Gesellschaft für Informatik e.V. (GI) GI. (Hrsg.): INFORMATIK 2021,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2021

On the State of Post-Quantum Cryptography Migration

Nouri Alnahawi[1], Alexander Wiesmaier[1], Tobias Grasmeyer[1], Julian Geißler[1], Alexander Zeier[2], Pia Bauspieß[1], Andreas Heinemann[1]

Abstract: Safeguarding current and future IT security from quantum computers implies more than the mere development of Post-Quantum Cryptography (PQC) algorithms. Much work in this respect is currently being conducted, making it hard to keep track of the many individual challenges and respective solutions so far identified. In consequence, it is difficult to judge, whether all (known) challenges have been sufficiently addressed, and whether suitable solutions have been provided. We present results of a literature survey and discuss discovered challenges and solutions categorized into different areas and utilize our findings to evaluate the state of readiness for a full scale PQC migration. We use our findings as starting point to initiate an open community project in the form of a website[3] to keep track of the ongoing efforts and the state of the art in PQC research. Thereby, we offer a single entry-point for the community into the subject reflecting the current state in a timely manner.

Keywords: system security; network security; post-quantum cryptography; integration; migration

1 Introduction and Related Work

Most cryptographic algorithms currently used are subject to security decay over time. This risk has become significantly greater in the light of the expected rise of quantum computers, as established asymmetric schemes like Rivest–Shamir–Adleman (RSA), Digital Signature Algorithm (DSA), and Elliptic-Curve Diffie–Hellman (ECDH) will be broken [Gr96; Sh97]. To maintain security against future and unknown threats, a migration from widely used and established cryptographic standards in IT-systems and infrastructures towards quantum-secure cryptographic schemes must be prepared and executed as soon as possible. This task involves many aspects that need to be taken into consideration and is a transition that has to occur on numerous levels. It is thus more than a simple exchange or replacement of a cryptographic scheme or system [Mo15; OP19]. In this paper we highlight all aspects of the current state of PQC in practice and discuss the main challenges regarding its integration and migration. We focus on research efforts and open questions around PQC development, integration, and adaptation to provide an overview of challenges already solved, challenges currently investigated, challenges recognized yet still unsolved, as well as current blind spots. Through a systematic literature review, using references quoted in [OP19] as a starting point for a keyword-based search, followed by classification and forward/backward citation chasing, we were able to extend and refine the categorization scheme by [OP19] and include

[1] Darmstadt University of Applied Sciences; first.last@h-da.de

[2] MTG AG; azeier@mtg.de

[3] `https://fbi.h-da.de/cma`, last accessed 2021-07-30

the respective state of the art. The adapted categorization scheme is presented in Fig. 1 and is also reflected in the structure of this paper. The corresponding overview in Table 1 highlights the current state and provides brief commentary on the major challenges and breakthroughs respectively. Thus, we present a comprehensive literature survey of relevant papers and the current state of research and readiness. Based on this, we discuss our findings, draw our conclusions and derive future work. As this can only be a snapshot of the current state, we initiated a website (`https://fbi.h-da.de/cma`) that we keep updating and invite the community to support us in keeping track of the current state over time.

Ott et al. [OP19] point out various contexts in which the migration towards PQC will take place and refer to many known requirements and challenges, as well as possible scenarios and contexts of the migration process on a higher level of abstraction. Campagna et al. [Ca15] provide recommendations on how to make common security standards quantum-secure, such as Transport Layer Security (TLS), Internet Key Exchange Protocol Version 2 (IKEv2), Secure/Multipurpose internet Mail Extensions (S/MIME), Secure Shell (SSH), and X.509. Furthermore, they describe important use cases for cryptography and potential migration strategies to transition to PQC. To implement PQC in practical applications, [NW17] name twelve challenges that need to be solved, including migration (hybrid approaches) and agility (agile protocols and update mechanisms). The challenges faced by the industry in the PQC transition process are discussed in [KNW18], and seven recommendations for next generation cryptography are offered. Armknecht et al. [Ar19] discuss a variety of problems in regard to achieving IT security and possible strategies to solve these. Aspects addressed include attacker models, TLS implementations and certificates. A survey of future challenges for PQC in the internet of things (IoT) is provided in [Fe20], as well as an extensive comparison of the performance of PQC algorithms and useful guidelines for post-quantum (PQ) blockchain security [FF20]. Barker et al. [BPS20] present PQC adoption challenges and thoughts on migrating to PQC after the standardization process of the NIST is concluded. Examples are a migration playbook and a way to get an inventory of used cryptography in an IT-system or infrastructure. Recommendations for action on migration to PQC are given in [BS20b], encouraging the use of crypto-agile hybrid solutions and the corresponding adaptation of cryptographic protocols. Following on the same footsteps with similar recommendations, [He21b; HKW21] offer a brief evaluation of the current state of both PQ and quantum cryptography and highlight the chances and limitations of quantum cryptography. A technical report by ETSI [ET20] provides strategies and recommendations for quantum-safe schemes defining a staged approach for a successful migration.

2 Towards New Standards

The focus of the standardization efforts towards PQC lies within developing new cryptographic primitives and algorithms, as these are considered the cornerstone of cryptographic systems. Nonetheless, efforts have been made in scheme integration, as well as in Requests for Comments (RFC).

NIST Candidate Algorithms PQC algorithms are based on mathematical problems that cannot be efficiently solved by quantum or classical computers [Be09]. These fall mainly into five categories [GAB19; NW17; OP19]: Multivariate (quadratic polynomial equation), lattice-based (a grid as a discrete subset of an n-dimensional real vector space), code-based (the problem of decoding general error correcting codes), isogeny-based (algebraic geometry), and hash-based.

The state of PQC standardization is represented by the respective ongoing NIST process [NI16]. It was initiated in 2016 [Ch16] with 82 algorithm submissions, from which 69 candidates were accepted into the project, and out of these, 26 advanced to the second round [Al19]. Round three was announced with 15 finalists [Mo20]. Including the alternatives, these are nine public-key encryption and key-establishment algorithms, and six digital signatures. Following the third NIST PQC conference, it is planned to release draft standards between 2022 and 2023, and hopefully finalize the process by 2024. An overview of all algorithm candidates is provided in Table 1.

As the process continues, improvements for the PQC schemes are still being studied and proposed. Vectorizing time-consuming primitives [KKP20] is used to improve Kyber using KEM SHA3 and AES variants [Av21]. A fast and first-order secure Kyber implementation optimized for ARM Cortex-M4 is presented in [He21a]. Number-theoretic transform (NTT) is another approach used to increase the performance significantly for Kyber [BKS19], NTRU [Al21a; Ch19] and Saber [Ch21b; DA19] on Cortex-M4 chips. Using advanced single-instruction multiple-data instructions (NEON) [DK21], optimized constant-time software implementations for Kyber, NTRU, and Saber are provided. Techniques to optimize memory requirements in computing discrete logarithms in SIKE [Co20] are presented in [HKP21]. Reducing the input of the hash function leads to noticeable improvements in lattice-based key-encapsulation mechanisms (KEMs), improving Kyber and Saber [Ju21] using generic Fujisaki-Okamoto (FO) transformation. A side-channel resistant implementation of Saber is provided in [Ab21], showing a novel primitive for masked logical shifting on arithmetic shares. Masking the underlying zero-knowledge proof system of Picnic [Ar21] should improve its security against SCAs. Sampling discrete Gaussians through arbitrary-centered sampling over Integers [ZSS20] and generating discrete Gaussians with arbitrary center and standard deviation [Ho20] offer improvements for lattices and Falcon [Fo20]. A speed up in the key generation of Rainbow [DS05] is proposed in [Pe20], eliminating some drawbacks of the scheme. Through efficient statistical zero-knowledge proofs for module/ring learning with errors (LWE) and short integer solution (SIS) relations [Bo20], it is shown that the security of lattice-based schemes can be improved. Costello [Co21] provides a thorough analysis of SIKE and highlights several aspects of its yet unbroken security.

Scheme Integration The cryptographic library liboqs, developed by the Open Quantum Safe project [SM16], provides quantum resistant cryptographic primitives, and compares implementations of the NIST candidates (except GEMSS [Ca19b]) integrated using OpenSSL within applications such as Apache web server and Chromium. They offer PQ and hybrid implementations for TLS, SSH, S/MIME and x.509 certificates [Mi21]. Early usage of PQ KE cipher-suites for the TLS protocol based on R-LWE [Bo15] is demonstrated in an integration into the OpenSSL library using the Apache web server showing that secure PQ KE is practical. Classic McEliece is used in a quantum safe MACsec [CS21], offering hybrid mode, ephemeral key-exchange (KE), and an end-to-end encryption in Ethernet networks. Suitable NIST candidates are evaluated for use in Domain Name System Security Extensions (DNSSEC) within certain constraints [Mü20]. However, most candidates require larger signature and public key (PK) sizes compared to classical algorithms. Other efforts focus on replacing the DH-based handshake using PQ secure KEMs or hybrid KE [Az21; Hü20] and using DH type authenticated KE protocols from supersingular isogenies [Ba21b; Fu18; KK18]. Moreover, a PQ handshake is successfully integrated in the WireGuard VPN using Kyber and Rainbow [MAY21].

RFC Drafts RFC8391 [Hu18] defines the eXtended Merkle Signature Scheme XMSS, a quantum-safe hash-based signature scheme. RFC8554 [MCF19] describes the hash-based Leighton-Micali signature system. It provides asymmetric authentication and can achieve a high security level, which is secure against a quantum computer. RFC drafts for hybrid KE schemes for TLS 1.2 and 1.3 are proposed in [CC20; SFG20; Wh17]. Older drafts for TLS include the use of additional shared secrets and the Quantum-Safe Hybrid (QSH) cipher-suite [SS17; SWZ16]. Another draft proposed in [Ka20] defines hybrid KE and PQ PK authentication methods for SSH. RFC8784 [Fl20] describes an extension of IKEv2 that is quantum-resistant by using pre-shared keys. A draft to integrate PQ KE into IKEv2 is proposed in [Tj19], using multiple payloads in conjunction with the existing (EC)DH payload. The intermediate exchange for IKEv2 is defined in [Sm21], for transferring large data in the IKEv2 Security Association (SA) establishment. This should help avoiding IP fragmentation of large IKE messages, but cannot be used in the initial IKEv2 exchange.

Other Algorithms Some other novel approaches seem very promising and practical, even though they are not part of the NIST standardization process. A new class of post-quantum signature schemes based on symmetric primitives is presented in [Ch17]. Supersingular EC [CD20] show a significant speed-up in commutative supersingular isogeny DH (CSIDH). Instead of using hidden field equations (HFE), PK encryption schemes can be constructed using multivariate quadratic polynomials [Sa20], based on the generalization of isomorphism of polynomials with two secrets (IP2S) problem to obtain a DH like structure. Implementing Gaussian pre-image sampling on module lattices [Be21] seems practical for signature schemes and for advanced constructions using trapdoors such as identity-based encryption. The PERN multivariate encryption scheme is proposed in [YWT20], based on solving nonlinear equations over real numbers. Mikata [Th21], a signature scheme over NTRU lattices, is arguably a more versatile variant of Falcon. Another variant of Falcon, Zalcon [Fo21], claims more suitable for constraint environments such as smart cards. Lattice-based KINDI-KEM, a former NIST candidate, is formally specified in DIN SPEC 91444 [Dr21].

3 Performance Considerations

Multiple research efforts deal with the performance of PQC algorithms, mostly focusing on hardware implementations and network performance.

Algorithm Performance As indicated by NIST [NI16], the algorithms can be classified into three categories. The first is for a 128-bit security level, category three is for 192 bits, and category 5 is for 256 bits. A thorough overview of all NIST candidates and their security levels is provided in [Fe20]. Benchmarks and comparisons of round two NIST candidates [Ba19; Da20] state that a higher security level increases latency and timing overhead. They indicate that Kyber, FrodoKEM [Al21b], Saber, and SIKE have both high-speed and lightweight implementations. Kyber also shows advantages in terms of execution times, power consumption, and energy usage. Dilithium stands out for its superior signature generation, in terms of speed and memory consumption. In general, lattice- and code-based algorithms are more feasible than isogeny-based algorithms due to the huge performance overhead of the latter [BRP20; PS20; We20]. Stateless hash-based symmetric signature schemes, such as SPHINCS+ [Au20], are generally less efficient than lattice-based signature schemes like Dilithium [Ba21a] or Falcon. They are mainly interesting for applications without high latency requirements, such as offline code signing or certificate signing. Test results show great advantage for SPHINCS+ over similar schemes, such as Picnic [Za20], in terms of speed, signature size, and security. Algorithms that require too much memory or depend on external libraries such as Classic McEliece [Ch20], BIKE [Ar20] and RAINBOW pose a serious challenge on the implementation level.

Hardware Performance Many research efforts highlight the challenges and benefits of implementing PQC algorithms on special hardware and IoT devices, compare their performance, and address required measures and recommendations [Fe20; Ga18; Su20]. They also benchmark PQC schemes such as XMSS, qTesla [Al20c], SIKE, Classic McEliece, Dilithium, Rainbow, and Kyber providing real-time performance evaluation on specific devices and in embedded systems, such as the ARM Cortex-M4, ARM Cortex-R5, IBM Z, and IoT Trust-Anchor chips [CC21; CKY21; Jo21; Ka19; Ma20; MK19]. Some algorithms are still not suitable for such hardware platforms. However, improvements, optimizations, and outlook for further optimization potential are provided. The suitability of PQC on resource constrained devices, such as automotive hardware security modules (HSM) and in vehicle to vehicle communication (V2V), is also analyzed and evaluated [Go21; Ni21; WS20]. Although it is considered feasible, the deployment of algorithms with multiple parameter sets and large key/packet sizes is still work in progress and requires several adaptations. On common IoT platforms, optimizations are offered [AS20], and it is encouraged to focus on smaller RAM usage vs smaller code-size [De21]. Moreover, it is recommended to choose Falcon over Dilithium for signatures, and that Saber or Kyber be selected as a KEM. Kyber is recommended in mobile applications and is suitable for usage on smartphones [Si21]. Saber is still being checked regarding its suitability for mobile devices [Ri21]. In general, lattice-based schemes such as NTRU-HRSS [Ch19; Hü17] and SPHINCS+ are recommended of IoT settings [Ne19]. However, a decreased security level needs to be considered. In many cases, Field Programmable Gate Arrays (FPGA) are used to investigate the possible performance benefits [Da20; Ko17; Ku20a; ZGF20]. Several high-performance hardware architectures, low level implementation mappings, as well as hybrid KE methods on FPGAs are proposed and evaluated for PQ algorithms, such as SIKE, SPHINCS, Kyber, NTRU, and Saber [Ba19; DMG21; HLX21; KAK18; Ku17]. In general, executing cryptographic algorithms on optimized hardware leads to a significant performance boost and is essential for the usage of these algorithms, especially for less performant PQ algorithms in performance critical use cases [TLW19].

Network Performance With larger signatures and keys, more data must be transferred within networks. This leads to packet fragmentation, which may result in high delays in lossy networks [PST19]. In general, protocols such as TLS, DTLS, and QUIC are able to handle bigger signature sizes, and while the overhead is significant, it is acceptable in most modern use cases [Ka18a; SKD20a; SM16]. The key establishment with Kyber-based TLS performs well compared to ECDH, whereas using SPHINCS+ signatures is challenging on embedded PQC-TLS servers, due to signature sizes and signing time [Bü20]. Additionally, the execution times for PQC algorithms are usually higher than for classical ones and a longer loading time for websites is a problem, because it may lead to bad user experience [Ad19; Kw19; SKD20b]. Use cases such as VPN are less impacted (establishing a connection only once in a while) [KS19]. Experiments in simulated [PST19] as well as in real networks [He19a; KV19] show which algorithms are suitable for these use cases. Some works evaluate the usage of PQC in Blockchain networks [AK18; Ca19a] and propose using lattice-based schemes as a replacement for ECDSA.

4 Security Considerations

The new PQ algorithms open up new undiscovered attack surfaces and introduce additional mathematical concepts into the cryptographic world. New risks that may come with these concepts have to be investigated.

Cryptanalysis Cryptanalysis examines the security of cryptographic schemes given a sophisticated attacker that is able to perform analytical and/or practical attacks. Many of the candidates that were submitted to the first round of the NIST challenge have fallen to various cryptanalysis attacks [Di20a]. In general, either the imposed security of the attacked algorithms dropped below the requirements of NIST, or the scheme was completely broken and the attackers were able to retrieve the private key [Sa19]. Some schemes seem to be secure under classical computing preliminaries only, but fail to resist quantum attacks

[DLW19]. In addition, PQC can not only be used for KE and signatures, other areas can be pseudo-random number generators and encryption [Ku20b]. On the other hand, researcher extracted indications for secure designs from those attacks. Methods to assure security against a certain type of attacks are presented in [Cr20; PS13] and [JS19] present models that enable direct comparisons between classical and quantum algorithms, improving security assumptions for PQC algorithms. Moreover, several new attacks targeting the foundations of the developed PQC schemes are introduced. A new key recovery technique based on MinRank can break multivariate primitives [SV20], whereas another on HFEs used in GEMSS shows that the proposed parameters of the scheme are not as secure as claimed [TPD21]. A new adaptive attack can recover the secret key for a realistic choice of parameters on homomorphic encryption schemes [FHR21]. Hybrid attacks on NTRU can be threatening and require revising its security estimates [Ng21]. Some security issues may occur due to state synchronization failures, which may be avoided through using hybrid stateless/stateful schemes with smaller signatures and faster signing [GFL19; Mc16]. The correctness of NIST candidates is also formally re-assessed [BS20a], and security notions, such as the anonymity and indistinguishability under (chosen/adaptive) ciphertext attacks (IND-CCA) [Al20a; GMP21], qIND-qCPA [GKS20], and random oracles in a PQ mode [KS20] are evaluated and improved. Moreover, new lower bounds on decoding attacks for lattice and code-based schemes are derived [KL21], whereas new upper bounds for rank attacks HFEs in multivariate schemes [ØSV21] are proven.

Side-Channel Attacks Side-channel attacks (SCA) target the specific circumstances of algorithm execution like timing and power consumption. PQC algorithms introduce new attack surfaces in this regard and have to be analyzed for weaknesses not only in a general regard of the algorithm but also in specific hardware circumstances. For all categories of PQC algorithms, SCAs were found, and at the same time effective countermeasures for these attacks have been introduced [Zh20a; Zh20b]. However, the research states that SCAs on PQC algorithms and their countermeasures are still in a very early state. Many SCAs on PQC are not yet evaluated and the current countermeasures usually use ad-hoc designs that protect against individual SCAs but remain vulnerable against others. Tendayi et al. [Te21] provide a multi-target and multi-tool platform to conduct test vector leakage assessment for NIST candidates. Chowdhury et al. [Ch21a] give an overview of several PQC-related SCAs. They discuss SCAs for the different categories of PQC algorithms, random number generators and physically non-cloneable functions.

There are also efforts to minimize the attack surface in general [DA20; Kh18; Zh20b], and other studies focusing on special types of attacks. Discrete Gaussian samplers are shown to be vulnerable to SCAs in many cases, such as timing information leakage with FPGA-based cumulative distribution tables (CDT) for discrete Gaussian samplers [Kh16], and the so-called flush, Gauss, and reload attack [Gr16] using CDT or Bernoulli sampling. Some of the most threatening discovered attacks include fault attacks on lattice-based schemes, such as (first-order) randomizing, zeroing, and skipping faults [BBK16]; the singularity attack on multivariate PK schemes [Di20b] using a system of linear equations; horizontal SCA on lattice-based algorithms [Ay18] estimating the secret key from a single power measurement with very high success rates; differential power analysis [GSE20; Ka18b], which shows that the security of a hardware implementation of SPHINCS-256 is compromised, due to its stateless construction, and that SC information can successfully recover the entire secret key from fewer than 30 observed Picnic signatures; correlation power analysis (CPA) [Pa18], through which a secret leakage on Rainbow-like multi-layered schemes is identified; improved torsion point attacks on SIDH variants [KP21] constructing backdoors for curves and base field primes, which implies that some modifications for SIKE should to be considered; single-trace SCAs [Am20; AR21] recovering the entire secret key on NewHope [Al20b], and a large portion of it on NTRU; theoretical fault injection attacks [Ta21], which can threaten SIKE. Moreover, electromagnetic (EM) SC assisted CCAs over multiple LWE/LWR-based PKEs and KEMs [Pr21] lead to complete key-recovery on lattice-based schemes. Additionally, the spatial dependencies, such as the dependency of the secret key and certain registers, of cryptographic algorithms can be exploited with the help of near-field micro-probes [An19]. However, multivariate signature schemes offer good protection against fault attacks, as potentially harmful attack vectors only partially succeed in recovering the key [KL19].

However, such attacks are not restricted to the new PQC algorithms, as they can still target some of the standard building blocks in many of the old and new schemes alike. Single trace soft-analytical SCA on KECCAK [KPP20] shows that is possible to exploit some vulnerabilities on 8-bit microcontrollers. Countermeasures such as masking and hiding are therefore recommended.

Downgrade Attacks Security protocols such as TLS may suffer from possible downgrade attacks leading the communicating parties to fall back to earlier versions of the protocol [LSH20]. This type of attacks could be especially exploited in the case of a downgrade from PQC to classical cryptography. Crockett et al. [CPS19] distinguish between three main cases, where the client, the server, or both are either aware or unaware of the new protocols. This implies a possible downgrade on the side that is already using a new protocol.

5 Migration Process

We distinguish between two levels regarding the process of migration towards PQC. Those being the migration of algorithms into existing cryptographic applications and security protocols, and the migration of IT-systems and infrastructures.

Algorithm Migration Several approaches show special interest in hybrid KE methods and hybrid combiners. The primary goal of these is to ensure that the desired security property holds as long as one of the component schemes remains unbroken [CPS19]. These approaches use two or more independent algorithms chosen from both PQ, and classical schemes. This way, it is neither necessary to fully trust the potentially outdated classical scheme, nor the relatively new PQ scheme until it had proven secure enough.

An experiment with a hybrid approach on Google servers is presented in [Br16]. The solution combines EC with NewHope. Another series of experiments presented in [KV19; La16] compare hybrid PQ to non-PQ key agreement in TLS. First implementations and case studies [CPS19; ZWH21] using TLS and SSH in OpenSSL reveal some challenges regarding message size for the protocol itself. Crockett et al. [CPS19] suggest conveying the cryptographic data either by extending the format of the protocol message, or through concatenating the data into a single value. The method of combining also affects the security and performance of the protocol.

A similar approach is proposed for IKEv2 [He19b; Zi15], showing the feasibility of hybrid KE with NIST candidates. The use of lattice-based PQC algorithms with the Apache Kafka Software using a hybrid approach [We20] shows that the performance of the hybrid solution is as good as the slowest algorithm used within. The use of lattice-based PQC algorithms for the industrial protocol Open Platform Communications Unified Architecture (OPC UA) is examined in [PS20]. The approaches are feasible but result in additional performance and communication overhead. Parallel usage of two independent cryptographic schemes within public key infrastructures is also possible with X.509-compliant hybrid certificates [Bi19a]. This approach enables a step-wise transition to PQ secure and hybrid algorithms. There are also new models for KEMs and authenticated KE protocols [Bi19b], proposing several combiners and a provably sound design for hybrid KE using KEMs. Fischlin et al. [FLP14] state a notion for robust multi-property combiners and implement a combiner that satisfies the strongest notion by preserving every property of the input hash functions. An underrepresented approach is possible through the usage of composite key structures for keys and signatures in PKCS#10, CMP, X.509, and CMS structures [OP20].

System Migration The migration process is not simply limited to algorithm exchange or replacement. Updating a set of software applications, their implemented algorithms or changing their underlying infrastructure requires a tedious process, which involves thorough planning and execution over a specific period of time. This is especially challenging when the systems to be migrated need to stay online and/or must maintain interoperability with other systems that may or may not (yet) be upgraded [OP19]. Therefore, one cannot assume a successful migration without considering the challenges related to the planned approach. According to [OP19], one must first identify the domains and their respective priorities in the planned migration. Moreover, there are interrelated dependencies that may not be easy to resolve. Thus, the migration could prove difficult in IT-infrastructures with security vulnerabilities, making them prone to failures. Several works recommend the use of a cryptographic inventory and automated discovery tools as the first step of a planned migration [BPS20; KNW18], which is also suggested by ETSI in their three-stage migration approach [ET20]. Fischer und El Bansarkhani [Qu21] propose a four-step process for the PQC migration. It starts by detecting the affected components and assessing their PQC readiness. Then, a risk analysis is conducted to prioritize the elements to be transitioned, followed by the actual migration of the individual components to PQC.

6 Discussion, Conclusion and Future Work

We discuss our major findings and address open issues. We follow the same categorization scheme presented in the structure of this paper and draw final thoughts and conclusions.

Towards New Standards The efforts undertaken towards establishing new cryptographic standards are promising, yet still focus more on low level cryptographic primitives and schemes. Following the third NIST PQC conference in June 2021, several algorithms have been, and are still being continuously analyzed and benchmarked. Given the rigorous selection process with worldwide participation and a current set of 15 finalists and alternative candidates, there should be little doubt that we will soon have a set of vetted PQC algorithms at our disposal. Many candidates have already proved acceptable replacements for different classical schemes and showed capable of integration within specific cryptographic protocols and applications utilizing them. However, this implies rather having a set of multiple established algorithms to be used in parallel. Consequently, algorithm selection depends greatly on other factors and future developments. Therefore, carefully selecting algorithms for specific use cases will be an important topic in the future. Still, there is enough room for further development to adapt to special requirements. However, there seem to be a lack of interest in the strategies required to execute the actual migration on a more sophisticated level of abstraction. The efforts made for testing, benchmarking or integration in new or existing protocols consist mainly of independent research and draft proposals, which is not sufficient for the overall migration process on a broader scale.

Performance Considerations As correctly assumed by NIST [NI16], the performance assessment of cryptographic algorithms on specialized hardware platforms has shown to be an important research question for the candidates of the standardization process. Depending on the choice of algorithm and field, PQC can very well be a replacement for classic algorithms. However, it is not very clear, which algorithms perform best in which situation, moreover on which hardware platforms or for which application scenarios. Generally, lattice and code-based algorithms proved more efficient in terms of speed than isogeny-based ones. However, code-based algorithms need more memory. Lattice-based signature schemes also proved more efficient in terms of speed than stateless hash-based schemes in scenarios with strong latency. Special FPGAs are expected to improve the overall performance significantly, but their usage is not always a valid option. Network devices have to handle the overhead introduced by PQC and still provide acceptable latency. This also impacts end user devices, e.g. smartphones, which have limited power resources and are used in mobile networks. For example, the overhead introduced by PQC is manageable in protocols such as TLS and DTLS. On the other hand, larger key sizes lead to longer loading times, negatively impacting user experience in lossy networks and web related use cases. This however, is not the case for VPN, which is less impacted by PQC. Thus, the efficiency of PQC must allow for usage within established and new application scenarios. Notably, IoT, which is still an underrepresented field, is of special interest due to its restricted resources. So far, lattice-based algorithms seem to be the best choice for such systems.

Security Considerations Due to the described performance challenges that come with the new PQ algorithms, the choice of the algorithm parameters and key sizes play a vital role in establishing security of a cryptographic scheme. Depending on the use case different algorithms and/or set of parameters may be suitable. It is important to understand the trade-off between security and algorithm requirements to be able to choose the right algorithms and/or parameters for different use cases. Moreover, since some PQC algorithm aspects are still fairly new and didn't face enough scrutiny, the long-term security of these algorithms remains unclear. Especially attack vectors like side channel attacks based on timing or power consumption are still in an early state and pose a risk. A very special technique that has not gotten enough research so far is the exploitation of location-based leakages. Some of the biggest issues regarding the security are related to design aspects. Cipher-suite negotiation determines an algorithm that all parties are willing to use. Downgrade attacks target these negotiations to force a weaker security. Many vulnerabilities have been found and fixed, but a crucial question remains, if less costly mitigation measures can be implemented that impact the overall performance as little as possible.

Migration Process The most common difficulties arise from the integration of PQC algorithms into existing protocols. The existing migration approaches address issues on the implementation and communication levels and offer promising solutions for many challenges; such as defining hybrid formats, algorithm negotiation and parameters. Many of the NIST candidates prove suitable for usage in a hybrid scheme; nonetheless, some protocols have size constraints that prevent some schemes from being used. A trade-off between increasing the size limits and performance needs further investigation for more precise results. Depending on the scenario, different design decisions are required.

On a broader scale, a full migration of IT-systems and infrastructures involves more complex issues. Not all systems will be updated to PQ algorithms in time or cannot be updated at all. Therefore, strategies on how to deal with these systems have to be developed. These could be automation frameworks that are used transparently within protocols or systems to manage their migration into PQC or ensure their security. Automated software is needed in order to deploy PQC algorithms and protocols with minimum human interaction. This is especially the case in larger IT-infrastructures such as data centers and cloud-based applications. Such software should be able to identify the currently used cryptographic components. Automated tools could also support real-time analysis of an ongoing migration, check for any weaknesses and verify the security of new PQC libraries. The aforementioned issues clearly point out the importance of developing frameworks capable of managing, executing and testing the various aspects within a migration process on different scales and implementation levels. Our survey shows a lack of such automated software. Too few projects and research dealing with these questions were found.

Conclusion Considering the expected rise of quantum computing, challenges posed upon classical cryptography and the IT-systems using them will become tangible threats jeopardizing the safety and security of IT-systems, applications and communication alike. In this paper, we present a survey of the ongoing research efforts towards realizing PQC in practice. Our findings indicate a major focus of the ongoing research on algorithms per se, and the feasibility of migrating different cryptographic schemes and security protocols with reasonable trade-offs regarding algorithm performance and communication efficiency. Considerable work on the standardization and integration into established standards, such as TLS, SSH, and X.509, has been done. It is nevertheless clear that the tasks involved in the entirety of the PQC migration stretch over a wide range of sub-fields and PQC-related categories. There are still many challenges and open issues that need to be addressed, especially on levels above algorithm development. These include protocol design, migration and deployment strategies, legacy systems, testing frameworks, and process automation.

Outlook The overview and findings at hand provide a starting point for providing answers to the yet untouched issues. Identifying the challenges and open issues is, however, only the first step in our research. Theoretical and practical case studies can be conducted to come up with new ideas and solutions. We initiated an online project (`https://fbi.h-da.de/cma`), inviting researchers to join us continuing the work started with the paper at hand. We are also working on the development of solutions aiding the community in the transition to PQC and achieving this migration (`https://fbi.h-da.de/pqc`). A first prototype of an easy-to-use cryptographic interface called eUCRITE (`https://fbi.h-da.de/eucrite`), providing minimal knowledge abstractions for both conventional and PQC functionalities is evolved. Other projects under development include an automated cryptographic infrastructure detection tool, a PQC testing framework, TLS 1.3 PQC integration evaluation, and a code-binding generator for PQC algorithms based on an abstract meta-description language. The next step of our endeavor is to utilize the gathered findings, knowledge and experience throughout our research on the way towards usable and agile PQC.

Acknowledgment: This research work has been funded by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

Appendix

Categorization Scheme

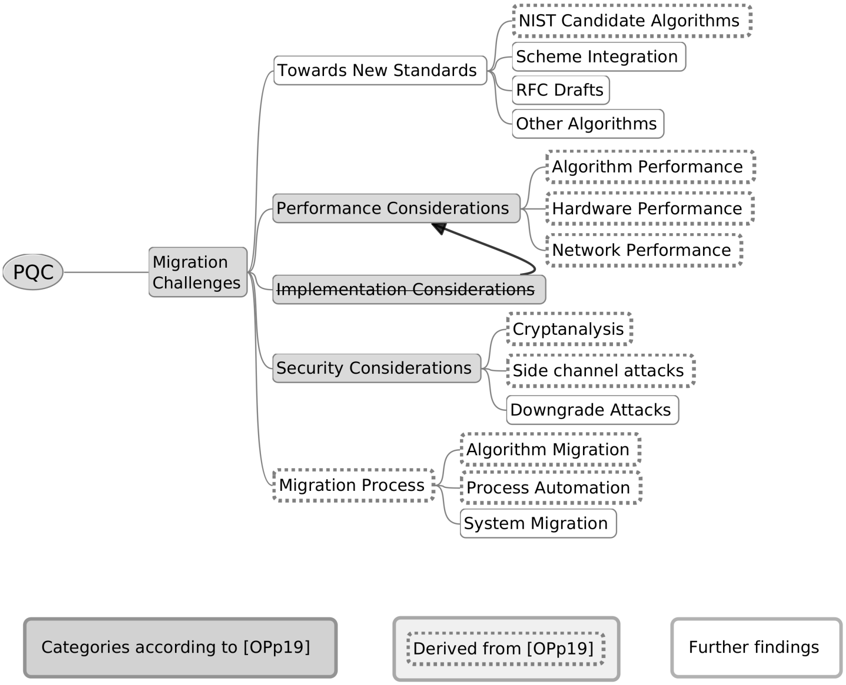

Fig. 1: Categories of PQC Migration as defined by [OP19] (grey). Extensions derived by us from [OP19] (dotted line). Further extensions by us (white and strikethrough).

Survey Overview

Tab. 1: Survey Overview

NIST Candidate Algorithms	
Basics of Post-Quantum Cryptography	[Be09]
Current state of NIST standardization process	[Al19; Ch16; Mo20; NI16]
Categories of PQC algorithms	[GAB19; NW17; OP19]
Improvements for NIST finalists	[Ab21; BKS19; Bo20; Co21; DK21; He21a; HKP21; Ho20; Ju21; KKP20; Pe20; ZSS20]
ALL NIST PQC finalists	[Al20c; Al21a; Ar20; Au20; Av21; Ba21a; Ca19b; Ch19; Ch20; Ch21b; Co20; DA19; DS05; Fo20; Za20]
Scheme Integration	
Integration into existing tools	[Bo15; Mi21; SM16]
Quantum safe MACsec	[CS21]
Integration into DNSSEC	[Mü20]
Handshakes with PQC	[Az21; Ba21b; Fu18; Hü20; KK18; MAY21]
RFC Drafts	
Hash Signatures	[Hu18; MCF19]
Hybrid KE schemes for TLS	[CC20; SFG20; Wh17]
Shared secrets and QSH cipher-suite	[SS17; SWZ16]
Hybrid key-exchange	[CC20; Ka20]
IKEv2	[Fl20; Sm21; Tj19]
Other Algorithms	
New class of signature schemes	[Ch17]
Speed-up for CSIDH	[CD20]
PKE using multivariate quadratic polynomials	[Sa20]
Signatures and identity-based encryption	[Be21]
PERN multivariate encryption scheme	[YWT20]
Falcon Variants	[Fo21; Th21]
Lattice-based KINDI-KEM	[Dr21]
Algorithm Performance	
Security levels and impact	[Ba19; Da20; Fe20]
Lattice and code superior to isogeny	[BRP20; PS20; We20]

Hardware Performance	
Hardware Implementations	[CC21; CKY21; Da20; Fe20; Ga18; Go21; Jo21; Ka19; Ko17; Ku20a; Ma20; MK19; Ni21; Su20; WS20]
FPGAs	[Ba19; Da20; DMG21; HLX21; KAK18; Ko17; Ku17; Ku20a; TLW19; ZGF20]
Mobile Devices	[Ri21; Si21]
IoT	[AS20; De21; Hü17; Ne19]
Network Performance	
Latency increased but acceptable	[Ad19; Ka18a; Kw19; PST19; SKD20a; SKD20b; SM16]
Hash-based crypto on embedded devices	[Bü20]
VPN less impacted by PQC	[KS19]
Experiments with various algorithms	[He19a; KV19; PST19]
Lattice for blockchain networks	[AK18; Ca19a]
Cryptanalysis	
Broken NIST candidates	[Di20a; DLW19; Sa19]
Code-based PRNG	[Ku20b]
Attack mitigations	[Cr20; JS19; PS13]
Avoiding synchronization failures	[GFL19; Mc16]
Formal assessments	[Al20a; BS20a; GKS20; GMP21; KS20]
Lower bounds in lattice and code PQC	[KL21]
Upper bounds for multivariate PQC	[ØSV21]
Key recovery	[SV20; TPD21]
Adaptive attack	[FHR21]
Hybrid attacks on NTRU	[Ng21]
Side-Channel Attacks	
Attacks and their countermeasures	[Ar21; BBK16; Ch21a; DA20; Kh16; Kh18; Zh20a; Zh20b]
Successful attacks	[Am20; An19; AR21; Ay18; Di20b; Gr16; GSE20; Ka18b; KPP20; Pa18; Pr21]
Potential threads	[Al20b; KL19; KP21; Ta21; Te21]

Downgrade Attacks	
Possible attack vectors	[LSH20]
Missing protocol awareness	[CPS19]
Algorithm Migration	
Large scale experiments and benchmarks	[Br16; KV19; La16]
Protocol Challenges	[CPS19; ZWH21]
Hybrid and Combiners	[Bi19a; Bi19b; FLP14; OP20; We20]
IKEv2 feasible for PQC	[He19b; Zi15]
Lattice-based PQC for OPC UA	[PS20]
System Migration	
Crypto inventory and automated discovery	[BPS20; ET20; KNW18]
Stages in the process of the PQC migration	[ET20; Qu21]

References

[Ab21] Abubakr, A.; Kamyar, M.; Viet Ba, D.; Jens-Peter, K.; Kris, G.: A Lightweight Implementation of Saber Resistant Against Side-Channel Attacks, Conference Name: Third PQC Standardization Conference, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/abdulgadir-lightweight-implementation-gmu-pqc2021.pdf, visited on: 07/23/2021.

[Ad19] Adam Langley: Real-world measurements of structured-lattices and supersingular isogenies in TLS, Oct. 2019, URL: https://www.imperialviolet.org/2019/10/30/pqsivssl.html, visited on: 09/17/2020.

[AK18] An, H.; Kim, K.: QChain: Quantum-resistant and Decentralized PKI using Blockchain, 2018, URL: https://caislab.kaist.ac.kr/publication/paper_files/2018/SCIS'18_HC_BC.pdf, visited on: 07/14/2021.

[Al19] Alagic, G.; Alperin-Sheriff, J.; Apon, D.; Cooper, D.; Dang, Q.; Liu, Y.-K.; Miller, C.; Moody, D.; Peralta, R.; Perlner, R.; Robinson, A.; Smith-Tone, D.: Status report on the first round of the NIST post-quantum cryptography standardization process, tech. rep. NIST IR 8240, Gaithersburg, MD: National Institute of Standards and Technology, Jan. 2019, NIST IR 8240, URL: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf, visited on: 02/24/2021.

[Al20a] Alagic, G.; Jeffery, S.; Ozols, M.; Poremba, A.: On Quantum Chosen-Ciphertext Attacks and Learning with Errors. en, Cryptography 4/1, p. 10, Mar. 2020, ISSN: 2410-387X, URL: https://www.mdpi.com/2410-387X/4/1/10, visited on: 07/13/2021.

[Al20b] Alkim, E.: NewHope - Algorithm Specifications and Supporting Documentation, Apr. 2020, URL: https://newhopecrypto.org/data/NewHope_2020_04_10.pdf, visited on: 07/19/2021.

[Al20c] Alkim, E.; Barreto, P. S. L. M.; Bindel, N.; Krämer, J.; Longa, P.; Ricardini, J. E.: The Lattice-Based Digital Signature Scheme qTESLA. In (Conti, M.; Zhou, J.; Casalicchio, E.; Spognardi, A., eds.): Applied Cryptography and Network Security. Vol. 12146, Series Title: Lecture Notes in Computer Science, Springer International Publishing, Cham, pp. 441–460, 2020, ISBN: 978-3-030-57807-7 978-3-030-57808-4, URL: http://link.springer.com/10.1007/978-3-030-57808-4_22, visited on: 03/18/2021.

[Al21a] Alkim, E.; Cheng, D. Y.-L.; Chung, C.-M. M.; Evkan, H.; Huang, L. W.-L.; Hwang, V.; Li, C.-L. T.; Niederhagen, R.; Shih, C.-J.; Wälde, J.; Yang, B.-Y.: Polynomial Multiplication in NTRU Prime: en, IACR Transactions on Cryptographic Hardware and Embedded Systems/, pp. 217–238, 2021, ISSN: 2569-2925, URL: https://tches.iacr.org/index.php/TCHES/article/view/8733, visited on: 03/18/2021.

[Al21b] Alkim, E.; W. Bos, J.; Ducas, L.; Longa, P.; Mironov, I.; Naehrig, M.; Nikolaenko, V.; Peikert, C.; Raghunathan, A.; Stebila, D.: FrodoKEM - Learning With Errors Key Encapsulation, June 2021, URL: https://frodokem.org/files/FrodoKEM-specification-20210604.pdf, visited on: 07/14/2021.

[Am20] Amiet, D.; Curiger, A.; Leuenberger, L.; Zbinden, P.: Defeating NewHope with a Single Trace. IACR Cryptol. ePrint Arch. 2020/, p. 368, 2020.

[An19] Andrikos, C.; Batina, L.; Chmielewski, L.; Lerman, L.; Mavroudis, V.; Papagiannopoulos, K.; Perin, G.; Rassias, G.; Sonnino, A.: Location, Location, Location: Revisiting Modeling and Exploitation for Location-Based Side Channel Leakages. In (Galbraith, S. D.; Moriai, S., eds.): Advances in Cryptology – ASIACRYPT 2019. Vol. 11923, Series Title: Lecture Notes in Computer Science, Springer International Publishing, Cham, pp. 285–314, 2019, ISBN: 978-3-030-34617-1 978-3-030-34618-8, URL: http://link.springer.com/10.1007/978-3-030-34618-8_10, visited on: 03/18/2021.

[Ar19] Armknecht, F.; Verbauwhede, I.; Volkamer, M.; Yung, M.: Biggest Failures in Security. en,/, p. 23, 2019.

[Ar20] Aragon, N.: BIKE: Bit Flipping Key Encapsulation Round 3 Submission./, Oct. 2020, URL: https://bikesuite.org/files/v4.1/BIKE_Spec.2020.10.22.1.pdf.

[AR21] Askeland, A.; Rønjom, S.: A Side-Channel Assisted Attack on NTRU, Published: Cryptology ePrint Archive, Report 2021/790, 2021.

[Ar21] Aranha, D. F.; Berndt, S.; Eisenbarth, T.; Seker, O.; Takahashi, A.; Wilke, L.; Zaverucha, G.: Side-Channel Protections for Picnic Signatures, Published: Cryptology ePrint Archive, Report 2021/735, 2021.

[AS20] An, S.; Seo, S. C.: Efficient Parallel Implementations of LWE-Based Post-Quantum Cryptosystems on Graphics Processing Units. en, Mathematics 8/10, Number: 10 Publisher: Multidisciplinary Digital Publishing Institute, p. 1781, Oct. 2020, URL: https://www.mdpi.com/2227-7390/8/10/1781, visited on: 07/13/2021.

[Au20] Aumasson, J.-P.: SPHINCS+ Submission to the NIST post-quantum project, v.3, Oct. 2020, URL: https://sphincs.org/data/sphincs+-round3-specification.pdf, visited on: 07/19/2021.

[Av21] Avanzi, R.: CRYSTALS-Kyber Algorithm Specifications And Supporting Documentation(version 3.01)./, Jan. 2021, URL: https://pq-crystals.org/kyber/data/kyber-specification-round3-20210131.pdf.

[Ay18] Aysu, A.; Tobah, Y.; Tiwari, M.; Gerstlauer, A.; Orshansky, M.: Horizontal side-channel vulnerabilities of post-quantum key exchange protocols. In: 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). Pp. 81–88, Apr. 2018.

[Az21] Azarderakhsh, R.; Khatib, R. E.; Koziel, B.; Langenberg, B.: Hardware Deployment of Hybrid PQC, Published: Cryptology ePrint Archive, Report 2021/541, 2021.

[Ba19] Basu, K.; Soni, D.; Nabeel, M.; Karri, R.: NIST Post-Quantum Cryptography - A Hardware Evaluation Study, tech. rep. 047, 2019, URL: https://eprint.iacr.org/2019/047, visited on: 04/02/2020.

[Ba21a] Bai, S.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schwabe, P.; Seiler, G.; Stehlé, D.: CRYSTALS-Dilithium - Algorithm Specifications and Supporting Documentation, Feb. 2021, URL: https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf, visited on: 07/14/2021.

[Ba21b] Banegas, G.; Bernstein, D. J.; Campos, F.; Chou, T.; Lange, T.; Meyer, M.; Smith, B.; Sotáková, J.: CTIDH: faster constant-time CSIDH, Published: Cryptology ePrint Archive, Report 2021/633, 2021.

[BBK16] Bindel, N.; Buchmann, J.; Krämer, J.: Lattice-Based Signature Schemes and their Sensitivity to Fault Attacks, Published: Cryptology ePrint Archive, Report 2016/415, 2016.

[Be09] Bernstein, D. J.: Introduction to post-quantum cryptography. In (Bernstein, D. J.; Buchmann, J.; Dahmen, E., eds.): Post-Quantum Cryptography. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 1–14, 2009, ISBN: 978-3-540-88701-0 978-3-540-88702-7, URL: http://link.springer.com/10.1007/978-3-540-88702-7_1, visited on: 07/17/2021.

[Be21] Bert, P.; Eberhart, G.; Prabel, L.; Roux-Langlois, A.; Sabt, M.: Implementation of Lattice Trapdoors on Modules and Applications./, July 9, 2021.

[Bi19a] Bindel, N.; Braun, J.; Gladiator, L.; Stöckert, T.; Wirth, J.: X.509-Compliant Hybrid Certificates for the Post-Quantum Transition. Journal of Open Source Software 4/40, p. 1606, Aug. 2019, ISSN: 2475-9066, URL: https://joss.theoj.org/papers/10.21105/joss.01606, visited on: 05/14/2021.

[Bi19b] Bindel, N.; Brendel, J.; Fischlin, M.; Goncalves, B.; Stebila, D.: Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange. In (Ding, J.; Steinwandt, R., eds.): Post-Quantum Cryptography. Vol. 11505, Series Title: Lecture Notes in Computer Science, Springer International Publishing, Cham, pp. 206–226, 2019, ISBN: 978-3-030-25509-1 978-3-030-25510-7, URL: http://link.springer.com/10.1007/978-3-030-25510-7_12, visited on: 03/12/2020.

[BKS19] Botros, L.; Kannwischer, M. J.; Schwabe, P.: Memory-Efficient High-Speed Implementation of Kyber on Cortex-M4. In (Buchmann, J.; Nitaj, A.; Rachidi, T., eds.): Progress in Cryptology – AFRICACRYPT 2019. Vol. 11627, Series Title: Lecture Notes in Computer Science, Springer International Publishing, Cham, pp. 209–228, 2019, ISBN: 978-3-030-23695-3 978-3-030-23696-0, URL: http://link.springer.com/10.1007/978-3-030-23696-0_11, visited on: 03/17/2021.

[Bo15] Bos, J. W.; Costello, C.; Naehrig, M.; Stebila, D.: Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem. In: 2015 IEEE Symposium on Security and Privacy. ISSN: 2375-1207, pp. 553–570, May 2015.

[Bo20] Boschini, C.; Camenisch, J.; Ovsiankin, M.; Spooner, N.: Efficient Post-quantum SNARKs for RSIS and RLWE and Their Applications to Privacy. PQCrypto 12100/, pp. 247–267, 2020.

[BPS20] Barker, W.; Polk, W.; Souppaya, M.: Getting Ready for Post-Quantum Cryptography:: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms, en, preprint, May 2020, URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.05262020-draft.pdf, visited on: 09/23/2020.

[Br16] Braithwaite, M.: Experimenting with Post-Quantum Cryptography, en, July 2016, URL: https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html, visited on: 04/03/2020.

[BRP20] Borges, F.; Reis, P. R.; Pereira, D.: A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography. IEEE Access 8/, pp. 142413–142422, 2020.

[BS20a] Bindel, N.; Schanck, J. M.: Decryption Failure Is More Likely After Success. In: PQCrypto. Pp. 206–225, 2020.

[BS20b] BSI: Migration zu Post-Quanten-Kryptografie - Handlungsempfehlungen des BSI. de,/, p. 9, Aug. 2020.

[Bü20] Bürstinghaus-Steinbach, K.; Krauß, C.; Niederhagen, R.; Schneider, M.: Post-Quantum TLS on Embedded Systems, tech. rep. 308, 2020, URL: https://eprint.iacr.org/2020/308, visited on: 04/03/2020.

[Ca15] Campagna, M.; Chen, L.; Dagdelen, O.; Ding, J.; Fernick, J.; Gisin, N.; Hayford, D.; Jennewein, T.; Lütkenhaus, N.; Mosca, M.: Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges. European Telecommunications Standards Institute ETSI White Paper/8, pp. 1–64, June 2015, URL: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

[Ca19a] Campbell, R.: Evaluation of Post-Quantum Distributed Ledger Cryptography. The Journal of the British Blockchain Association 2/1, pp. 1–8, May 2019, ISSN: 25163949, 25163957, URL: https://jbba.scholasticahq.com/article/7679-evaluation-of-post-quantum-distributed-ledger-cryptography, visited on: 07/13/2021.

[Ca19b] Casanova, A.: GeMSS: A Great Multivariate Short Signature. NIST Round 2/, 2019, URL: https://www-polsys.lip6.fr/Links/NIST/GeMSS_specification.pdf.

[CC20] Crockett, E.; Campagna, M.: Internet-Draft: Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS), Mar. 2020, URL: https://datatracker.ietf.org/doc/html/draft-campagna-tls-bike-sike-hybrid-03.

[CC21] Chen, M.-S.; Chou, T.: Classic McEliece on the ARM Cortex-M4, Published: Cryptology ePrint Archive, Report 2021/492, 2021.

[CD20] Castryck, W.; Decru, T.: CSIDH on the surface. In: International Conference on Post-Quantum Cryptography (PQCrypto 2020). Vol. 12100, Springer, pp. 111–129, 2020.

[Ch16] Chen, L.; Jordan, S.; Liu, Y.-K.; Moody, D.; Peralta, R.; Perlner, R.; Smith-Tone, D.: Report on Post-Quantum Cryptography, tech. rep. NIST IR 8105, National Institute of Standards and Technology, Apr. 2016, NIST IR 8105, URL: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf, visited on: 02/24/2021.

[Ch17] Chase, M.; Derler, D.; Goldfeder, S.; Orlandi, C.; Ramacher, S.; Rechberger, C.; Slamanig, D.; Zaverucha, G.: Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives, Published: Cryptology ePrint Archive, Report 2017/279, 2017.

[Ch19] Chen, C.; Danba, O.; Hostein, J.; Hülsing, A.; Rijneveld, J.; M. Schanck, J.; Schwabe, P.; Whyte, W.; Zhang, Z.: NTRU - Algorithm Specifications And Supporting Documentation, Mar. 2019, URL: https://ntru.org/f/ntru-20190330.pdf, visited on: 07/14/2021.

[Ch20] Chou, T.; Cid, C.; UiB, S.; Gilcher, J.; Lange, T.; Maram, V.; Misoczki, R.; Niederhagen, R.; Paterson, K. G.; Persichetti, E., et al.: Classic McEliece: conservative code-based cryptography./, Oct. 2020.

[Ch21a] Chowdhury, S.; Covic, A.; Acharya, R. Y.; Dupee, S.; Ganji, F.; Forte, D.: Physical security in the post-quantum era: A survey on side-channel analysis, random number generators, and physically unclonable functions. en, Journal of Cryptographic Engineering/, Feb. 2021, ISSN: 2190-8508, 2190-8516, URL: http://link.springer.com/10.1007/s13389-021-00255-w, visited on: 03/18/2021.

[Ch21b] Chung, C.-M. M.; Hwang, V.; Kannwischer, M. J.; Seiler, G.; Shih, C.-J.; Yang, B.-Y.: NTT Multiplication for NTT-unfriendly Rings: en, IACR Transactions on Cryptographic Hardware and Embedded Systems/, pp. 159–188, Feb. 2021, ISSN: 2569-2925, URL: https://tches.iacr.org/index.php/TCHES/article/view/8791, visited on: 03/18/2021.

[CKY21] Chou, T.; Kannwischer, M. J.; Yang, B.-Y.: Rainbow on Cortex-M4, Published: Cryptology ePrint Archive, Report 2021/532, 2021.

[Co20] Costello, C.; De Feo, L.; Jao, D.; Longa, P.; Naehrig, M.; Renes, J.: Supersingular Isogeny Key Encapsulation, Oct. 2020, URL: https://sike.org/files/SIDH-spec.pdf, visited on: 07/14/2021.

[Co21] Costello, C.: The Case for SIKE: A Decade of the Supersingular Isogeny Problem, Published: Cryptology ePrint Archive, Report 2021/543, 2021.

[CPS19] Crockett, E.; Paquin, C.; Stebila, D.: Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH. In. NIST, p. 24, 2019.

[Cr20] Cremers, C.; Düzlü, S.; Fiedler, R.; Fischlin, M.; Janson, C.: BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures, Published: Cryptology ePrint Archive, Report 2020/1525, 2020.

[CS21] Cho, J. Y.; Sergeev, A.: Post-quantum MACsec in Ethernet Networks. Journal of Cyber Security and Mobility/, Mar. 2021, ISSN: 2245-4578, 2245-1439, URL: https://journals.riverpublishers.com/index.php/JCSANDM/article/view/5973, visited on: 07/13/2021.

[DA19] D'Anvers, J.-P.: SABER: Mod-LWR based KEM (Round 3 Submission). NIST/, 2019, URL: https://www.esat.kuleuven.be/cosic/pqcrypto/saber/files/saberspecround3.pdf.

[DA20] D'Anvers, J.-P.: A Side-channel Resistant Implementation of SABER. IACR Cryptol. ePrint Arch 733/, 2020, URL: https://eprint.iacr.org/2020/733.pdf.

[Da20] Dang, V. B.; Farahmand, F.; Andrzejczak, M.; Mohajerani, K.; Nguyen, D. T.; Gaj, K.: Implementation and Benchmarking of Round 2 Candidates in the NIST Post-Quantum Cryptography Standardization Process Using Hardware and Software/Hardware Co-design Approaches. Published: Cryptology ePrint Archive, Report 2020/795, 2020.

[De21] Derek, A.: Requirements for Post-Quantum Cryptography on Embedded Devices in the IoT, Conference Name: Third PQC Standardization Conference, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/atkins-requirements-pqc-iot-pqc2021.pdf, visited on: 07/23/2021.

[Di20a] Ding, J.; Deaton, J.; Schmidt, K.; Vishakha; Zhang, Z.: Cryptanalysis of the Lifted Unbalanced Oil Vinegar Signature Scheme. In (Micciancio, D.; Ristenpart, T., eds.): Advances in Cryptology – CRYPTO 2020. Springer International Publishing, Cham, pp. 279–298, 2020, ISBN: 978-3-030-56877-1.

[Di20b] Ding, J.; Zhang, Z.; Deaton, J.; Wang, L.-C.: A Complete Cryptanalysis of the Post-Quantum Multivariate Signature Scheme Himq-3. In (Meng, W.; Gollmann, D.; Jensen, C. D.; Zhou, J., eds.): Information and Communications Security. Springer International Publishing, Cham, pp. 422–440, 2020, ISBN: 978-3-030-61078-4.

[DK21] Duc Tri, N.; Kris, G.: Optimized Software Implementations of CRYSTALS-Kyber, NTRU, and Saber Using NEON-Based Special Instructions of ARMv8, Conference Name: Third PQC Standardization Conference, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/hess-fast-quantum-safe-pqc2021.pdf, visited on: 07/23/2021.

[DLW19] Dong, X.; Li, Z.; Wang, X.: Quantum cryptanalysis on some generalized Feistel schemes. en, Science China Information Sciences 62/2, p. 22501, Feb. 2019, ISSN: 1674-733X, 1869-1919, URL: http://link.springer.com/10.1007/s11432-017-9436-7, visited on: 11/16/2020.

[DMG21] Dang, V. B.; Mohajerani, K.; Gaj, K.: High-Speed Hardware Architectures and Fair FPGA Benchmarking of CRYSTALS-Kyber, NTRU, and Saber, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/gaj-high-speed-hardware-gmu-pqc2021.pdf, visited on: 07/23/2021.

[Dr21] Dr. Rachid, El Bansarkhani; Hans-Peter, Fischer; Andreas, Schwab; Dr. Michael, Riecker; Dr. Juliane, Krämer: Definition of a quantum computer resistant encryption scheme, Apr. 2021, URL: https://www.din.de/en/innovation-and-research/din-spec-en/current-din-specs/wdc-beuth:din21:336773230, visited on: 07/24/2021.

[DS05] Ding, J.; Schmidt, D.: Rainbow, a New Multivariable Polynomial Signature Scheme. In (Ioannidis, J.; Keromytis, A.; Yung, M., eds.): Applied Cryptography and Network Security. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, pp. 164–175, 2005, ISBN: 978-3-540-31542-1.

[ET20] ETSI: Migration strategies and recommendations to Qantum Safe schemes, July 2020, URL: https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf, visited on: 07/28/2021.

[Fe20] Fernández-Caramés, T. M.: From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. IEEE Internet of Things Journal 7/7, pp. 6457–6480, 2020, URL: https://ieeexplore.ieee.org/abstract/document/8932459.

[FF20] Fernández-Caramès, T. M.; Fraga-Lamas, P.: Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. IEEE Access 8/, pp. 21091–21116, 2020, ISSN: 2169-3536.

[FHR21] Fauzi, P.; Hovd, M. N.; Raddum, H.: A Practical Adaptive Key Recovery Attack on the LGM (GSW-like) Cryptosystem. In (Cheon, J. H.; Tillich, J.-P., eds.): Post-Quantum Cryptography. Springer International Publishing, Cham, pp. 483–498, 2021, ISBN: 978-3-030-81293-5.

[Fl20] Fluhrer, S.; Kampanakis, P.; McGrew, D.; Smyslov, V.: Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security, June 2020, URL: `https://rfc-editor.org/rfc/rfc8784.txt`.

[FLP14] Fischlin, M.; Lehmann, A.; Pietrzak, K.: Robust Multi-Property Combiners for Hash Functions. en, Journal of Cryptology 27/3, pp. 397–428, July 2014, ISSN: 0933-2790, 1432-1378, URL: `http://link.springer.com/10.1007/s00145-013-9148-7`, visited on: 03/12/2020.

[Fo20] Fouque, P.-A.: Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU Specification v1.2./, Jan. 2020, URL: `https://falcon-sign.info/falcon.pdf`.

[Fo21] Fouque, P.-A.; Gérard, F.; Rossi, M.; Yu, Y.: Zalcon: an alternative FPA-free NTRU sampler for Falcon, 2021, URL: `https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/yang-zalcon-pqc2021.pdf`, visited on: 07/23/2021.

[Fu18] Fujioka, A.; Takashima, K.; Terada, S.; Yoneyama, K.: Supersingular Isogeny Diffie-Hellman Authenticated Key Exchange, Published: Cryptology ePrint Archive, Report 2018/730, 2018.

[Ga18] Gaj, K.: Challenges and Rewards of Implementing and Benchmarking Post-Quantum Cryptography in Hardware. In: Proceedings of the 2018 on Great Lakes Symposium on VLSI. ACM, Chicago IL USA, pp. 359–364, May 2018, ISBN: 978-1-4503-5724-1, URL: `https://dl.acm.org/doi/10.1145/3194554.3194615`, visited on: 01/17/2021.

[GAB19] Grote, O.; Ahrens, A.; Benavente-Peces, C.: A Review of Post-quantum Cryptography and Crypto-agility Strategies. In: 2019 International Interdisciplinary PhD Workshop (IIPhDW). IEEE, Wismar, Germany, pp. 115–120, May 2019, ISBN: 978-1-72810-423-2, URL: `https://ieeexplore.ieee.org/document/8755433/`, visited on: 07/20/2021.

[GFL19] Gazdag, S.-L.; Friedl, M.; Loebenberger, D.: Post-Quantum Software Updates. en,/, ISBN: 9783885796886 Publisher: Gesellschaft für Informatik e.V., 2019, ISSN: 1617-5468, URL: `http://dl.gi.de/handle/20.500.12116/25014`, visited on: 07/18/2021.

[GKS20] Gagliardoni, T.; Krämer, J.; Struck, P.: Quantum indistinguishability for public key encryption. arXiv preprint arXiv:2003.00578/, 2020.

[GMP21] Grubbs, P.; Maram, V.; Paterson, K. G.: Anonymous, Robust Post-Quantum Public Key Encryption, Published: Cryptology ePrint Archive, Report 2021/708, 2021.

[Go21] Gonzalez, R.; Hülsing, A.; Kannwischer, M. J.; Krämer, J.; Lange, T.; Stöttinger, M.; Waitz, E.; Wiggers, T.; Yang, B.-Y.: Verifying Post-Quantum Signatures in 8 kB of RAM, Published: Cryptology ePrint Archive, Report 2021/662, 2021.

[Gr16] Groot Bruinderink, L.; Hülsing, A.; Lange, T.; Yarom, Y.: Flush, Gauss, and Reload – A Cache Attack on the BLISS Lattice-Based Signature Scheme. In (Gierlichs, B.; Poschmann, A. Y., eds.): Cryptographic Hardware and Embedded Systems – CHES 2016. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, pp. 323–345, 2016, ISBN: 978-3-662-53140-2.

[Gr96] Grover, L. K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96. ACM Press, Philadelphia, Pennsylvania, United States, pp. 212–219, 1996, ISBN: 978-0-89791-785-8, URL: http://portal.acm.org/citation.cfm?doid=237814.237866, visited on: 07/16/2021.

[GSE20] Gellersen, T.; Seker, O.; Eisenbarth, T.: Differential Power Analysis of the Picnic Signature Scheme. IACR Cryptol. ePrint Arch. 2020/, p. 267, 2020.

[He19a] Heesch, M. v.; Adrichem, N. v.; Attema, T.; Veugen, T.: Towards Quantum-Safe VPNs and Internet, Published: Cryptology ePrint Archive, Report 2019/1277, 2019.

[He19b] Heider, T.: Towards a Verifiably SecureQuantum-Resistant Key Exchangein IKEv2, PhD thesis, Ludwig-Maximilians-Universität München, Oct. 2019, URL: https://www.nm.ifi.lmu.de/pub/Diplomarbeiten/heid19/PDF-Version/heid19.pdf, visited on: 07/14/2021.

[He21a] Heinz, D.; Kannwischer, M. J.; Land, G.; Schwabe, P.; Sprenkels, D.: First-Order Masked Kyber on ARM Cortex-M4, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/heinz-first-order-pqc2021.pdf, visited on: 07/23/2021.

[He21b] Hemmert, D. T.; Lochter, M.; Loebenberger, D.; Margraf, Marian; Reinhardt, S.; Sigl, G.: Quantencomputerresistente Kryptografie: Aktuelle Aktivitäten und Fragestellungen. In: Tagungsband zum 17. Deutschen IT-Sicherheitskongress. SecuMedia Verlag, Ingelheim, Germany, German Federal Office for Information Security (BSI), pp. 367–380, Feb. 2021.

[HKP21] Hutchinson, A.; Karabina, K.; Pereira, G.: Memory Optimization Techniques for Computing Discrete Logarithms in Compressed SIKE. IACR Cryptol. ePrint Arch. 2021/, p. 368, 2021.

[HKW21] Hagemeier, D. H.; Kousidis, D. S.; Wunderer, D. T.: Standardisierung von Post-Quanten-Kryptografie und Empfehlungen des BSI. In: Tagungsband zum 17. Deutschen IT-Sicherheitskongress. SecuMedia Verlag, Ingelheim, Germany, German Federal Office for Information Security (BSI), pp. 382–294, Feb. 2021, ISBN: 978-3-922746-83-6.

[HLX21] He, P.; Lee, C.-Y.; Xie, J.: Compact Coprocessor for KEM Saber: Novel Scalable Matrix Originated Processing, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/xie-compact-coprocessor-pqc2021.pdf, visited on: 07/23/2021.

[Ho20] Howe, J.; Prest, T.; Ricosset, T.; Rossi, M.: Isochronous Gaussian Sampling: From Inception to Implementation. In: PQCrypto. Pp. 53–71, 2020.

[Hü17] Hülsing, A.; Rijneveld, J.; Schanck, J.; Schwabe, P.: High-Speed Key Encapsulation from NTRU. In (Fischer, W.; Homma, N., eds.): Cryptographic Hardware and Embedded Systems – CHES 2017. Springer International Publishing, Cham, pp. 232–252, 2017, ISBN: 978-3-319-66787-4.

[Hu18] Huelsing, A.; Butin, D.; Gazdag, S.-L.; Rijneveld, J.; Mohaisen, A.: XMSS: eXtended Merkle Signature Scheme, Issue: 8391 Num Pages: 74 Series: Request for Comments Published: RFC 8391, May 2018, URL: https://rfc-editor.org/rfc/rfc8391.txt.

[Hü20] Hülsing, A.; Ning, K.-C.; Schwabe, P.; Weber, F.; Zimmermann, P. R.: Post-quantum WireGuard, Published: Cryptology ePrint Archive, Report 2020/379, 2020.

[Jo21] Jonathan Bradbury, B. H.: Fast Quantum-Safe Cryptography on IBM Z, Conference Name: Third PQC Standardization Conference, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/hess-fast-quantum-safe-pqc2021.pdf, visited on: 07/23/2021.

[JS19] Jaques, S.; Schanck, J. M.: Quantum Cryptanalysis in the RAM Model: Claw-Finding Attacks on SIKE. In (Boldyreva, A.; Micciancio, D., eds.): Advances in Cryptology – CRYPTO 2019. Vol. 11692, Series Title: Lecture Notes in Computer Science, Springer International Publishing, Cham, pp. 32–61, 2019, ISBN: 978-3-030-26947-0 978-3-030-26948-7, URL: http://link.springer.com/10.1007/978-3-030-26948-7_2, visited on: 11/16/2020.

[Ju21] Julien, D.; Kathrin, H.; Eike, K.; Vadim, L.; Gregor, S.: Faster Kyber and Saber via a Generic Fujisaki-Okamoto Transform for Multi-User Security in the QROM, Conference Name: Third PQC Standardization Conference, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/duman-faster-kyber-pqc2021.pdf, visited on: 07/23/2021.

[Ka18a] Kampanakis, P.; Panburana, P.; Daw, E.; Geest, D. V.: The Viability of Post-quantum X.509 Certificates, tech. rep. 063, 2018, URL: http://eprint.iacr.org/2018/063, visited on: 03/10/2020.

[Ka18b] Kannwischer, M. J.; Genêt, A.; Butin, D.; Krämer, J.; Buchmann, J.: Differential Power Analysis of XMSS and SPHINCS. In (Fan, J.; Gierlichs, B., eds.): Constructive Side-Channel Analysis and Secure Design. Vol. 10815, Series Title: Lecture Notes in Computer Science, Springer International Publishing, Cham, pp. 168–188, 2018, ISBN: 978-3-319-89640-3 978-3-319-89641-0, URL: http://link.springer.com/10.1007/978-3-319-89641-0_10, visited on: 08/26/2020.

[Ka19] Kannwischer, M. J.; Rijneveld, J.; Schwabe, P.; Stoffelen, K.: pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4. Published: Cryptology ePrint Archive, Report 2019/844, 2019.

[Ka20] Kampanakis, P.; Steblia, D.; Friedl, M.; Hansen, T.; Sikeridis, D.: Post-quantum public key algorithms for the Secure Shell (SSH) protocol, Internet-Draft draft-kampanakis-curdle-pq-ssh-00, Backup Publisher: Internet Engineering Task Force Num Pages: 13, Internet Engineering Task Force, Oct. 2020, URL: https://datatracker.ietf.org/doc/html/draft-kampanakis-curdle-pq-ssh-00.

[KAK18] Koziel, B.; Azarderakhsh, R.; Kermani, M. M.: A High-Performance and Scalable Hardware Architecture for Isogeny-Based Cryptography. IEEE Transactions on Computers 67/11, pp. 1594–1609, Nov. 2018, ISSN: 1557-9956.

[Kh16] Khalid, A.; Howe, J.; Rafferty, C.; O'Neill, M.: Time-independent discrete Gaussian sampling for post-quantum cryptography. In: 2016 International Conference on Field-Programmable Technology (FPT). IEEE, Xi'an, China, pp. 241–244, Dec. 2016, ISBN: 978-1-5090-5602-6, URL: http://ieeexplore.ieee.org/document/7929543/, visited on: 07/20/2021.

[Kh18] Khalid, A.; Oder, T.; Valencia, F.; O' Neill, M.; Güneysu, T.; Regazzoni, F.: Physical Protection of Lattice-Based Cryptography: Challenges and Solutions. In: Proceedings of the 2018 on Great Lakes Symposium on VLSI. ACM, Chicago IL USA, pp. 365–370, May 2018, ISBN: 978-1-4503-5724-1, URL: https://dl.acm.org/doi/10.1145/3194554.3194616, visited on: 01/17/2021.

[KK18] Kiefer, F.; Kwiatkowski, K.: Hybrid ECDHE-SIDH Key Exchange for TLS, Internet-Draft draft-kiefer-tls-ecdhe-sidh-00, Backup Publisher: Internet Engineering Task Force Num Pages: 13, Internet Engineering Task Force, Nov. 2018, URL: https://datatracker.ietf.org/doc/html/draft-kiefer-tls-ecdhe-sidh-00.

[KKP20] Koteshwara, S.; Kumar, M.; Pattnaik, P.: Performance Optimization of Lattice Post-Quantum Cryptographic Algorithms on Many-Core Processors. In: 2020 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS). Pp. 223–225, Aug. 2020.

[KL19] Krämer, J.; Loiero, M.: Fault Attacks on UOV and Rainbow. In (Polian, I.; Stöttinger, M., eds.): Constructive Side-Channel Analysis and Secure Design. Vol. 11421, Series Title: Lecture Notes in Computer Science, Springer International Publishing, Cham, pp. 193–214, 2019, ISBN: 978-3-030-16349-5 978-3-030-16350-1, URL: http://link.springer.com/10.1007/978-3-030-16350-1_11, visited on: 11/20/2020.

[KL21] Kirshanova, E.; Laarhoven, T.: Lower bounds on lattice sieving and information set decoding, Published: Cryptology ePrint Archive, Report 2021/785, 2021.

[KNW18] Kreutzer, M.; Niederhagen, R.; Waidner, M.: Eberbacher Gespräch: Next Generation Crypto, de, Jan. 2018, URL: https://www.sit.fraunhofer.de/de/eberbach-crypto/, visited on: 07/17/2021.

[Ko17] Koziel, B.; Azarderakhsh, R.; Mozaffari Kermani, M.; Jao, D.: Post-Quantum Cryptography on FPGA Based on Isogenies on Elliptic Curves. IEEE Transactions on Circuits and Systems I: Regular Papers 64/1, pp. 86–99, Jan. 2017, ISSN: 1558-0806.

[KP21] Kutas, P.; Petit, C.: Torsion point attacks on "SIDH-like" cryptosystems, Conference Name: Third PQC Standardization Conference Place: Birmingham, Bruxelles, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/kutas-torsion-point-pqc2021.pdf, visited on: 07/23/2021.

[KPP20] Kannwischer, M. J.; Pessl, P.; Primas, R.: Single-Trace Attacks on Keccak. IACR Transactions on Cryptographic Hardware and Embedded Systems/, pp. 243–268, June 2020, ISSN: 2569-2925, URL: https://tches.iacr.org/index.php/TCHES/article/view/8590, visited on: 02/10/2021.

[KS19] Kampanakis, P.; Sikeridis, D.: Two PQ Signature Use-cases: Non-issues, challenges and potential solutions, tech. rep. 1276, 2019, URL: https://eprint.iacr.org/2019/1276, visited on: 04/02/2020.

[KS20] Krämer, J.; Struck, P.: Encryption Schemes Using Random Oracles: From Classical to Post-Quantum Security. In: PQCrypto. Pp. 539–558, 2020.

[Ku17] Kuo, P.-C.; Li, W.-D.; Chen, Y.-W.; Hsu, Y.-C.; Peng, B.-Y.; Cheng, C.-M.; Yang, B.-Y.: High Performance Post-Quantum Key Exchange on FPGAs, tech. rep. 690, 2017, URL: https://eprint.iacr.org/2017/690, visited on: 04/03/2020.

[Ku20a] Kumar, V. B. Y.; Gupta, N.; Chattopadhyay, A.; Kasper, M.; Krauß, C.; Niederhagen, R.: Post-Quantum Secure Boot. In: 2020 Design, Automation Test in Europe Conference Exhibition (DATE). Pp. 1582–1585, 2020.

[Ku20b] Kuznetsov, A.; Kiian, A.; Smirnov, O.; Cherep, A.; Kanabekova, M.; Chepurko, I.: Testing of Code-Based Pseudorandom Number Generators for Post-Quantum Application. In: 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT). Pp. 172–177, 2020.

[KV19] Kwiatkowski, K.; Valenta, L.: The TLS Post-Quantum Experiment, en, Oct. 2019, URL: https://blog.cloudflare.com/the-tls-post-quantum-experiment/, visited on: 04/06/2020.

[Kw19] Kwiatkowski, K.; Sullivan, N.; Langley, A.; Levin, D.; Mislove, A.: Measuring TLS key exchange with post-quantum KEM. In: Workshop Record of the Second PQC Standardization Conference. https://csrc. nist. gov/CSRC/media/Events/Second-PQC-Standardization-Conference/documents/accepted-papers/kwiatkowski-measuring-tls. pdf. 2019.

[La16] Langley, A.: ImperialViolet - CECPQ1 results, Nov. 2016, URL: https://www.imperialviolet.org/2016/11/28/cecpq1.html, visited on: 06/26/2020.

[LSH20] Lee, S.; Shin, Y.; Hur, J.: Return of version downgrade attack in the era of TLS 1.3. In: Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies. ACM, Barcelona Spain, pp. 157–168, Nov. 2020, ISBN: 978-1-4503-7948-9, URL: https://dl.acm.org/doi/10.1145/3386367.3431310, visited on: 02/23/2021.

[Ma20] Mayes, K.: Performance Evaluation and Optimisation for Kyber on the MULTOS IoT Trust-Anchor. In: 2020 IEEE International Conference on Smart Internet of Things (SmartIoT). Pp. 1–8, Aug. 2020.

[MAY21] Mathilde, R.; Aymeric, G.; Yolan, R.: PQ-WireGuard: we did it again, Conference Name: Third PQC Standardization Conference, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/raynal-pq-wireguard-pqc2021.pdf, visited on: 07/23/2021.

[Mc16] McGrew, D.; Kampanakis, P.; Fluhrer, S.; Gazdag, S.-L.; Butin, D.; Buchmann, J.: State Management for Hash-Based Signatures. In (Chen, L.; McGrew, D.; Mitchell, C., eds.): Security Standardisation Research. Springer International Publishing, Cham, pp. 244–260, 2016, ISBN: 978-3-319-49100-4.

[MCF19] McGrew, D.; Curcio, M.; Fluhrer, S.: Leighton-Micali Hash-Based Signatures, Issue: 8554 Num Pages: 61 Series: Request for Comments Published: RFC 8554, Apr. 2019, URL: https://rfc-editor.org/rfc/rfc8554.txt.

[Mi21] Michael, B.; Vlad, G.; Basil, H.; Christian, P.; John, S.; Douglas, S.; Goutam, T.: Updates from the Open Quantum Safe Project, Conference Name: Third PQC Standardization Conference, Apr. 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/schanck-open-quantum-safe-project-pqc2021.pdf, visited on: 07/23/2021.

[MK19] Marzougui, S.; Krämer, J.: Post-Quantum Cryptography in Embedded Systems. In: Proceedings of the 14th International Conference on Availability, Reliability and Security. ACM, Canterbury CA United Kingdom, pp. 1–7, Aug. 2019, ISBN: 978-1-4503-7164-3, URL: https://dl.acm.org/doi/10.1145/3339252.3341475, visited on: 07/18/2021.

[Mo15] Mosca, M.: Cybersecurity in an era with quantum computers: will we be ready?, Published: Cryptology ePrint Archive, Report 2015/1075, 2015.

[Mo20] Moody, D.; Alagic, G.; Apon, D. C.; Cooper, D. A.; Dang, Q. H.; Kelsey, J. M.; Liu, Y.-K.; Miller, C. A.; Peralta, R. C.; Perlner, R. A.; Robinson, A. Y.; Smith-Tone, D. C.; Alperin-Sheriff, J.: Status report on the second round of the NIST post-quantum cryptography standardization process, tech. rep. NIST IR 8309, Gaithersburg, MD: National Institute of Standards and Technology, July 2020, NIST IR 8309, URL: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf, visited on: 01/17/2021.

[Mü20] Müller, M.; de Jong, J.; van Heesch, M.; Overeinder, B.; van Rijswijk-Deij, R.: Retrofitting post-quantum cryptography in internet protocols: a case study of DNSSEC. en, ACM SIGCOMM Computer Communication Review 50/4, pp. 49–57, Oct. 2020, ISSN: 0146-4833, URL: https://dl.acm.org/doi/10.1145/3431832.3431838, visited on: 01/17/2021.

[Ne19] Nejatollahi, H.; Dutt, N.; Ray, S.; Regazzoni, F.; Banerjee, I.; Cammarota, R.: Post-Quantum Lattice-Based Cryptography Implementations: A Survey. ACM Computing Surveys 51/6, Jan. 2019, URL: https://doi.org/10.1145/3292548, visited on: 04/02/2020.

[Ng21] Nguyen, P. Q.: Boosting the Hybrid Attack on NTRU: Torus LSH, Permuted HNF and Boxed Sphere, Conference Name: Third PQC Standardization Conference, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/nguyen-boosting-hybridboost-pqc2021.pdf, visited on: 07/23/2021.

[NI16] NIST: Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process, Dec. 2016, URL: https://csrc.nist.rip/groups/ST/post-quantum-crypto/documents/call-for-proposals-final-dec-2016.pdf, visited on: 07/19/2021.

[Ni21] Nina, B.; Sarah, M.; Hanif, R.; Geoff, T.: Suitability of 3rd Round Signature Candidates for Vehicle-to-Vehicle Communication –Extended Abstract, Conference Name: Third PQC Standardization Conference, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/bindel-suitability-abstract-pqc2021.pdf, visited on: 07/23/2021.

[NW17] Niederhagen, R.; Waidner, M.: Practical Post-Quantum Cryptography. Fraunhofer SIT, 2017.

[OP19] Ott, D.; Peikert, C.; participants other workshop, o. w.: Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility. arXiv:1909.07353 [cs]/, arXiv: 1909.07353, Sept. 2019, URL: http://arxiv.org/abs/1909.07353, visited on: 02/06/2020.

[OP20] Ounsworth, M.; Pala, M.: Composite Keys and Signatures For Use In Internet PKI, Internet-Draft draft-ounsworth-pq-composite-sigs-03, Backup Publisher: Internet Engineering Task Force Num Pages: 18, Internet Engineering Task Force, July 2020, URL: https://datatracker.ietf.org/doc/html/draft-ounsworth-pq-composite-sigs-03.

[ØSV21] Øygarden, M.; Smith-Tone, D.; Verbel, J.: On the Effect of Projection on Rank Attacks in Multivariate Cryptography, Published: Cryptology ePrint Archive, Report 2021/655, 2021.

[Pa18] Park, A.; Shim, K.-A.; Koo, N.; Han, D.-G.: Side-Channel Attacks on Post-Quantum Signature Schemes based on Multivariate Quadratic Equations. en, IACR Transactions on Cryptographic Hardware and Embedded Systems/, pp. 500–523, Aug. 2018, ISSN: 2569-2925, URL: https://tches.iacr.org/index.php/TCHES/article/view/7284, visited on: 09/25/2020.

[Pe20] Petzoldt, A.: Efficient key generation for rainbow. In: International Conference on Post-Quantum Cryptography. Springer, pp. 92–107, 2020.

[Pr21] Prasanna, R.; Martianus Frederic, E.; Shivam, B.; Anupam, C.; Sujoy Sinha, R.: On Generic Side-Channel Assisted Chosen Ciphertext Attacks on Lattice-based PKE/KEMs, Conference Name: Third PQC Standardization Conference, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/ravi-generic-side-channel-pqc2021.pdf, visited on: 07/23/2021.

[PS13] Perlner, R.; Smith-Tone, D.: A Classification of Differential Invariants for Multivariate Post-quantum Cryptosystems. In (Hutchison, D.; Kanade, T.; Kittler, J.; Kleinberg, J. M.; Mattern, F.; Mitchell, J. C.; Naor, M.; Nierstrasz, O.; Pandu Rangan, C.; Steffen, B.; Sudan, M.; Terzopoulos, D.; Tygar, D.; Vardi, M. Y.; Weikum, G.; Gaborit, P., eds.): Post-Quantum Cryptography. Vol. 7932, Series Title: Lecture Notes in Computer Science, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 165–173, 2013, ISBN: 978-3-642-38615-2 978-3-642-38616-9, URL: http://link.springer.com/10.1007/978-3-642-38616-9_11, visited on: 11/16/2020.

[PS20] Paul, S.; Scheible, P.: Towards Post-Quantum Security for Cyber-Physical Systems: Integrating PQC into Industrial M2M Communication. In (Chen, L.; Li, N.; Liang, K.; Schneider, S., eds.): Computer Security – ESORICS 2020. Vol. 12309, Series Title: Lecture Notes in Computer Science, Springer International Publishing, Cham, pp. 295–316, 2020, ISBN: 978-3-030-59012-3 978-3-030-59013-0, URL: http://link.springer.com/10.1007/978-3-030-59013-0_15, visited on: 10/01/2020.

[PST19] Paquin, C.; Stebila, D.; Tamvada, G.: Benchmarking Post-Quantum Cryptography in TLS, tech. rep. 1447, 2019, URL: http://eprint.iacr.org/2019/1447, visited on: 09/18/2020.

[Qu21] QuantiCor: Sicherheitsrisiko Quantencomputer, 2021, URL: https://quanticor-security.de/whitepaper/, visited on: 07/21/2021.

[Ri21] Ribeiro, L. A. D. S.; da Silva Lima, J. P.; de Queiroz, R. J. G. B.; Chagas, A. B.; Quintino, J. P.; da Silva, F. Q. B.; Santos, A. L. M.; Ribeiro, J. R. J.: Saber Post-Quantum Key Encapsulation Mechanism (KEM): Evaluating Performance in Mobile Devices and Suggesting Some Improvements, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/ribeiro-saber-pq-key-pqc2021.pdf, visited on: 07/23/2021.

[Sa19] Samardjiska, S.; Santini, P.; Persichetti, E.; Banegas, G.: A Reaction Attack Against Cryptosystems Based on LRPC Codes. In (Schwabe, P.; Thériault, N., eds.): Progress in Cryptology – LATINCRYPT 2019. Springer International Publishing, Cham, pp. 197–216, 2019, ISBN: 978-3-030-30530-7, URL: https://link.springer.com/chapter/10.1007/978-3-030-30530-7_10.

[Sa20] Santoso, B.: Generalization of Isomorphism of Polynomials with Two Secrets and Its Application to Public Key Encryption. In: International Conference on Post-Quantum Cryptography. Springer, pp. 340–359, 2020.

[SFG20] Stebila, D.; Fluhrer, S.; Gueron, S.: Internet-Draft: Hybrid key exchange in TLS 1.3, Feb. 2020, URL: https://tools.ietf.org/id/draft-stebila-tls-hybrid-design-03.html.

[Sh97] Shor, P. W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. en, SIAM Journal on Computing 26/5, pp. 1484–1509, Oct. 1997, ISSN: 0097-5397, 1095-7111, URL: http://epubs.siam.org/doi/10.1137/S0097539795293172, visited on: 07/16/2021.

[Si21] da Silva Lima, J. P.; Ribeiro, L. A. D. S.; de Queiroz, R. J. G. B.; Quintino, J. P.; da Silva, F. Q. B.; Santos, A. L. M.; José, R.: Evaluating Kyber post-quantum KEM in a mobile application, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/ribeiro-evaluating-kyber-pqc2021.pdf, visited on: 07/23/2021.

[SKD20a] Sikeridis, D.; Kampanakis, P.; Devetsikiotis, M.: Assessing the Overhead of Post-Quantum Cryptography in TLS 1.3 and SSH. In: Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies. CoNEXT '20, event-place: Barcelona, Spain, Association for Computing Machinery, New York, NY, USA, pp. 149–156, 2020, ISBN: 978-1-4503-7948-9, URL: https://doi.org/10.1145/3386367.3431305.

[SKD20b] Sikeridis, D.; Kampanakis, P.; Devetsikiotis, M.: Post-Quantum Authentication in TLS 1.3: A Performance Study, tech. rep. 071, 2020, URL: http://eprint.iacr.org/2020/071, visited on: 03/10/2020.

[SM16] Stebila, D.; Mosca, M.: Post-quantum Key Exchange for the Internet and the Open Quantum Safe Project. In (Avanzi, R.; Heys, H., eds.): Selected Areas in Cryptography – SAC 2016. Lecture Notes in Computer Science, https://github.com/open-quantum-safe/liboqs, Springer International Publishing, Cham, pp. 14–37, 2016, ISBN: 978-3-319-69453-5.

[Sm21] Smyslov, V.: Intermediate Exchange in the IKEv2 Protocol, Internet-Draft draft-ietf-ipsecme-ikev2-intermediate-06, Backup Publisher: Internet Engineering Task Force Num Pages: 11, Internet Engineering Task Force, Mar. 2021, URL: https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-ikev2-intermediate-06.

[SS17] Schanck, J. M.; Stebila, D.: A Transport Layer Security (TLS) Extension For Establishing An Additional Shared Secret, Internet-Draft draft-schanck-tls-additional-keyshare-00, Backup Publisher: Internet Engineering Task Force Num Pages: 10, Internet Engineering Task Force, Apr. 2017, URL: https://datatracker.ietf.org/doc/html/draft-schanck-tls-additional-keyshare-00.

[Su20] Suhail, S.; Hussain, R.; Khan, A.; Hong, C. S.: On the Role of Hash-based Signatures in Quantum-Safe Internet of Things: Current Solutions and Future Directions. IEEE Internet of Things Journal 8/1, pp. 1–17, Apr. 2020, URL: https://ieeexplore.ieee.org/document/9152977, visited on: 08/12/2020.

[SV20] Smith-Tone, D.; Verbel, J. A.: A Rank Attack Against Extension Field Cancellation. In: PQCrypto. Pp. 381–401, 2020.

[SWZ16] Schanck, J. M.; Whyte, W.; Zhang, Z.: Quantum-Safe Hybrid (QSH) Ciphersuite for Transport Layer Security (TLS) version 1.2, Internet-Draft draft-whyte-qsh-tls12-02, Backup Publisher: Internet Engineering Task Force Num Pages: 19, Internet Engineering Task Force, July 2016, URL: https://datatracker.ietf.org/doc/html/draft-whyte-qsh-tls12-02.

[Ta21] Tasso, É.; De Feo, L.; El Mrabet, N.; Pontié, S.: Resistance of Isogeny-Based Cryptographic Implementations to a Fault Attack. In: Constructive Side-Channel Analysis and Secure Design (COSADE) 2021. Lugano, Switzerland, Oct. 2021, URL: https://hal-cea.archives-ouvertes.fr/cea-03266892.

[Te21] Tendayi, K.; Michael, F.; Tristen, T.; Alexander, N.; David, A.; Miaoqing, H.: Power-based Side Channel Attack Analysis on PQC Algorithms, Conference Name: Third PQC Standardization Conference, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/kamucheka-power-based-pqc2021.pdf, visited on: 07/23/2021.

[Th21] Thomas, E.; Akira, T.; Mehdi, T.; Alexandre, W.: Mitaka: A Simpler, Parallelizable, Maskable Variant of Falcon, Conference Name: Third PQC Standardization Conference, 2021, URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/espitau-mitaka-pqc2021.pdf, visited on: 07/23/2021.

[Tj19] Tjhai, C.; Tomlinson, M.; grbartle@cisco.com; Fluhrer, S.; Geest, D. V.; Garcia-Morchon, O.; Smyslov, V.: Framework to Integrate Post-quantum Key Exchanges into Internet Key Exchange Protocol Version 2 (IKEv2), Internet-Draft draft-tjhai-ipsecme-hybrid-qske-ikev2-04, Backup Publisher: Internet Engineering Task Force Num Pages: 21, Internet Engineering Task Force, July 2019, URL: https://datatracker.ietf.org/doc/html/draft-tjhai-ipsecme-hybrid-qske-ikev2-04.

[TLW19] Tian, J.; Lin, J.; Wang, Z.: Ultra-Fast Modular Multiplication Implementation for Isogeny-Based Post-Quantum Cryptography. In: 2019 IEEE International Workshop on Signal Processing Systems (SiPS). ISSN: 2374-7390, pp. 97–102, Oct. 2019.

[TPD21] Tao, C.; Petzoldt, A.; Ding, J.: Efficient Key Recovery for all HFE Signature Variants. In. Springer-Verlag, 2021.

[We20] Weller, D. L.: Incorporating post-quantum cryptography in a microservice environment. en,/, p. 36, Feb. 2020.

[Wh17] Whyte, W.; Zhang, Z.; Fluhrer, S.; Garcia-Morchon, O.: Internet-Draft: Quantum-Safe Hybrid (QSH) Key Exchange for Transport Layer Security (TLS) version 1.3, Oct. 2017, URL: https://tools.ietf.org/html/draft-whyte-qsh-tls13-06.

[WS20] Wang, W.; Stöttinger, M.: Post-Quantum Secure Architectures for Automotive Hardware Secure Modules, tech. rep. 026, 2020, URL: `https://eprint.iacr.org/2020/026`, visited on: 05/14/2021.

[YWT20] Yasuda, T.; Wang, Y.; Takagi, T.: Multivariate Encryption Schemes Based on Polynomial Equations over Real Numbers. In: PQCrypto. Pp. 402–421, 2020.

[Za20] Zaverucha, G.: The Picnic Signature Algorithm Specification. NIST Round 3/, Apr. 2020, URL: `https://github.com/microsoft/Picnic/blob/master/spec/spec-v3.0.pdf`.

[ZGF20] Zoni, D.; Galimberti, A.; Fornaciari, W.: Efficient and Scalable FPGA-Oriented Design of QC-LDPC Bit-Flipping Decoders for Post-Quantum Cryptography. IEEE Access 8/, pp. 163419–163433, 2020.

[Zh20a] Zhang, C.; Liu, Z.; Chen, Y.; Lu, J.; Liu, D.: A Flexible and Generic Gaussian Sampler With Power Side-Channel Countermeasures for Quantum-Secure Internet of Things. IEEE Internet of Things Journal 7/9, Conference Name: IEEE Internet of Things Journal, pp. 8167–8177, Sept. 2020, ISSN: 2327-4662.

[Zh20b] Zhang, F.; Yang, B.; Dong, X.; Guilley, S.; Liu, Z.; He, W.; Zhang, F.; Ren, K.: Side-Channel Analysis and Countermeasure Design on ARM-based Quantum-Resistant SIKE. IEEE Transactions on Computers/, Conference Name: IEEE Transactions on Computers, pp. 1–1, 2020, ISSN: 1557-9956.

[Zi15] Zimmer, E.: Post-Quantum Kryptographie für IPsec, Feb. 2015, URL: `https://svs.informatik.uni-hamburg.de/publications/2015/2015-02-24-Zimmer-DFN-PQC-fuer-IPsec.pdf`, visited on: 07/14/2021.

[ZSS20] Zhao, R. K.; Steinfeld, R.; Sakzad, A.: COSAC: COmpact and Scalable Arbitrary-Centered Discrete Gaussian Sampling over Integers. In: PQCrypto. Pp. 284–303, 2020.

[ZWH21] Zeier, A.; Wiesmaier, A.; Heinemann, A.: Zur Integration von Post-Quantum Verfahren in bestehende Softwareprodukte. de, arXiv:2102.00157 [cs]/, arXiv: 2102.00157, Jan. 2021, URL: `http://arxiv.org/abs/2102.00157`, visited on: 03/15/2021.