Post-Quantum Security in Cyber-Physical Systems

Ole Knief
RWTH Aachen University
ole.knief@rwth-aachen.de

***Abstract*—Quantum computing is capable of breaking currently used cryptography schemes. In order to secure digital communication against attacks with quantum computers, the underlying cryptography schemes need to change, aiming for protection to such quantum attacks. Changes towards post-quantum secure alternatives come with trade-offs, which collide with restrictions in cyber-physical systems. This paper takes a look at state-of-the-art approaches implementing these post-quantum secure schemes in restricting environments while working around the restrictions. By categorizing the solutions into their underlying techniques, a trend towards key size and handshake reductions, as well as algorithmic speedups becomes apparent. The solutions promise opportunities to make the algorithms applicable in practice, by addressing different restrictions found in cyber-physical systems. Even tough multiple propositions exist, many are not comparable due to missing comparable metrics, creating a lack of consensus in this research field. Furthermore, current research does not take practical considerations into account, only approaching the research problem from a theoretical standpoint, which is not always appropriate.**

***Index Terms*—Cryptography, Quantum computing, Post-quantum, Cyber-physical systems, Real-time systems**

I. Introduction

Cyber-physical systems have become an essential part of the modern technology landscape and can be found in various different use cases. On a bigger scale, they serve as an essential building block for many physical processes which can be managed at least in part autonomously [1]. Practical applications include their integration into the operation technology in industrial production or control systems for critical infrastructure, ensure smooth operation of the physical system [1]. Going beyond the responsibilities of traditional information technology, cyber-physical systems can impact the physical world around them and therefore need to assure safety towards the process, as well as the people affected by them [2]. Consequently, the security of these systems needs to be thoroughly evaluated and implemented, in order to prevent unauthorized access, possibly resulting in harm of people by controlling the system in a dangerous manner or destroying essential equipment, such as inducing power outages by destroying power grids. Even tough different cyber-physical system have differing requirements as a consequence of their weighted security goals, availability as their top priority is a common denominator [3]. While integrity and authentication remain to be important security goals [4], they are commonly not implemented due to potential conflicts with strict requirements towards availability and latency [3]. Information that can be gained by listening to the communications in the networks can be of interest, however confidentiality is commonly the least important part of security assessments in these application areas [2].

Confidentiality, integrity, and authenticity can be achieved by commonly used cryptography schemes, offering services such as encryption, authentication, or integrity checks [1]. Schemes like this are based on multiple cryptographic primitives for different use cases [5]. The foundation of the cryptographic primitives is a mathematical problem statement, which is easily solvable in case the required secret is known, such as shared key, but not breakable since that would come with such high computation requirements, which are practically not feasible. Underlying the whole field of cryptography is the assumption, that no algorithm in existence can find a solution to these cryptographic primitives in polynomial time, without knowledge of the shared secret, such as a key [5]. It turns out, that even tough this assumption still holds up in practice, it can not be proven, that these algorithms do not exist [6], which falls back to the debate on complexity classes in the field of theoretical computer science, as part of the theory of computation [7].

Exactly this is where the innovation of quantum computing strikes security of digital communication critically. The advent of quantum computers and the theoretical algorithms they can execute, can break some mentioned cryptographic primitives in polynomial time [8]. Inevitably, all security measures affected by this development need to be exchanged for newly development algorithms, that are not susceptible to quantum specific attacks and hold up the promises of their security services even in the time of quantum computing. Post-quantum cryptography is the umbrella term for algorithms with the aforementioned properties [9], providing so-called post-quantum security.

However, this transition to post-quantum security might not be as straight forward for cyber-physical systems as other parts of digital technology. For the most part, the underlying digital components in cyber-physical systems tend to be heavily restricted, which turns out to be a great challenge to overcome [4].

Even tough the research field of post-quantum cryptography has seen a lot of attention over the last decade, this paper discusses how many solutions require high capabilities from the devices they secure and are therefore not fit for every use case scenario, especially in these restricted systems. Fortunately, different research teams have made an effort to make post-quantum cryptography available for all sorts of restricted systems.

The goal of this paper is to give a conclusive overview on how far the research field has come to achieve this goal and

discuss how the different approaches solve these challenges. In order to work towards a fully fledged understanding on how these approaches accomplish their tasks, this paper will introduce high level concepts of the quantum computing's relation to cryptography, the concepts behind post-quantum cryptography as well as giving an impression as to which device restrictions of cyber-physical systems need to be considered. With the required background knowledge in mind, this paper goes over multiple propositions found in current scientific literature regarding the introduction of post-quantum cryptography into cyber-physical systems and categorizes them in their approach. Moreover, this paper addresses which implementation challenges each approach category addresses and how these approaches solve the problems, the paper identifies. A final discussion about the coverage of the stated problem field by the presented solutions to post-quantum security in cyber-physical systems, as well as the identification of gaps in the literature, concludes the paper.

II. Post-Quantum Cryptography

In order to understand the necessity and impact of post-quantum cryptography for future security mechanisms, it is helpful to look at quantum computing on a high level and understand how the traditional encryption schemes differ from the new ones.

A. Quantum Computing Breaks Cryptography

Even tough the theoretical invention of the quantum computer was over 40 years ago [10], at this point in time no research group has come close to building a commercial grade quantum computer that is able to break traditional cryptography schemes. Experts in the field have vastly different opinions as to when this stage will finally be reached, but most agree on the fact that this point in time will certainly arise [11]. Since the inner workings of quantum computers are of extreme complexity, this brief overview on quantum computing should only help to grasp the fundamental concepts through a high level of abstraction in order to understand the implied threats to digital security, when such a computer exists in practice.

In contrast to classical computers, quantum computer operate on so-called quantum bits (qubits) instead of classical bits [12]. Due to their size of atomic scale, they are subject to quantum-physical properties, which allow new approaches to computation. Just like ordinary bits, qubits can represent the two basic states of computation, which are 0 and 1. Both can be measured at will and therefore behave like a classical computer. As an extension to this, qubits can utilize quantum mechanics to represent a third state, a superposition. In this case, the qubit represents both 0 and 1 at the same time, both with a respective probability with which they can be measured. It is important to note, that a measurement will always collapse the superposition and only ever yield one of the two states [12]. Quantum algorithms are transforming these qubits by changing the probabilities of the different states in a controlled manner and leverage the interference of different possible measurement results in order to compute solutions to problems, which were thought to be impossible to compute due to their complexity [8].

Some of these quantum algorithms are especially relevant regarding the threat to digital security. One of which is the algorithm proposed by Shor [13]. Many asymmetrical cryptography schemes, like asymmetrical encryption and especially authentication rely on the complexity of the integer factorization problem for primes or the discrete logarithm such as RSA and ECC [14]. In contrast to the classical approach for a solution to these problems, which are based on brute-forcing the exponential possible combinations, Shor's algorithm can compute the answers in polynomial time [8]. This behavior can be seen in Fig. 1, where the run time complexity of a pre-quantum factorization algorithm, namely the number field sieve algorithm, which is the most efficient way of implementing a brute-force approach to this problem [15], compares to that of Shor's algorithm.

Similarly, many symmetric cryptography schemes rely on the complexity of the exponential amount of possible keys which can be used. In his paper [16], Grover proposed a quantum algorithm which can reduce the complexity of the key search to its square root, essentially reducing the effective key length to its half [8]. The same algorithm can be used for weakening the complexity of cryptographic hash functions and therefore also threaten hash-based authentication, like some message-authentication codes [8], [9].

B. What is Different in Post-Quantum Cryptography

To fix the aforementioned underlying flaws of traditional cryptographic primitives, multiple research teams propose new algorithms to secure digital communication in the future. The following section gives an overview of the post-quantum algorithms properties and how they are different to classical algorithms. Additionally, the section goes over the application

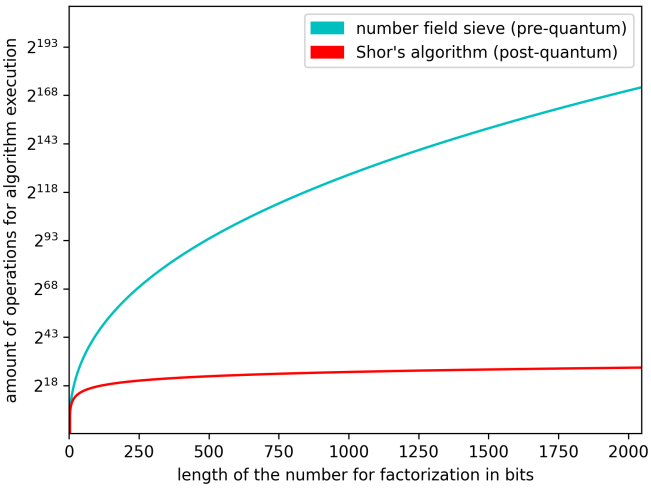

Fig. 1. A comparison of post-quantum and pre-quantum algorithm's runtime for factorization. While the number field sieve pre-quantum algorithm for brute-force runs in sub-exponential time [15], Shor's post-quantum algorithm has only polynomial time complexity [15].

areas for such algorithms, and how they relate to hybrid encryption schemes.

1) Algorithm Properties: The main difference between post-quantum and classical cryptography is the underlying problem, which introduces the complexity for a third party trying to insert itself into the communication. It needs to be assured, that implementing an algorithm, which might be able to compute a solution to the problem in polynomial time, remains impossible [9]. Since it can not be guaranteed, that it is impossible to create a new (quantum) algorithm, which may solve a problem in polynomial time, this assumption is impossible to prove definitively [6]. Still, there exist a number of problems, for which such an algorithm has not yet been found and are therefore fit for usage in post-quantum cryptography, all of which introduce a number of different properties for the cryptography scheme [6].

2) Application Areas: Post-quantum security will need to find application in any scenario, where traditional cryptography is will be affected, once a capable quantum computer exists. However, the impact on symmetric and asymmetric cryptography differs fundamentally. Since quantum computing only weakens the security of symmetric schemes instead of breaking it, security implementations can be secured by squaring the complexity, e.g., doubling the key length or substituting the scheme, such as for hash functions [8], [14]. The application for asymmetric schemes need to be considered more carefully. The amount of time a quantum computer needs for breaking an asymmetric scheme will decrease with technical improvements, but will remain in the spectrum of days or even weeks for the foreseeable future [17]. For example in systems which switch authentication certificates regularly, e.g., at least weekly, the system will still be considered secure, even if smaller quantum computer exist [14]. Even though this assumption will not hold in the long run where asymmetric systems based on the prior mentioned complexity problems will need to be substituted, it may be considered for the near future. Moreover, the future existence of capable quantum computers will enable adversaries to store encrypted messages, which are currently sent in networks and decrypt them later on with such a quantum computer, breaking future confidentiality [18], [19].

3) Hybrid Schemes: The migration to new cryptography schemes is not an endeavor without risks. On one hand, as mentioned before, it can not be proven that a newly proposed post-quantum algorithm is unbreakable. On the other hand, there could be fundamental implementation flaws in the algorithm, which has not yet stood the test of time, unlike the established traditional schemes [20], [21]. In order to solve this, different studies propose hybrid approaches, which are the conjunction of a post-quantum scheme and a traditional one. They ensure at least the current security level and the potential extra security of the post-quantum algorithm. It is important to note that hybrid schemes are essentially intended to be an intermediary step in the process of fully transitioning to post-quantum cryptography for all necessary communication [20], [21].

III. Implementation Challenges in Cyber-Physical Systems

Changing fundamental transmissions due to shifts in the utilized cryptography schemes can be a complex and challenging task. Many aspects need to be considered, which may result in a long integration process. Since cost is an important factor to consider for the planning of cyber-physical systems, cyber-physical systems must deal with several restrictions [1] regarding several factors. Due to the restrictiveness of cyber-physical systems across the board, the integration of new security measures into these systems turns out to be even more challenging [1]. In the following, we will discuss the challenges that come with post-quantum cryptography in cyber-physical systems, which need to be considered and worked around thoroughly, since they might conflict with a naive implementation of new security solutions. Tab. I summarizes the core consequences for cryptographic algorithms this section mentions.

A. General Requirements in Cyber-Physical Systems

Communication in cyber-physical system differs fundamentally from classical communication of typical IT systems. The differences are not only a consequence of the protocols which accomplish the communication, but arise from different expectations regarding the messages sent, as well as in the participating devices.

1) Support for Legacy Devices: In many cases, the devices which reside in cyber-physical systems are designed in a way, which enables them to last over long periods of time without failure [22]. This is especially true for complex systems, such as power grids [3]. The digital components of these systems are seldom exchanged for new equipment, since such a procedure would come with great financial implications, which is undesirable [1]. Moreover, exchanges of equipment will likely affect the availability of the respective system [22]. Age of devices is therefore an important aspect to consider

TABLE I
Restrictions in CPS

Restriction	Consequence for Cryptography
General Requirements	
Legacy Devices	Pre-quantum cryptography schemes need to be supported over many years in the future, for backwards compatibility
Message Timings	Cryptography schemes may not take too much time in order to not violate enforced deadlines for different message types
Hardware	
Computational Effort	Cryptography algorithm execution can be restricted or even impossible due to missing computational capabilities
Bandwidth	Great handshake sizes commonly found in post-quantum cryptography can not be transmitted
Auxiliary Modules	Hardware acceleration is oftentimes not available. Post-quantum algorithms that require them will perform drastically worse

when planing the implementation of post-quantum cryptography, in case they require modern features which might not be supported. This can become a major issue if only a set of system components can support the new cryptography schemes. It is essential that any component in the system retains support for traditional cryptography schemes in order to support communication with legacy devices [19], while simultaneously providing the required protection in a post-quantum world [9].

2) Timing Requirements: In contrast to IT systems, where the transmission time for most network traffic is not critical, this is not the case in many cyber-physical systems [2]. Since cryptographic algorithms do not only execute once but need to be applied to almost all messages send by a network device, such as for encryption and decryption of every message sent within a communication [5], a slight decrease in performance may significantly affect a communication exchange between devices. Increases in execution durations of these cryptographic algorithms might render its utilization impossible in time critical systems, such as in measurement communication in power grids. Its cause are precisely defined deadlines of measurements in these quickly changing physical processes, which might become useless for the control mechanisms if there is a transmission duration increase of mere milliseconds [2].

B. Hardware Restrictions

Since complex systems in the cyber-physical realm commonly consist of a variety of smaller subsystems, the digital components confined in these subsystems mainly handle smaller tasks and come with fitting device requirements. Most of the time, this implicates heavily resource constraint systems [1], which now need to be expanded in their security capabilities. Some of these new requirements might conflict with what these systems are able to provide.

1) Computational Effort: The devices in question mainly deal with the task they are intended to accomplish, such as reading measurements and applying input from control commands [23]. Any security measures which will be added upon these computationally expensive tasks need to be of less priority than the main task. Depending on the system, the room for this induced overhead can greatly differ, but in any case may not interfere with the main process. This constraint also demonstrates, that even the simplest solution to quantum computers breaking symmetrical cryptography can not be easily implemented, since doubling the key size for traditional cryptography schemes might not even be feasible for a vast amount of devices [23].

2) Bandwidth: The aforementioned resource constraints do not end with the computational capabilities based on processing and memory limitations, but also extend to the complex networks connecting the devices [1] and their connection to it. Sometimes the provided interface for the digital components, as well as the networks over which they communicate, only support transmission sizes for the communication pattern for which they were designed [19]. Cryptographic handshakes tend to be large by nature, transmitting information such as the required certificates. The restricted bandwidth can conflict with increasing cryptographic complexity, if cryptography certificate sizes need to increase, rendering the handshake transmission impossible [19].

3) Auxiliary Modules: Oftentimes, when evaluating the performance of different post-quantum cryptography schemes, involved parties make some technical assumptions about the devices. This can drastically influence the performance in case the devices which run the algorithms do not meet the assumptions, possibly rendering them useless for their purpose. A typical case for this are auxiliary modules for computation, which can do the heavy lifting of some post-quantum algorithms, that commonly exist on newer hardware [19], but not necessarily on older ones. The performance comparisons proposed by different papers, which are the first reference point for the schemes' applicability, need to be reviewed with caution and understanding of the devices capabilities.

C. The Fundamental Challenges

The challenges the Sections III-A and III-B mention impose restrictions, which need to be considered for new cryptography solutions applied in cyber-physical systems. Most of these challenges not typically found in IT systems and are therefore not necessarily considered for the broad application of new cryptography schemes [20]. It is essential to mention, that the types of devices in cyber-physical systems are plentiful, all of which come with their own combination of restrictions [1]. Regarding security, the kind of device restrictions for an individual device are a subset of the restrictions mentioned in the sections prior. Each of these device restrictions pose different needs for post-quantum cryptography, which need to be addressed.

IV. Solutions and new Approaches

In order to address the missing consideration of cyber-physical system in the classical discussion of post-quantum cryptography [20], multiple newer research proposals tackle the challenges discussed in Section III. In the following section, we first take a look at how post-quantum security can generally be achieved with the help of state-of-the-art cryptography solutions, firstly discussing the computational problems and secondly how respective post-quantum algorithms implement them. Afterwards, we discuss how modern research addresses the integration of the aforementioned algorithms as post-quantum security measures for highly restrictive systems, and their ideas for the algorithm implementation. Understanding the common ground between the researchers ideas and their differences grants the opportunity of judging the progress as a whole and identify subfield in this research environment not yet addressed.

A. The Common Foundation

Developing a post-quantum cryptography schemes is a complex task in general. The identification and implementation of algorithms that address the aforementioned properties

reliably, requires many experts of different field [6], while the development process oftentimes ends in finding a central error in the approach, leading to a fundamental restructuring of the algorithms. This was repeatedly seen in a competition started by the National Institute of Standards and Technology (NIST), where many research teams compete in order to work towards a standardized post-quantum security solution [24]. Throughout the competition, many proposed algorithms were either discarded due to lack of adequate performance compared to other competitor's solutions, or were subject to discovery of security flaws as mentioned above [25], such as with the SIKE algorithm [26]. It needs to be stated that most research teams developing an approach for integration of post-quantum security in restricted systems build on the algorithms proposed as part of the NIST competition. The researcher's contribution is mostly either changing the setting which utilizes the algorithm, in order to make them executable in the respective environment, or adapting aspect of the algorithm to make them fit the requirements. The following present these fundamental proposition which arise from the NIST competition and are therefore the central building blocks of the future stated solutions. Tab. II acts a summary of the information in this section, giving a high level overview of the different proposition's properties.

1) Computational Problems: As mentioned in the Section II, it is necessary to find mathematical problems which are easily verifiable but for which no known algorithm exists, that can find a solution in polynomial time without knowledge of the required secret. A handful of these problems exist and have seen a lot of attention for usage as cryptography primitives over the years.

One of the more commonly known alternatives are code-based encryption schemes. This scheme goes back to the original proposition made by McEliece to use error-code generators as public key systems in which carefully chosen errors can contain a message [9]. Even though Grover's algorithm affects this scheme, which therefore requires changes to its complexity [27], it is still a non-broken algorithm that is considered as a basis for post-quantum encryption. However, this scheme is suffering from high key sizes, minimizing the use cases. Proposed modifications to address this have ended up in significant security flaws and are therefore not recommendable [9].

Other cryptographic primitives often referred to are lattice-based encryption schemes. These public-key systems are a direct alternative to McEliece's proposition. In order to encode messages securely, a point is embedded in a high-dimensional lattice, which is essentially a high degree polynomial, just like the message [9]. The underlying complexity lies within the identification of the shortest or closest vector, both complex computational problems [23]. Even tough lattice-based encryption is seen as more efficient compared to McEliece, especially regarding key sizes, this alternative is comparatively new and has therefore not been tested as extensively. Due to the fact that issues have been discovered multiple times, the confidence in these schemes is not at the same level as for code-based ones [9]. Moreover, lattices have been incorporated into signatures as well, providing efficient computation times as well as key sizes similar to signatures based on RSA. At this time, these systems are still in development and suffer not only from implementation problems, but also algorithmic challenges [9].

One of the most straight forward ways to sign a message are hash based message authentication codes (HMACs) [28]. Unfortunately, since Grover's algorithm also affects them drastically, the naive implementation does not necessarily provide meaningful security anymore [29]. Post-quantum hash-based cryptography instead expands simple hash functions into Merkle signature schemes, allowing for single use signatures. In case of repetitive signatures, which utilizing the same secret, secrecy is threatened [9], [23]. The implied computational effort of the secrets' generation is one of the major downsides to this approach. Extending the security of hash-based schemes, multivariate-equation signatures enables signing messages with calculation over polynomials, enabling signatures with remarkably small sizes [9].

2) Presented Algorithms: Multiple research groups have concerned themselves with implementing the preceding options in a secure and efficient manner. As previously stated, many of these implementations have turned out to be flawed in one way or another and will therefore not be part of the discussion. Throughout the multiple round of NIST's competition, a handful of algorithms has proven themselves as top candidates for a future standardization [30], [31]. For encryption and key establishment purposes, code-based algorithms are in the majority. It is notable, that the Classic McEliece algorithm is still part of the selection, as well as two others, namely BIKE and HQC [30]. Both of these algorithms offer substantially smaller key sizes then Classic McEliece, however they can not compete in terms of cipher text sizes, which Classic McEliece keeps comparatively short. Nevertheless, all three algorithms showcase the inherent trade of between efficiency and security, rendering small security parameters, such as small key sizes and therefore little communication overhead, substantially more insecure than larger ones [32].

Only a single algorithm in the encryption category uses lattice-based primitives. CRYSTALS-Kyber offers a new post-quantum encryption scheme, outperforming the code-based competitors in key sizes, as well as computation times for the algorithms application and key generation [33]. Also based on lattice problems and part of the same family, CRYSTALS-Dilithium proposes an algorithm implementation for signatures. Even tough Dilithium can provide small key and signature sizes, its direct competitor, the Falcon algorithm, improves upon these aspects and excels at providing small signature sizes [34].

Lastly, SPHINCS+ provides a completely different approach to post-quantum secure signatures. This purely hash-based alternative does not rely on big keys, restricting them to merely 32 bytes. A great trade-off lies within the signature sizes, substantially greater than the lattice-based signature schemes [34].

TABLE II
POSSIBLE CRYPTOGRAPHY SCHEMES

Cryptography Scheme	Influence by Quantum Computing	Advantage	Disadvantage
Encryption			
Code based	Weakened by Grover	Short ciphertext	Great key sizes, inefficient computation
Lattice based	Unaffected	Small key sizes	Comparatively new, not as well tested
Signatures			
Lattice based	Unaffected	Efficient computation, small key sizes	Comparatively new, not as well tested
Hash based	Weakened by Grover	Well supported, efficient computation	Need for high complexity variation
Multivariate-equation	Unaffected	Small key sizes and signatures	Not well analyzed yet

One pattern emerges from this discussion: state-of-the-art algorithms implementing post-quantum security differ in their properties compared to traditional algorithms. This does not only refer to their security properties, such as their capabilities to secure communications from attack by quantum computers, but also affect performance properties, such as execution speed of algorithms or sizes of keys and ciphertexts. Since these property changes come with new requirements of the devices which utilize them, directly applying the algorithms to restricted devices in cyber-physical system can cause issues, if they violate restricting discussed in Section III. These circumstances necessitate the proposition of algorithms, that can integrate the aforementioned algorithms but fit them to cyber-physical systems.

B. Proposed Solutions

Translating these algorithms from the usage in the common Internet to cyber-physical systems with their restricted capabilities turns out to be difficult. The naive implementations of the aforementioned solutions tends to introduce different requirements compared to the security measures that are currently in place. Research in this field tries applying changes to the proposed algorithms in order to change newly imposed requirements, making the application for restricted systems possible [20]. Since this research field provides a vast amount of solutions, oftentimes referring to specific use cases, this paper discusses only a selection of approaches, with the main focus on providing a broad overview on how these goals can be generally achieved. The following will discuss a handful of propositions for each approach classification, which can generally be dissected into three categories. We start with a discussion of approaches for key size reductions, followed by propositions regarding handshake reduction. Lastly, approaches to algorithm speedups conclude this section. Tab. III summarizes all approaches contained in this section, giving an overview of the approaches, which of the cyber-physical restrictions they address and which consequence follow from their respective implementation.

1) Key size reduction: When considering the restrictions discussed in Section III, limitations in areas such as bandwidth can cause issues for solutions that require great key sizes [19]. In the discussion of algorithmic key sizes, this property needs to be seen in combination with other properties it influences. For example, as a generalized trend key sizes tend to inversely correlate with signature sizes for hash-based signature schemes [34]. Even tough there are some exceptions, it is a trend that exists at the extremes targeting the generation of either hash-based signatures or keys with sizes under or close to 100 bytes [34]. Another property regards the time it takes the algorithm to execute based on the key itself, since this also vastly differs [33]. A small key is not necessarily better, if the generation and application time is exceedingly greater. These three aspects are generally important to consider and are therefore subject to research proposals trying to reduce their resource requirements.

An important aspect to consider when talking key lengths, are the key lengths' correlation to security levels. Security algorithms are defined by their security levels, most often represented in the form of security bits. For an algorithm to be considered secure, it requires a security bit amount of at least 112, but generally 128 bits is the referenced amount [9], [41]. Increases of security bits for an algorithm will come with an increase of the key lengths [38]. As a comparison base, the RSA equivalent to a security level of 128 bits require key of length 3072 bits [41]. The impact of required security levels is one of the major drawbacks to the McEliece. To be specific, major issues with the McEliece cryptosystem for public key establishments are the key sizes [32], especially compared to other competitors and the computational inefficiency of the algorithm. In order to achieve the before mentioned security levels, key sizes increase dramatically [35]. To counteract this, Hashemi et al. [35] try to modify this encryption scheme, aiming for a reduction in key sizes. The standard approach for a McEliece implementation requires key length up to 6084 bits in order to achieve a security bit level of only 80 [35]. This new approach can reduce the key length to 4753, for the same security level of 80 bits [35]. This is a moderate reduction, but still far from practical key sizes for systems, that are restricted in ways mentioned in Section III, especially for more mature security levels. Generally speaking, a key size reduction is a risky endeavor for the aforementioned reasons and will always come with trade-offs, which need to be evaluated carefully, even tough it is still one of the aspects that can be adjusted for complexity reduction.

Yang et al. propose a similar lattice-based signature schemes [36]. This proposition addresses a new cryptography scheme in that realm. Based on carefully considered mathematical properties, the proposition achieves a great reduction not only in public and private key sizes, but also for the ciphertext length as well as computational cost. This is

TABLE III
PROPOSED SOLUTIONS FOR FITTING POST-QUANTUM SECURITY IN CYBER-PHYSICAL SYSTEMS

Proposition	Addressed Problems	Effect	Trade-off
Key Size Reduction			
Algorithmic change in McEliece [35]	• Computational Effort • Bandwidth	• Key sizes reduced by 1/3	• Still not small enough for many systems • Security levels are not high enough
Changing mathematical properties of lattice-based signatures [36]	• Computational Effort • Bandwidth	• Key sizes reduced • Smaller cipher text • Great scaling	• Missing large scale security evaluation
Reduction of either key or cipher text [21]	• Computational Effort • Bandwidth	• Great size reduction for a chosen property	• Other properties' sizes might increase
Handshake Reduction			
Naive implementation of NIST algorithms [19]	• Message Timings • Bandwidth	• Great speedup compared to RSA	• No support for legacy devices
Hybrid signature scheme based on RSA [19]	• Legacy Devices	• Support for legacy devices	• Introduces great overhead • Threatens message timings
Enabling variable frame sizes in TLS [14]	• Bandwidth	• Support large handshakes in post-quantum schemes	• Highly protocol dependent
Algorithmic Speedup			
Reimplementation of RSA [37]	• Legacy Devices • Computational Effort	• Only requires changes to an already supported protocol • No additional requirements	• Not one of the most efficient schemes
Reduction of redundant network [14] communication	• Bandwidth	• Frees resources useable for PQC Schemes	• Performance highly dependent of communication environment
Lightweight algorithm alternatives [38]	• Computational Effort	• Reduction of computation overhead	• Mostly only applicable to lower security levels
Custom assembly instruction set [39]	• Computational Effort • Auxiliary Modules	• Speedup of calculation steps common in PQC Schemes	• Not applicable to all PQC schemes
Mathematical optimization of cryptographic primitive calculation [40]	• Computational Effort	• Calculation speedups up to 80%	• Threat of introducing security flaws

especially apparent for larger security levels, which require massive scaling of the variables. These kinds of propositions will need to be carefully evaluated for their practical security levels in comparison to the commonly used ones, however they offer a theoretical approach to reducing implied overheads by a great margin.

Slightly differing from both previously mention proposals, not every study is trying to reduce multiple properties at the same time, but focus on one algorithmic property in combination with a specific restriction at a time. This might be especially relevant for restricted systems, that are less restricted in some capabilities then in other, such as devices with less bandwidth restrictions but high computational capabilities. For example, if computational time is the main concern, but not its network bandwidth, a reduction in private key sizes may be sensible, even tough other aspects might increase, such as message size. One of these proposals by Wang et al. [21] is focusing on exactly that. By introducing their new key generation function, they manage to create small private keys. On top of the smaller key size, their function simplifies the calculation process for the scheme, lowering the computational requirements by basing the calculation on simple mathematical instructions.

2) Handshake reduction: As mentioned in Section III, some cyber-physical system suffer from timing restrictions, allowing only a certain timeframe between data generation, such as a measurement, and its digestion at the receiver of the communication [2]. The before mentioned timing restrictions cause any delay inserted into the communication to be potentially critical. Durations of communication establishment's as a whole, which are also referred to as handshakes, can therefore be a major issue for restricted systems. The amount of time it takes for two communication partners to establish a connection, is heavily reliant of the used cryptography scheme. Due to the complexity of the NIST competition's algorithms, naive implementation can come with handshake duration increases [33], that may not be feasible due the timing requirements for time critical message types [2]. This implies a need for their reduction in order to maintain operability of the systems.

Multiple studies propose solutions on how to tackle this challenge. One of the proposals [19] evaluates the naive approach mentioned above. The idea is to keep the handshakes as they are right now with typical asymmetric algorithm that can not be used anymore, such as RSA and elliptical curves. This does not only include a simplified version of the key exchange without authentication, but a full on realistic scenario with state-of-the-art security mechanisms. This encompasses a procedure similar to TLS, in which each communication partner proves their identity to one another, incorporating encryption schemes, as well as signature schemes which both need to be post-quantum secure. The utilized algorithms enabling the secure scheme are not self developed, but combine promising algorithms from the NIST competition, in this case Kyber for the key exchange and Falcon as well as Dilithium for the signatures. Comparisons of the different setup combinations and the respective time they took for completing the handshake in comparable Internet of Things environments showcase a

dramatic speedup compared to a traditional handshake. The same result could be reproduced by a Sepulveda et al. focusing on DTLS communication in the Internet of Things [42]. For this scenario, the key exchanges for the post-quantum key exchanges tend to be drastically quicker compared to the current algorithms in use, such as RSA.

The same can not be said about hybrid post-quantum systems. As described in Section II-B3, hybrid systems are a solution for combining security levels since they incorporate a traditional cryptography scheme with a post-quantum secure one [20], [21]. The inherent challenge coming alongside that, is the introduced overhead, since a system needs to essentially manage the overhead for each algorithm, which affects the handshake duration dramatically. A study by Chen et al. [19] implements a hybrid approach based on a traditional RSA scheme combined with Kyber, Falcon and Dilithium, evaluates the performance implications. It becomes clear that the additional overhead to the traditional scheme is always existent and depending on the post-quantum secure part of the scheme can increase the handshake duration greatly. However, the extensive evaluation shows that the post-quantum part of the hybrid approach is only responsible for a fraction of the total runtime, while the traditional schemes takes requires most of the execution's time. Therefore, a solution to this challenge can not be located within the post-quantum aspect of the scheme. Instead, the traditional algorithm is the main performance concern. Hybrid schemes can therefore retain the possibility of backward compatibility, but necessarily perform drastically worse than pure post-quantum cryptography [19].

Moreover, handshakes themselves can cause issues in restricted systems if they suffer from bandwidth restriction as discussed in Section III, contrasting the ones previously mentioned, which focus on computational cost. Twardokus et al. [14] analyze post-quantum solutions in vehicles as part of the cyber-physical field, describes the network based issues. In these use cases, the protocols generally introduce bandwidth restrictions in form of limits on how long payloads for network frames may be. For traditional schemes, this poses no further issues. However, due to the increasing size of many post-quantum secure handshakes, specifically post-quantum signatures, this may become an issue if the required handshake can not be established due to message size restrictions. Since a simple signature size reduction is not a simple endeavor as previously mentioned, the only considerable solution is a switch of the underlying protocols, enabling variable frame sizes, such as in TLS [14].

3) Algorithm speedup: As one of the categories with the most research proposals, reimplementations of different algorithms has become a prominent procedure, with the aim of providing speedups of algorithm execution, in order to enable post-quantum security in restricted systems. However, research suggest multiple ways in which this is achievable. As one of the possible solutions, Mustafa et al. [37] offer a reimplementation of RSA. The main idea is to enable post-quantum security to systems that already utilize cryptography schemes based on RSA without introducing additional requirements, but instead improving upon efficiency and other security concerns, specifically for Internet of Things environments. In order to achieve this, the underlying cryptographic primitive of RSA needs to change. Since Shor's algorithm breaks integer factorization, post-quantum secure RSA utilizes vector factorization in lattices, which is not known to be susceptible to quantum computing attacks. A switch to this computational problem achieves the aforementioned goals. This approach outperforms other algorithms such as NTRU by a great margin [37].

Twardokus et al. [14] offer a vastly different proposal. In order to integrate post-quantum security in their communication system, they identify the missing capabilities the system offers for a simple post-quantum implementation. The main concern are signature sizes, which are responsible for a big part of the network communication. They identify that many certificates retransmit without necessity. By deploying a machine learning approach, they identify the redundant certificate communication and remove them. This reduces the network communication and frees up computational and network resources, which can now be used for post-quantum security [14]. Even tough this solution is not applicable all the time, it is a promising approach to freeing up resources in restricted systems by communication optimization.

Even tough symmetric cryptography is not as strongly affected by quantum computing as asymmetric cryptography, research groups have analyzed the impact on them in the Internet of Things. As previously mentioned, a security level of 128 bits is considered as the current security standard. Since Grover's algorithm can reduce the security level of some symmetric ciphers such as AES to its half, AES-256 will now be necessary in cyber-physical systems, as AES-128 only provides 64 security bits in a post-quantum scenario [9]. Instead of doubling the complexity of symmetric cipher, Alassaf et al. [38] propose the switch to symmetric cipher not affected by Grover's algorithm, reducing the computational requirements compared to its alternative. The suggested lightweight variation of the SIMON algorithm can only beat AES in terms of computation duration, when they use small key sizes. However, SIMON can achieve the same security level with slightly higher computation times for less than half the memory occupation and offers a new opportunity for post-quantum security for systems, dealing with memory constrains specifically.

Nannipieri et al. [39] present a fundamentally different approach to algorithm speedups by optimization. Many devices in the Internet of Things utilize RISC-V processors. It is possible to add custom dedicated assembly instruction to them, enabling hardware based acceleration for algorithms, which can use these instructions. Since algorithms like Kyber and Dilithium are utilizing complex instruction without them being necessarily natively supported by all Internet of Things devices, the addition of these instructions can provide extensive speedups of up to 65% [39]. This may be able to counteract hardware based restrictions and offering support for these post-quantum algorithms on devices, which would otherwise not be

able to execute them in a feasible manner.

As a final step for algorithm optimization, manipulations of the cryptographic primitives can be applied. Since most of the current state-of-the-art post-quantum cryptography schemes rely on lattice-based problems due to their efficiency, some research proposals [40] try to make the underlying mathematical calculations more efficient. In certain scenarios, the research yield a speedup of up to 80% without security trade-offs. This might offer solutions toward arithmetical optimization for algorithms such as Kyber, Dilithium or Falcon regarding their computational efforts. These proposed approaches hint at a broad spectrum of possible improvements to how post-quantum cryptography schemes can be applied in cyber-physical systems, which we will discuss in the next section.

V. Discussion

Even though many researchers evaluate their propositions on a small scale in test setups, without necessarily taking all practically relevant aspects into account, they hint at multiple adjustable variables, in order to fit post-quantum cryptography to these communication schemes and enables them in practice. One of the most notable pattern holding true for almost all papers analyzing different post-quantum cryptography schemes, is their superior efficiency and security, especially when compared to the pre-quantum alternatives. As one of the most promising contenders, the Kyber algorithm delivers a post-quantum security alternative for public-key encryption, even more efficient than the RSA encryption scheme [19]. In opposition to this, alternative signature schemes seem to always perform worse than the most efficient pre-quantum schemes. This behavior conflicts with cyber-physical communication pattern mostly relying on authentication and integrity checks, while putting message secrecy at the last spot in their priorities. Even with the prior mentioned optimizations to signatures, concerns about the application in restricted systems remain. While all of these concerns are reasonable and need to be addressed in order to make these systems secure from a theoretical point of view, they generally do not consider practical scenarios.

A. Missing practical considerations

A prime example for this would be the security level, which cryptography schemes need to provide. Even tough quantum computers will be able to attack authentication by computing signatures if a signature can be gathered, they can not compute the secret instantly, but need time for the computation [14]. While this duration will decrease over the years with increases of the qubit count, the point in time when breaking the secret keys in mere hours will be possible is still multiple decades away. Only one of the papers [14] considers this fact and concludes, that the certificates for signatures need only be strong enough, so they are not broken in their respective time frame of usage, in order to prevent message forging. Obviously, this case will not hold up forever. Nevertheless, it is essential for the current research towards integration of post-quantum security schemes, to take this into account. Another practical case which research mostly ignores is the trade-off currently in use in live systems. Enforcing security for all messages would be the most secure scenario, however this is not always achievable, as stated in Section I. Live systems already make these trade-offs. Since the time based performance of some pre-quantum schemes are too low for low latency communication patterns, meeting these requirements for post-quantum security should not be the goal and therefore not a primary comparison measure. Post-quantum security should first and foremost improve upon the security of pre-quantum schemes and does not have to outperform them in other aspects, however this is a recurring research trend.

B. Future Work

Apart from the missing practical considerations, the current state of the research field does not allow for reliable performance comparisons between approaches, which are either hard or not achievable at all. Many approaches take time based measurement instead on clock cycles in a non-reproducible setting. Combining this with heavily different hardware setups and therefore performance of the devices, any metric can only be compared to standard algorithms as a comparison base. This creates issues for approach to approach comparisons, rendering them mostly meaningless. A study recreating the prior mentioned approaches and applying them to classes of devices used in practical applications, such as industry settings, would grant the field a comparative overview of its current state. Part of this should be a clear measurement of metrics regarding the restriction types as discussed in Tab. I in order to classify different approaches more precisely and fitting them to the devices restrictions respectively. This seems to be a necessary and essential step for developing relevant future work in this research field.

VI. Conclusion

The upcoming advances of quantum computing threaten the security of many commonly used cryptography schemes. When commercial grade quantum computers exist, they break most asymmetric cryptography schemes, while only weakening symmetric schemes, which remain useable after parameter changes. In contrast, asymmetric cryptography needs to be redeveloped in a post-quantum secure manner, while enabling their usage in cyber-physical systems dealing with restrictions of hardware as well as additional operational requirements. Research in this field yield several propositions to achieve this. The defining solutions can be divided into key size reductions, handshake reductions and algorithmic speedups, all of which addressing different restriction type combinations of the embedded devices. While public key exchanges tend to be more easily integrated, the complexity of post-quantum signatures remain a challenge for cyber-physical systems, requiring more intense future work. Despite the lack of standardized evaluation metrics slowing the process for developing new approaches and comparing them to the already established ones, research in this field delivers promising approaches for securing cyber-physical systems in a quantum age.

REFERENCES

[1] S. Kirmani, A. Mazid, I. A. Khan, and M. Abid, "A Survey on IoT-Enabled Smart Grids: Technologies, Architectures, Applications, and Challenges," *Sustainability*, vol. 15, no. 1, p. 717, Dec. 2022. [Online]. Available: https://www.mdpi.com/2071-1050/15/1/717

[2] J. Gaspar, T. Cruz, C.-T. Lam, and P. Simões, "Smart Substation Communications and Cybersecurity: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 4, pp. 2456–2493, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10217175/

[3] L. Bader, M. Serror, O. Lamberts, Ö. Sen, D. Van Der Velde, I. Hacker, J. Filter, E. Padilla, and M. Henze, "Comprehensively Analyzing the Impact of Cyberattacks on Power Grids," in *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*. Delft, Netherlands: IEEE, Jul. 2023, pp. 1065–1081. [Online]. Available: https://ieeexplore.ieee.org/document/10190485/

[4] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014. [Online]. Available: http://link.springer.com/10.1007/s11276-014-0761-7

[5] J. Buchmann, *Einführung in die Kryptographie*, ser. Springer-Lehrbuch. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016. [Online]. Available: https://link.springer.com/10.1007/978-3-642-39775-2

[6] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on Post-Quantum Cryptography," National Institute of Standards and Technology, Tech. Rep. NIST IR 8105, Apr. 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[7] M. Sipser, *Introduction to the theory of computation*, third edition, international edition ed. Australia Brazil Japan Korea Mexiko Singapore Spain United Kingdom United States: Cengage Learning, 2013.

[8] M. Roetteler and K. M. Svore, "Quantum Computing: Codebreaking and Beyond," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 22–36, Sep. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8490171/

[9] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, Sep. 2017. [Online]. Available: https://www.nature.com/articles/nature23461

[10] P. Benioff, "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines," *Journal of Statistical Physics*, vol. 22, no. 5, pp. 563–591, May 1980. [Online]. Available: http://link.springer.com/10.1007/BF01011339

[11] D. M. Mosca and D. M. Piani, "Quantum threat timeline report 2020," *Global Risk Institute*, 2021. [Online]. Available: https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2020/

[12] D. McMahon, *Quantum computing explained*. Hoboken, N.J: Wiley-Interscience : IEEE Computer Society, 2008, oCLC: ocn122424963.

[13] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997, arXiv:quant-ph/9508027. [Online]. Available: http://arxiv.org/abs/quant-ph/9508027

[14] G. Twardokus, N. Bindel, H. Rahbari, and S. McCarthy, "When Cryptography Needs a Hand: Practical Post-Quantum Authentication for V2V Communications," in *Proceedings 2024 Network and Distributed System Security Symposium*. San Diego, CA, USA: Internet Society, 2024. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2024-267-paper.pdf

[15] V. Kasirajan, *Fundamentals of Quantum Computing: Theory and Practice*. Cham: Springer International Publishing, 2021. [Online]. Available: https://link.springer.com/10.1007/978-3-030-63689-0

[16] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*. Philadelphia, Pennsylvania, United States: ACM Press, 1996, pp. 212–219. [Online]. Available: http://portal.acm.org/citation.cfm?doid=237814.237866

[17] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 433, Apr. 2021, arXiv:1905.09749 [quant-ph]. [Online]. Available: http://arxiv.org/abs/1905.09749

[18] R. A. Grimes, *Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto*, 1st ed. Wiley, Nov. 2019. [Online]. Available: https://onlinelibrary.wiley.com/doi/book/10.1002/9781119618232

[19] S. Paul and P. Scheible, "Towards Post-Quantum Security for Cyber-Physical Systems: Integrating PQC into Industrial M2M Communication," in *Computer Security - ESORICS 2020*, L. Chen, N. Li, K. Liang, and S. Schneider, Eds. Cham: Springer International Publishing, 2020, vol. 12309, pp. 295–316, series Title: Lecture Notes in Computer Science. [Online]. Available: http://link.springer.com/10.1007/978-3-030-59013-0_15

[20] S. Paul and E. Guerin, "Hybrid OPC UA: Enabling Post-Quantum Security for the Industrial Internet of Things," in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. Vienna, Austria: IEEE, Sep. 2020, pp. 238–245. [Online]. Available: https://ieeexplore.ieee.org/document/9212112/

[21] L. Wang, J. Chen, K. Zhang, and H. Qian, "A post-quantum hybrid encryption based on QC-LDPC codes in the multi-user setting," *Theoretical Computer Science*, vol. 835, pp. 82–96, Oct. 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0304397520303558

[22] T. Krause, R. Ernst, B. Klaer, I. Hacker, and M. Henze, "Cybersecurity in Power Grids: Challenges and Opportunities," *Sensors*, vol. 21, no. 18, p. 6225, Sep. 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/18/6225

[23] S. Kumari, M. Singh, R. Singh, and H. Tewari, "Post-quantum cryptography techniques for secure communication in resource-constrained Internet of Things devices: A comprehensive survey," *Software: Practice and Experience*, vol. 52, no. 10, pp. 2047–2076, 2022, _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/spe.3121. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.3121

[24] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, and D. Smith-Tone, "Status report on the third round of the NIST Post-Quantum Cryptography Standardization process," National Institute of Standards and Technology (U.S.), Gaithersburg, MD, Tech. Rep. NIST IR 8413-upd1, Sep. 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf

[25] W. Castryck and T. Decru, "An Efficient Key Recovery Attack on SIDH," in *Advances in Cryptology – EUROCRYPT 2023*, C. Hazay and M. Stam, Eds. Cham: Springer Nature Switzerland, 2023, vol. 14008, pp. 423–447, series Title: Lecture Notes in Computer Science. [Online]. Available: https://link.springer.com/10.1007/978-3-031-30589-4_15

[26] "SIKE – Supersingular Isogeny Key Encapsulation." [Online]. Available: http://sike.org/

[27] D. J. Bernstein, T. Lange, and C. Peters, "Attacking and Defending the McEliece Cryptosystem," in *Post-Quantum Cryptography*, J. Buchmann and J. Ding, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, vol. 5299, pp. 31–46, series Title: Lecture Notes in Computer Science. [Online]. Available: http://link.springer.com/10.1007/978-3-540-88403-3_3

[28] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC Editor, Tech. Rep. RFC2104, Feb. 1997. [Online]. Available: https://www.rfc-editor.org/info/rfc2104

[29] A. Hosoyamada and T. Iwata, "On Tight Quantum Security of HMAC and NMAC in the Quantum Random Oracle Model," in *Advances in Cryptology – CRYPTO 2021*, T. Malkin and C. Peikert, Eds. Cham: Springer International Publishing, 2021, vol. 12825, pp. 585–615, series Title: Lecture Notes in Computer Science. [Online]. Available: https://link.springer.com/10.1007/978-3-030-84242-0_21

[30] Computer Security Division, Information Technology Laboratory, "Round 4 Submissions - Post-Quantum Cryptography," Jan. 2017. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-4-submissions

[31] "Selected algorithms 2022 - post-quantum cryptography," Computer Security Division, Information Technology Laboratory, Tech. Rep., Jan. 2017, cSRC NIST. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

[32] O. Kuznetsov, S. Kandiy, E. Frontoni, and O. Smirnov, "Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece," *CEUR-WS.org*, vol. Proceedings of the Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC 2023) co-located with International Conference on Problems of Infocommunications. Science and Technology (PICST 2023), Kyiv, Ukraine, August 1, 2023 (online), no. 3504, pp. 1–11, 2023. [Online]. Available: https://ceur-ws.org/Vol-3504/paper1.pdf

[33] I. Tzinos, K. Limniotis, and N. Kolokotronis, "Evaluating the performance of post-quantum secure algorithms in the TLS protocol," *Journal of Surveillance, Security and Safety*, vol. 3, no. 3, pp. 101–127, Sep. 2022, publisher: OAE Publishing Inc. [Online]. Available: https://www.oaepublish.com/articles/jsss.2022.15

[34] P. Kampanakis and D. Sikeridis, "Two PQ Signature Use-cases: Non-issues, challenges and potential solutions." 2019, publication info: Preprint. MINOR revision. [Online]. Available: https://eprint.iacr.org/2019/1276

[35] S. H. Odin Hashemi and G. A. Hodtani, "A Modified McEliece Public-Key Cryptosystem Based On Irregular Codes Of QC-LDPC and QC-MDPC," in *2019 27th Iranian Conference on Electrical Engineering (ICEE)*. Yazd, Iran: IEEE, Apr. 2019, pp. 1373–1376. [Online]. Available: https://ieeexplore.ieee.org/document/8786376/

[36] X. Yang, H. Cao, W. Li, and H. Xuan, "Improved Lattice-Based Signcryption in the Standard Model," *IEEE Access*, vol. 7, pp. 155 552–155 562, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8882330/

[37] I. Mustafa, I. U. Khan, S. Aslam, A. Sajid, S. M. Mohsin, M. Awais, and M. B. Qureshi, "A Lightweight Post-Quantum Lattice-Based RSA for Secure Communications," *IEEE Access*, vol. 8, pp. 99 273–99 285, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9096276/

[38] N. Alassaf, A. Gutub, S. A. Parah, and M. Al Ghamdi, "Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications," *Multimedia Tools and Applications*, vol. 78, no. 23, pp. 32 633–32 657, Dec. 2019. [Online]. Available: http://link.springer.com/10.1007/s11042-018-6801-z

[39] P. Nannipieri, S. Di Matteo, L. Zulberti, F. Albicocchi, S. Saponara, and L. Fanucci, "A RISC-V Post Quantum Cryptography Instruction Set Extension for Number Theoretic Transform to Speed-Up CRYSTALS Algorithms," *IEEE Access*, vol. 9, pp. 150 798–150 808, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9605604/

[40] S. Akleylek, E. Alkım, and Z. Y. Tok, "Sparse polynomial multiplication for lattice-based cryptography with small complexity," *The Journal of Supercomputing*, vol. 72, no. 2, pp. 438–450, Feb. 2016. [Online]. Available: http://link.springer.com/10.1007/s11227-015-1570-1

[41] E. Barker, "Recommendation for Key Management Part 1: General," National Institute of Standards and Technology, Tech. Rep. NIST SP 800-57pt1r4, Jan. 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

[42] J. Sepulveda, S. Liu, and J. M. Bermudo Mera, "Post-Quantum Enabled Cyber Physical Systems," *IEEE Embedded Systems Letters*, vol. 11, no. 4, pp. 106–110, Dec. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8626118/