashion or to establish a secure connection between networks are MACsec [25] and IPsec [26].

*1) MACsec:* As MACsec relies only on symmetric algorithms during the key agreement, using a 256-bit key is sufficient for post-quantum security. In addition, it is important to ensure that the key distribution is quantum-secure. Especially, since the session keys do not provide forward secrecy, i.e., a compromise of the long-term key material affects past session keys [27].

*2) IPsec:* For IPsec, Request For Comments (RFC) 8784 [28] defines a method to use pre-shared keys to achieve post-quantum security. This provides a viable solution already today. Potential adoptions of PQC for the Internet Key Exchange Protocol Version 2 (IKEv2) are in draft status. For example, the document specifying a Hybrid Key Exchange with ML-KEM [29] is currently an individual submission without IETF endorsement.

### B. Communication Protocols

Common communication protocols include Transport Layer Security (TLS) and Secure Shell (SSH).

*1) Transport Layer Security (TLS):* The Transport Layer Security (TLS) protocol allows a secure end-to-end connection between applications. Various research has been conducted on how to best integrate post-quantum cryptography in the protocol and related performance, e.g., [30] [31].

All this research focuses on the actual TLS 1.3 version. For TLS 1.3, a draft specifies a hybrid use of algorithms [32]. This ensures that the connections remain secure even if used algorithms are broken. An experimental implementation of this draft is available in the Botan library [33] since version 3.2. Another implementation of the draft is provided by the Open Quantum Safe project [34] in the form of an OpenSSLv3 provider and an integration into a BoringSSL fork. However, those two implementations should not be considered *production quality* according to the project.

Note that a recent IETF draft states that TLS 1.2 will not be further enhanced, which implies, it will not support PQC, despite TLS 1.2 is still widespread [35].

Further experiments on challenges when using PQC-TLS at a large scale were conducted by Google [3]. Their tests revealed incompatibilities in network products that will be fixed via firmware updates. Similar PQC-support is enabled by Cloudflare [36], targeting support of all outbound connections by March 2024. This can be used with browsers supporting the hybrid cipher suite consisting of X25519 and Kyber-768, like Chrome, where it has been enabled since version 116 [37].

Hence, a draft standard and first implementations are available, and some widespread experiments have been conducted successfully. Stable and standardized support of PQC for TLS 1.3 is expected to build on the released NIST standards.

*2) Secure Shell (SSH):* Secure Shell (SSH) is a protocol for secure execution of remote commands. A very prominent implementation is OpenSSH, which is part of many major Linux distributions. OpenSSH made a hybrid key exchange method that combines Number Theory Research Unit (NTRU)-Prime with an Elliptic-curve Diffie–Hellman (ECDH) key exchange default in version 9.0/9.0p1 [38]. However, this implementation relies on an individual IETF draft submission that has already expired [39]. Other, at the time of writing, active drafts of individual IETF submissions are [40] and [41]. The ladder one is implemented and used by Amazon Web Services (AWS) [42]. The Open Quantum Safe project [34] also provides an implementation of this draft, but it is currently inactive.

Overall, with OpenSSL, that uses a hybrid approach per default, and the AWS implementation, there are real-world possibilities for PQC key-agreement, despite there being no final standard yet.

### C. Message Security

On the message layer, the application can choose to encrypt/sign the transferred data, depending on the use case. Potential solutions include JOSE/COSE for sharing data between applications, S/MIME for mail/web pages and PGP for arbitrary data, including file exchange.

*1) JOSE/COSE:* JSON and CBOR are formats for data exchange between applications. The related signing and encryption standards are JOSE and COSE. For COSE, hash-based signatures are defined in RFC 8778 [43]. Active IETF drafts exist to support Dilithium [44] and SPHINCS+ signatures [45]. In addition to those working group drafts, other individual drafts have been submitted to the IETF as well.

*2) S/MIME:* The S/MIME standard [46] mandates the support of RSA-based and EC-based ciphers for signing and encryption. Preparing the standard for the quantum-age is part of the *Limited Additional Mechanisms for PKIX and SMIME (lamps)* working group charta [47]. Nevertheless, the possibility of integrating PQC-ciphers into the mail client Thunderbird is briefly discussed in [48], and a demo integration was done by the MTG AG [49].

*3) PGP:* The options for using post-quantum ciphers in PGP were analyzed by Wussler [50], leading to an IETF draft [51]. A former version of this draft was formally analyzed by Tran et al. [52].

While there is work underway for all three standards, there is still a lack of practical implementations and experiments that will lead to solutions that can be used in production environments.

### D. Public Key Infrastructures (PKIs) and Certificates

Public Key Infrastructures (PKIs) are essential for ensuring trust in the digital world. Ranging from communication protocols to digitally signed documents - a reliable PKI is required to ensure the identity of the counterpart. For trustworthy certificates in the presence of quantum computers, the whole chain, starting from the root certificate must be quantum-secure.

The draft [53] defines a composite certificate combining ML-DSA with traditional signature algorithms. This solution ensures that the certificate remains secure even in case one of the algorithms is broken. A similar approach is used for KEM solutions [54] in the context of PKI-related profiles and protocols like Cryptographic Message Syntax (CMS) [55] and Public Key Infrastructure for X.509 (PKIX).

Various drafts are already published to be ready to proceed now the NIST standards are finalized. They include certificates using stateless hash-based digital signatures [56], Kyber [57], and Dilithium [58].

During the transition phase, it is important that also legacy systems that might not support post-quantum cryptography can verify a certificate with classic algorithms. The specifications above cannot be used in such a scenario, as they require the verifying system process PQC signatures. A possible approach in the transition scenario is using related certificates, as laid out in the draft specifications [59] and [60]. The impact of hybrid certificates on current implementations was investigated in [61]. The authors concluded the certificates can be processed by the tested solutions without or with minor modifications.

Another option is specified in by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) [62], namely to include an alternative signature in a certificate. This allows clients that are not capable of processing PQC algorithm to ignore this signature, while others can benefit from it. However, the drawback of this approach is the increased certificate size for all consuming entities.

When it comes to commercial products, PKI solution vendors are working towards addressing the upcoming challenges, preparing examples [63], offering experimental suites [6], [64] or solutions [65].

Despite various activities that are underway, neither the majority of the standardization work nor the related implementations have been concluded yet. As especially the root certificates are commonly valid for several years, it is important to plan their replacement together with a sound transition approach.

## V. Foundations and Libraries

Together with research and standardization of PQC algorithms, their implementation is progressing. A popular project to support *the transition to quantum-resistant cryptography* is Open Quantum Safe [34]. It is part of the Linux Foundation's Post-Quantum Cryptography Alliance. Its main working items are a C library for post-quantum algorithms, called liboqs, and prototype integration into protocols and applications. Currently, liboqs supports Kyber, Dilithum, Falcon and SPHINCS+ algorithms selected by NIST, the round 4 candidates Classic McEliece, BIKE and HQC, as well as, FrodoKEM and NTRU-Prime. The project provides several language wrappers to allow using it for example in C++, JAVA, Go, and Python. However, the project page does recommend refraining from using the library in production environments, as it has not undergone a thorough audit/analysis process yet.

Another popular library that provides PQC support is Bouncy Castle for Java and C# [66]. Its implementation includes all algorithms supported by liboqs, plus the NIST round 3 candidates Saber, NTRU, Picnic, Rainbow and Great Multivariate Short Signature (GeMSS). The project states that those algorithms can be used for experiments as they are still subject to change and that the provided KEM algorithms are suited for short-term protection in a hybrid setting, not for long-term protection.

Overall, there are two aspects to consider about using PQC algorithms today: (1) First standards have recently been finalized and the security research is ongoing. They also do not have the benefit of a long history of intensive security research that current standards possess. Therefore, the Bouncy Castle team, in line with the BSI, recommends using the current PQC algorithms in a hybrid mode. (2) In addition to the security of the algorithms, quality [67] and security of its implementations are important. This includes sufficient quality assurance and auditing to prevent vulnerabilities and security bugs as well as resistance against potential side-channel attacks like [68]–[70].

## VI. Conclusions and Recommendations

Quantum computers endanger the security cryptographic algorithms. Especially asymmetric algorithms are affected. This requires new algorithms as well as updated standards to make use of those new algorithms. Various efforts from research over standardization to implementation are currently under way to address this challenge. This paper started by looking at possibilities to secure the underlying network infrastructure. As IPsec and MACsec can rely on secret-key cryptography, the remaining challenge is secure key management.

In order to achieve end-to-end security, SSH can be used with post-quantum security, e.g., via OpenSSH, whereas TLS implementations are still in an experimental state. Standards for message encryption are still at a comparably early stage. However, libraries, especially BouncyCastle for JAVA and C#, provide algorithms that can already integrated into applications; given the required expert knowledge is available.

Overall, the transition will require thorough planning. This paper highlighted where first steps can be done already today. Depending on the use case, hybrid approaches can protect against quantum attacks while preventing risks due to attacks on comparably new PQC algorithms. Furthermore, becoming crypto-agile, in the sense that algorithms can be exchanged easily, will not only help in addressing the current PQC challenge, but also reduce the effort of future transitions of cryptographic algorithms.

## References

[1] "Post-Quantum Use In Protocols (pquip)," retrieved: September, 2024. [Online]. Available: https://datatracker.ietf.org/wg/pquip/about/

[2] "Quantum-Safe Cryptography (QSC)," retrieved: September, 2024. [Online]. Available: https://www.etsi.org/technologies/quantum-safe-cryptography

[3] Googe, "How Google is preparing for a post-quantum world, note = retrieved: September, 2024." [Online]. Available: https://cloud.google.com/blog/products/identity-security/how-google-is-preparing-for-a-post-quantum-world

[4] IBM, "Make the world quantum safe," retrieved: September, 2024. [Online]. Available: title={https://www.ibm.com/quantum/quantum-safe},

[5] Microsoft, "Post-quantum cryptography," retrieved: September, 2024. [Online]. Available: https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/

[6] Utimaco, "Post Quantum Cryptography," retrieved: September, 2024. [Online]. Available: https://utimaco.com/solutions/applications/post-quantum-cryptography

[7] ETSI, "ETSI TR 103 619 V1.1.1 (2020-07) - CYBER; Migration strategies and recommendations to Quantum Safe schemes ." [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

[8] Post-Quantum Cryptography (PQC) Working Group, "Risk model technical paper," FS-ISAC, Tech. Rep., 2023, retrieved: September, 2024. [Online]. Available: https://www.fsisac.com/hubfs/Knowledge/PQC/RiskModel.pdf

[9] T. Patterson, "Moving toward a Quantum Security Maturity Index," retrieved: September, 2024. [Online]. Available: https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_tom-patterson_accenture_moving-toward-a-quantum-security-maturity-index.pdf

[10] DigiCert, "Post-Quantum Cryptography (PQC) Maturity Model," retrieved: September, 2024. [Online]. Available: https://www.digicert.com/resources/post-quantum-cryptography-maturity-model.pdf

[11] Intel, "Intel® Software Guard Extensions (Intel®SGX)," retrieved: September, 2024. [Online]. Available: https://www.intel.de/content/www/de/de/products/docs/accelerator-engines/software-guard-extensions.html

[12] ——, "Intel® Trust Domain Extensions (Intel® TDX)," retrieved: September, 2024. [Online]. Available: https://www.intel.com/content/www/us/en/developer/tools/trust-domain-extensions/overview.html

[13] AMD, "AMD Secure Encrypted Virtualization (SEV)," retrieved: September, 2024. [Online]. Available: https://www.amd.com/de/developer/sev.html

[14] G. Caruso, "Post-quantum algorithms support in Trusted Execution Environment," Ph.D. dissertation, Politecnico di Torino, 2024.

[15] NIST, "NIST CFP," retrieved: September, 2024. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Call-for-Proposals

[16] N. I. of Standards and Technology, "Module-lattice-based key-encapsulation mechanism standard," U.S. Department of Commerce, Washington, D.C., Tech. Rep. Federal Information Processing Standards Publication (FIPS) 203, 2024.

[17] ——, "Module-lattice-based digital signature standard," U.S. Department of Commerce, Washington, D.C., Tech. Rep. Federal Information Processing Standards Publication (FIPS) 204, 2024.

[18] ——, "Stateless hash-based digital signature standard," U.S. Department of Commerce, Washington, D.C., Tech. Rep. Federal Information Processing Standards Publication (FIPS) 205, 2024.

[19] National Cyber Security Center, "Next steps in preparing for post-quantum cryptography," 2023-11-039 2023. [Online]. Available: https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography

[20] Federal Office for Information Security, "Kryptographische Verfahren: Empfehlungen und Schlüssellängen," Bonn, Deutschland, 2024. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf

[21] E. Alkim et al., "FrodoKEM - Practical quantum-secure key encapsulation from generic lattices." [Online]. Available: https://frodokem.org/

[22] D. Cooper, D. Apon, Q. Dang, M. Davidson, M. Dworkin, and C. Miller, "Recommendation for Stateful Hash-Based Signature Schemes," 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf

[23] ANSSI, "ANSSI views on the Post-Quantum Cryptography transition (2023 follow up)," 2023. [Online]. Available: https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf

[24] P. Ravi, D. Jap, S. Bhasin, and A. Chattopadhyay, "Machine Learning based Blind Side-Channel Attacks on PQC-based KEMs - A Case Study of Kyber KEM," Cryptology ePrint Archive, Paper 2024/169, 2024, https://eprint.iacr.org/2024/169. [Online]. Available: https://eprint.iacr.org/2024/169

[25] M. Seaman, "IEEE Standard for Local and metropolitan area networks–Media Access Control (MAC) Security." [Online]. Available: https://1.ieee802.org/security/802-1ae/

[26] S. Frankel and S. Krishnan, “IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap,” RFC 6071, Feb. 2011. [Online]. Available: https://www.rfc-editor.org/info/rfc6071

[27] ETSI, “ETSI TR 103 617 V1.1.1 (2018-09) - Quantum-Safe Virtual Private Networks.” [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103600_103699/103617/01.01.01_60/tr_103617v010101p.pdf

[28] S. Fluhrer, P. Kampanakis, D. McGrew, and V. Smyslov, “Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security,” RFC 8784, Jun. 2020. [Online]. Available: https://www.rfc-editor.org/info/rfc8784

[29] 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-ikev2-03, Mar. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-kampanakis-ml-kem-ikev2/03/

[30] J. I. E. Pablos, M. E. Marriaga, and A. P. d. Pozo, “Design and Implementation of a Post-Quantum Group Authenticated Key Exchange Protocol With the LibOQS Library: A Comparative Performance Analysis From Classic McEliece, Kyber, NTRU, and Saber,” *IEEE Access*, vol. 10, pp. 120 951–120 983, 2022.

[31] J. Henrich, A. Heinemann, A. Wiesmaier, and N. Schmitt, “Performance Impact of PQC KEMs on TLS 1.3 Under Varying Network Characteristics,” in *Information Security*, E. Athanasopoulos and B. Mennink, Eds. Cham: Springer Nature Switzerland, 2023, pp. 267–287.

[32] D. Stebila, S. Fluhrer, and S. Gueron, “Hybrid key exchange in TLS 1.3,” Internet Engineering Task Force, Internet-Draft draft-ietf-tls-hybrid-design-10, Apr. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/10/

[33] Botan, “Botan - Release Notes,” retrieved: September, 2024. [Online]. Available: https://botan.randombit.net/news.html#version-3-2-0-2023-10-09

[34] “Open Quantum Safe Project,” retrieved: September, 2024. [Online]. Available: https://openquantumsafe.org/

[35] R. Salz and N. Aviram, “TLS 1.2 is in Feature Freeze,” Internet Engineering Task Force, Internet-Draft draft-ietf-tls-tls12-frozen-00, Apr. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-tls12-frozen/00/

[36] W. Evans, B. Westerbaan, C. Patton, P. Wu, and V. Gonçalves, “Post-quantum cryptography goes GA,” retrieved: September, 2024. [Online]. Available: https://blog.cloudflare.com/post-quantum-cryptography-ga/

[37] D. O’Brien, “Protecting Chrome Traffic with Hybrid Kyber KEM,” retrieved: September, 2024. [Online]. Available: https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html

[38] OpenSSH, “Openssh 9.0 release notes,” retrieved: September, 2024. [Online]. Available: https://www.openssh.com/txt/release-9.0

[39] M. Friedl, J. Mojzis, and S. Josefsson, “Secure Shell (SSH) Key Exchange Method Using Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512: sntrup761x25519-sha512,” Internet Engineering Task Force, Internet-Draft draft-josefsson-ntruprime-ssh-02, Sep. 2023, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-josefsson-ntruprime-ssh/02/

[40] S. Josefsson, “Secure Shell Key Exchange Method Using Hybrid Classic McEliece and X25519 with SHA-512: mceliece6688128x25519-sha512,” Internet Engineering Task Force, Internet-Draft draft-josefsson-ssh-mceliece-00, Dec. 2023, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-josefsson-ssh-mceliece/00/

[41] P. Kampanakis, D. Stebila, and T. Hansen, “PQ/T Hybrid Key Exchange in SSH,” Internet Engineering Task Force, Internet-Draft draft-kampanakis-curdle-ssh-pq-ke-02, May 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-kampanakis-curdle-ssh-pq-ke/02/

[42] AWS Security Blog, “Post-quantum hybrid SFTP file transfers using AWS Transfer Family,” retrieved: September, 2024. [Online]. Available: https://aws.amazon.com/de/blogs/security/post-quantum-hybrid-sftp-file-transfers-using-aws-transfer-family

[43] R. Housley, “Use of the HSS/LMS Hash-Based Signature Algorithm with CBOR Object Signing and Encryption (COSE),” RFC 8778, Apr. 2020. [Online]. Available: https://www.rfc-editor.org/info/rfc8778

[44] M. Prorock, O. Steele, R. Misoczki, M. Osborne, and C. Cloostermans, “ML-DSA for JOSE and COSE,” Internet Engineering Task Force, Internet-Draft draft-ietf-cose-dilithium-03, Jun. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-cose-dilithium/03/

[45] ——, “SLH-DSA for JOSE and COSE,” Internet Engineering Task Force, Internet-Draft draft-ietf-cose-sphincs-plus-02, Jan. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-cose-sphincs-plus/02/

[46] J. Schaad, B. C. Ramsdell, and S. Turner, “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification,” RFC 8551, Apr. 2019. [Online]. Available: https://www.rfc-editor.org/info/rfc8551

[47] R. Housley and T. Hollebeek, “Limited Additional Mechanisms for PKIX and SMIME (lamps).” [Online]. Available: https://datatracker.ietf.org/wg/lamps/about/

[48] C. Döberl et al., “Quantum-resistant End-to-End Secure Messaging and Email Communication,” in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ser. ARES ’23. New York, NY, USA: Association for Computing Machinery, 2023, pp. 1–8. [Online]. Available: https://doi.org/10.1145/3600160.3605049

[49] MTG AG, “PQC Anwendungen jetzt testen!” retrieved: September, 2024. [Online]. Available: https://www.mtg.de/de/post-quantum-kryptografie/pqc-demo/#PQC_Testanwendungen

[50] A. Wussler, “Post-Quantum cryptography in OpenPGP,” Master’s thesis, Wien, 2023.

[51] S. Kousidis, J. Roth, F. Strenzke, and A. Wussler, “Post-Quantum Cryptography in OpenPGP,” Internet Engineering Task Force, Internet-Draft draft-ietf-openpgp-pqc-03, May 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-openpgp-pqc/03/

[52] D. D. Tran, K. Ogata, and S. Escobar, “A formal analysis of OpenPGP’s post-quantum public-key algorithm extension,” in *Proceedings of the 2nd International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols (FAVPQC), 2023*. Brisbane, Australia: JAIST Press, 2023, pp. 22–35.

[53] M. Ounsworth, J. Gray, M. Pala, J. Klaußner, and S. Fluhrer, “Composite ML-DSA for use in Internet PKI,” Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-pq-composite-sigs-01, Jun. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/01/

[54] ——, “Composite ML-KEM for Use in the Internet X.509 Public Key Infrastructure and CMS,” Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-pq-composite-kem-03, Mar. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-kem/03/

[55] R. Housley, J. Gray, and T. Okubo, “Using Key Encapsulation Mechanism (KEM) Algorithms in the Cryptographic Message Syntax (CMS),” Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-cms-kemri-08, Feb. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-cms-kemri/08/

[56] K. Bashiri, S. Fluhrer, S.-L. Gazdag, D. V. Geest, and S. Kousidis, “Internet X.509 Public Key Infrastructure: Algorithm Identifiers for HSS and XMSS,” Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-x509-shbs-01, Jun. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-x509-shbs/01/

[57] S. Turner, P. Kampanakis, J. Massimo, and B. Westerbaan, “Internet X.509 Public Key Infrastructure - Algorithm Identifiers for Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM),” Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-kyber-certificates-03, Mar. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-kyber-certificates/03/

[58] J. Massimo, P. Kampanakis, S. Turner, and B. Westerbaan, “Internet X.509 Public Key Infrastructure: Algorithm Identifiers for ML-DSA,” Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-dilithium-certificates-03, Feb. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-dilithium-certificates/03/

[59] A. Becker, R. Guthrie, and M. J. Jenkins, “Related Certificates for Use in Multiple Authentications within a Protocol,” Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-cert-binding-for-multi-auth-05, Apr. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-cert-binding-for-multi-auth/05/

[60] C. Bonnell, J. Gray, D. Hook, T. Okubo, and M. Ounsworth, “A Mechanism for Encoding Differences in Paired Certificates,” Internet Engineering Task Force, Internet-Draft draft-bonnell-lamps-chameleon-certs-03, Jan. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-bonnell-lamps-chameleon-certs/03/

[61] J. Fan et al., “Impact of post-quantum hybrid certificates on PKI, common libraries, and protocols,” *International Journal of Security*

*and Networks*, vol. 16, no. 3, pp. 200–211, 2021. [Online]. Available: https://www.inderscienceonline.com/doi/abs/10.1504/IJSN.2021.117887

[62] Telecommunication Statdardization Sector of ITU, “Directory Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks,” Oct. 2019.

[63] GlobalSign, “Post Quantum Computing - Future-proofing digital trust with safe certificates,” retrieved: September, 2024. [Online]. Available: https://www.globalsign.com/en/post-quantum-computing

[64] Keyfactor, “Post-Quantum Cryptography Keys and Signatures,” retrieved: September, 2024. [Online]. Available: https://doc.primekey.com/ejbca/ejbca-operations/ejbca-ca-concept-guide/certificate-authority-overview/post-quantum-cryptography-keys-and-signatures

[65] Entrust, “Post-Quantum Cryptography,” retrieved: September, 2024. [Online]. Available: https://www.entrust.com/solutions/post-quantum-cryptography

[66] “Bouncy Castle,” retrieved: September, 2024. [Online]. Available: https://www.bouncycastle.org/

[67] M. J. Kannwischer, P. Schwabe, D. Stebila, and T. Wiggers, “Improving software quality in cryptography standardization projects,” in *IEEE European Symposium on Security and Privacy, EuroS&P 2022 - Workshops, Genoa, Italy, June 6-10, 2022*. Los Alamitos, CA, USA: IEEE Computer Society, 2022, pp. 19–30.

[68] P. Ravi, A. Chattopadhyay, J. P. D’Anvers, and A. Baksi, “Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results,” *ACM Trans. Embed. Comput. Syst.*, vol. 23, no. 2, pp. 1–54, mar 2024. [Online]. Available: https://doi.org/10.1145/3603170

[69] C. Mujdei et al., “Side-channel Analysis of Lattice-based Post-quantum Cryptography: Exploiting Polynomial Multiplication,” *ACM Trans. Embed. Comput. Syst.*, vol. 23, no. 2, pp. 1–23, mar 2024. [Online]. Available: https://doi.org/10.1145/3569420

[70] A. T. Hoang et al., “Deep Learning Enhanced Side Channel Analysis on CRYSTALS-Kyber,” in *2024 25th International Symposium on Quality Electronic Design (ISQED)*, 2024, pp. 1–8.

Copyright (c) IARIA, 2024. ISBN: 978-1-68558-206-7