Benchmarking of Pre- and Post-Quantum Group Encryption Schemes with Focus on IoT

Thomas Prantl, Dominik Prantl, André Bauer, Lukas Iffländer, Alexandra Dmitrienko, Samuel Kounev
University of Würzburg
firstname.lastname@uni-wuerzburg.de

Christian Krupitzer
University of Hohenheim
christian.krupitzer@uni-hohenheim.de

***Abstract*—In the next few years, both the number of IoT devices and the performance of quantum computers will increase. Both technologies pose a challenge to our current crypto-strategies. Therefore, post-quantum n-to-n communication encryption is a crucial field of research. Here, the development of new schemes and the analysis, and comparison of existing schemes is necessary. However, current work only investigates the performance of post-quantum schemes only for 1-to-1 communication. Therefore, in this paper, we analyze existing post-quantum schemes concerning n-to-n communication and compare them with pre-quantum schemes. Our results show that the pre-quantum schemes perform better regarding computation times than the post-quantum schemes, but the differences are sometimes only marginal. However, these marginal differences in computation times lead to the lower energy efficiency of the post-quantum schemes. In terms of features, there is no difference between both scheme classes. We show that the post-quantum schemes require unicast, whereas some pre-quantum schemes also support broadcast. Deciding whether to use pre- or post-quantum schemes for n-to-n encryption in IoT use cases depends on (i) whether energy efficiency is essential – e.g., in case of limited power supply – and (ii) whether unicast or broadcast is available.**

***Index Terms*—Group Encryption Scheme, Benchmark, Post-Quantum Encryption, Internet of Things**

I. Introduction

Using quantum computers with their unimaginable computing power no longer seems to be just a future dream but has almost become a reality. A computer built on quantum mechanics' strange properties can, in some instances, perform calculations exponentially faster than binary computers. Already back in October 2019, Google announced that they developed a quantum computer 10.000 times faster than modern supercomputers at the task of sampling the output of a pseudo-random quantum circuit [1], [2]. This computing power achieved by current quantum computers is already awe-inspiring and will increase at an unimaginable rate in the coming years. According to Moore's Law, conventional computer systems double their speed every two years. The speed of quantum computers, on the other hand, is assumed to increase twice exponentially in the same period, according to Neven's law [3].

This increasing computing power of quantum computers will be an essential component for accelerating many conventional applications. For example, using quantum computers can reduce the calculation of different protein foldings in three-dimensional space from years to a few minutes [4]. This speed-up will allow the pharmaceutical industry to develop new drugs and vaccines in a fraction of the time required today. Quantum computers also apply to AI, for example, to accelerate training processes to such an extent that today's take days are complete in minutes. This acceleration will enable more extensive and more complex AI algorithms and support more sophisticated AIs [4].

However, besides all these advantages that quantum computers can offer, they can also accelerate or enable applications that endanger many aspects of modern life. An increasing number of everyday activities — such as doing sports together and exchanging training data with friends and family via the FitBit smartwatch [5], or shopping in supermarkets without checkouts [6] — shift to the Internet. A cornerstone of this development is the deployment of effective and highly performant cryptographic algorithms. The confidence in the security of primitives used in today's cryptosystems is very high, and attackers seldom attempt direct attacks. Instead, they exploit other attack vectors, such as implementation errors or social engineering, to penetrate the system. With the appearance of sufficiently capable quantum computers, many security guarantees provided by today's cryptographic systems will vanish.

The US government's Institute NIST has launched a competition and standardization process for post-quantum cryptosystems [7] to continue secure Internet operation in the future. Besides security guarantees, good performance and applicability to all types of devices—from powerful PCs to resource-constrained IoT devices—is crucial to post-quantum cryptosystems. In addition, post-quantum encryption must support not only 1-to-1 communication but also IoT typical n-to-n communication —as in the previously presented use cases of sharing training data via the FitBit smartwatch with a group and shopping at Amazon Go stores without a checkout— of dynamic groups, with changing group membership dynamics. In recent years, several possible candidates for future post-quantum encryption methods have been presented and analyzed in terms of performance. So far, this analysis only

considered the suitability for 1-to-1 communication ignoring n-to-n communication. Therefore, in this paper, we want to fill the gap and analyze post-quantum encryption schemes concerning their performance for n-to-n communication and compare their performance to traditional pre-quantum n-to-n encryption schemes. We chose an IoT use case as an evaluation scenario to evaluate the suitability of the post-quantum schemes considering resource-limited hardware. Specifically, we use the benchmark for n-to-n encryption schemes presented at ICPE 2021 [8] for the evaluation of the schemes. More specifically, this paper provides the following contributions:

1) the completion of the requirements analysis of pre-quantum schemes of the benchmark, proposed in [8];
2) the determination of features and requirements of the selected post-quantum schemes;
3) the extension of the performance analysis of pre-quantum schemes of the benchmark, proposed in [8];
4) the determination of the performance of the selected post-quantum group encryption schemes;
5) comparing pre- and post-quantum schemes in terms of features, requirements, and performance.

The remainder of this paper is structured as follows. Section II discusses how to implement n-to-n encryption using a trustworthy third party and 1-to-1 encryption. Section III introduces a benchmark for group encryption schemes, including metrics, workload patterns, the IoT measurement setup, and features and requirements of group encryption schemes. In addition, Section III presents the selected pre- and post-quantum schemes. Next, we show the results of scheme comparison in terms of features and requirements in Section IV and present the results in terms of performance in Section V. We compare our work to the state of the art in Section VI and discuss future directions in Section VII.

II. SKDC - Group encryption based on 1-to-1 encryption schemes

This section introduces the *Simple Key Distribution Center* (SKDC), the simplest way to implement n-to-n encryption using 1-to-1 encryption [9]. SKDC allows us later to extend 1-to-1 post-quantum schemes to n-to-n post-quantum schemes. Thus, we present for $SKDC$ (i) the encryption and decryption of messages, (ii) the involved actors (including their tasks and connections), (iii) the initial creation of a group consisting of n members, and (iv) changing the group composition, i.e., adding or revoking members from this group. Figure 1 illustrates our used approach to implement SKDC.

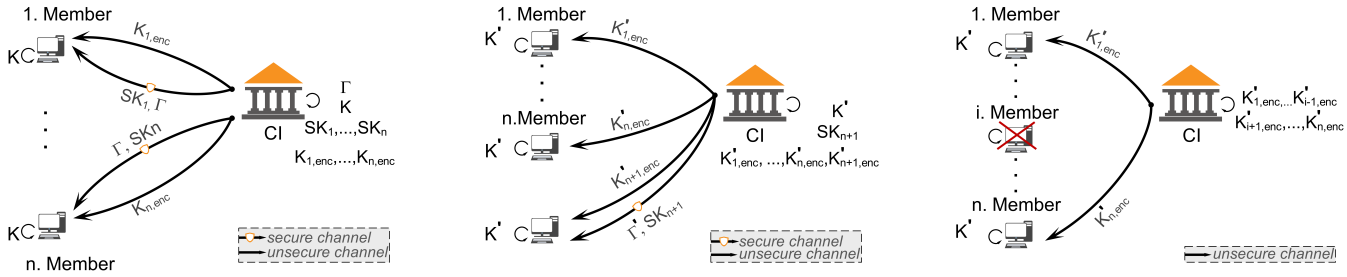
Encryption and Decryption: $SKDC$ uses 1-to-1 encryption methods to implement group encryption. It is irrelevant to the basic functionality of $SKDC$ whether these are post-quantum procedures or not. It is essential to choose a 1-to-1 encryption method and uniformly carry out all encryptions and decryptions. For these reasons, in this section, we describe the functioning of $SKDC$ in general and not specific to post-quantum encryption.

Involved Actors: The actors consist of the group members, who should communicate securely with each other, and a central instance (CI), which controls the creation and management of the groups. In general, any group member could fill in this role; however, we assume a dedicated CI in the following. For example, in a smart home scenario, the corresponding smart devices could form a group, and the home server could act as the CI. The CI generates the keys for managing the group memberships, defines the parameters for decryption and encryption, and further distributes them to the group members. Since the CI creates and thus knows the group key, the CI can read all group messages and, therefore, must be a trustworthy party. Secure channel must be available once between the CI and each group member for inclusion in a group. Thereby, using a secure channel means that the transmitted information is not accessible by third parties (i.e., confidential), fresh and integrity protected. One way to realize such a channel is to connect the IoT device directly via a wire. For subsequent communication between a group member and the CI, an insecure connection suffices as long as it guarantees all messages reaching their destination. Otherwise, it could happen that, e.g., when removing a member, another member misses this information and continues to encrypt messages such that the excluded member can read them.

In line with the benchmark [8] we use for comparing pre-quantum and post-quantum group encryption schemes, we assume for $SKDC$ and the rest of this paper that messages neither become delayed nor replayed, falsified, or intercepted. For the sake of simplicity and in line with [8], we also assume an integrated group management approach, i.e., the CI knows all initial group members and when to add or remove members.

Initial Group Creation: Figure 1a shows the initial group creation with n group members. First, the CI must determine the system parameter Γ. In the case of SDKC, Γ consists only of selecting a 1-to-1 encryption scheme used by all involved actors. Next, the CI determines and stores for each group member i its secret key SK_i. Storing all SK_i's allows the CI to revoke group members later efficiently. Then, the CI informs each group member about its SK_i and Γ using a secure channel. Afterward, the CI determines the group key K and encrypts K to $K_{i,enc}$ for each group member using the respective secret key SK_i and Γ. The CI then sends the respective $K_{i,enc}$ to the corresponding group member, not requiring a secure channel since only the corresponding group member and CI know the secret key SK_i necessary for decryption. Using its SK_i and Γ, each group member can decrypt $K_{i,enc}$ to receive the group key K. Each group member can now use K and Γ to encrypt messages for the group or decrypt messages from a group member.

Addition of Group Members: As shown in Figure 1b, adding a new group member requires the CI to provide a secret key SK_{n+1} and Γ for the new group member through a secure channel and store the new secret key. Additionally, the CI must determine a new group key K', encrypt it for each group member individually using its secret key SK_i and Γ to $K'_{i,enc}$ and send each group member its $K'_{i,enc}$, so that each group member can decrypt $K'_{i,enc}$ to K'. Again, the transmission of the encrypted version $K'_{i,enc}$ of the new group key K' does



(a) SKDC: Group creation (b) SKDC: Member addition (c) SKDC: Member revocation

Fig. 1: Visualization of the group management operations (a) group creation, (b) member addition and (c) member revocation of our approach to realize SKDC.

not require a secure channel.

Revocation of Group Members: Figure 1c illustrates the revocation process of the i-th group member. The revocation process requires the CI to determine a new group key K' to guarantee that the revoked group entity cannot encrypt or decrypt group messages anymore. This process happens analogously to creating a new group without the excluded member, except that no secret keys distribution is necessary.

III. Evaluation Environment

This section briefly introduces the benchmark presented in [8], which we use to compare post-quantum group encryption schemes among each other and with pre-quantum group encryption schemes. The benchmark includes metrics, the IoT measurement environment, and requirements and features of group encryption schemes. Thus, we present the following aspects of the benchmark in turn: (i) workload patterns, (ii) requirements and features, (iii) measurement setup, and (iv) metrics. In addition, we briefly introduce the pre- and post-quantum schemes that we compare using the benchmark.

A. Workload Pattern

The workload patterns of the benchmark [8] describe the operations of the benchmarked group encryption scheme. The benchmark differentiates between actors that execute the respective operation and in which phase this occurs. For our selected pre- and post-quantum schemes, the actors consist of the CI and the group members. The operations under consideration consist of the encryption and decryption of messages among group members and group management operations. The latter consists of the initial creation of a group and the subsequent addition and removal of group members. These group management operations take place in two phases: deployment phase and operational phase. For example, when creating a group, the CI must, in the deployment phase, generate the corresponding public and secret keys individually for each group member and distribute them to the corresponding group members in a secure manner. In a deployment phase, the CI can generate a group key and send it, individually encrypted for each group member, to the group members. No secure channel is necessary for the transmission of the encrypted group key.

The member addition operation also comprises a deployment and operational phase. In the deployment phase, the corresponding keys for the new group member must first be created by the CI and securely transmitted to the new group member before the CI then distributes the encrypted group key again in the operational phase. In contrast, the revocation process of a group member does not consist of two phases but only of the operational phase.

B. Requirements and Features

The benchmark [8] considers which *requirements* the respective group encryption schemes place on the topology and confidentiality for the respective operations. Concerning topology, we differentiate whether (i) the CI can broadcast the group management messages to the group members since each group member receives the same message, or (ii) each group member receives individual messages, and thus unicast is necessary. Concerning confidentiality, a distinction is made whether (i) the information of the respective group management operation is confidential and must reach the group members securely, or (ii) it can also be publicly known.

The benchmark analyzes whether the group encryption methods support the following three features: (i) group size limit, (ii) group backward secrecy, and (iii) forward secrecy. The group size limit describes whether a group's size limits group update operations. For example, a possible limitation is that for a necessary calculation, the required parameters increase with the group size and only fit into the memory up to specific limit. The group backward secrecy means that a new group member does not have access to data transmitted before joining the group, while group forward secrecy implies no access to transmitted information after revocation of the member. We assume that backward/forward secrecy is present when the addition/revocation of group members triggers an immediate propagation of corresponding information.

C. Measurement Setup

The measurement environment of the benchmark [8] implements an IoT scenario because IoT devices (i) are typically

resource-constrained, and (ii) usually communicate with a large number of other IoT devices and thus represent a realistic deployment scenario for group encryption. Figure 2 illustrates the benchmark [8] measurement setup consisting of the following four components: an observed group member, its power supply, a power meter measuring its energy consumption, and the CI. In line with [8], we used an ESP32—a 32-bit microcontroller—as the observed group member, the Elegoo Power Supply Module1PC as the power supply for the ESP32, the Yokogawa WT310 as the power meter, and a Lenovo B50-50 80S2004AGE laptop as the CI.

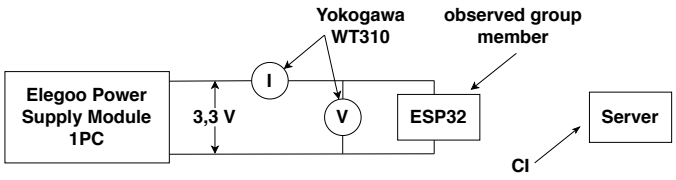


Fig. 2: Circuit diagram of the measurement setup

D. Metrics

In the following, we present the metrics of the benchmark [8], including storage space requirements, computation times, and energy efficiency.

Storage Requirements: The benchmark [8] considers the size of the encrypted messages and the memory requirements for parameters. For the latter, the benchmark distinguishes (1) whether the memory requirement is temporary (e.g., short-term storing of parameters for key update calculations) or permanent (e.g., secret keys) and (2) whether the memory requirement affects a group member or the CI. We use the mean memory requirement and its standard deviation as the accuracy measure.

Computation Times: The benchmark [8] defines the computation time $\bar{t}_A$ for an action A as the average time required to execute A; see Equation 1. Assuming that A' is the decryption of a message by a group member, $\bar{t}_{A'}$ comprises decrypting a message n times and is the average of the corresponding times $t_{A',1}, \ldots, t_{A',n}$, needed for the single decryptions. The benchmark [8] determines the accuracy of the calculation time using Gaussian error propagation in Equation 2. Here Δt_A stands for the measurement accuracy for an action A's execution time.

$$\bar{t}_A = \frac{1}{n}\sum_{i=1}^{n} t_{A,i} \quad (1) \qquad \Delta\bar{t}_A = \frac{\sqrt{n} * \Delta t_A}{n} \quad (2)$$

Energy Efficiency: The benchmark [8] defines the energy efficiency E, according to Equation 3, as the throughput T_A (see Equation 7) to power consumption W ratio. The accuracy of the energy efficiency ΔE results from using Gaussian error propagation in Equation 4.

$$E = \frac{\text{Throughput}}{\text{Power Consumption}} = \frac{T_A}{W} \quad (3)$$

$$\Delta E = \sqrt{\frac{\Delta T_A^2}{W^2} + \frac{T_A^2 * \Delta W^2}{W^4}} \quad (4)$$

In line with the benchmark [8], we calculate W according to Equation 5 as the average power consumption per second. In this equation, n stands for the measurement duration in seconds and W_i for the power consumption during the ith second. The benchmark [8] calculates the accuracy again using Gaussian error propagation and considers the accuracy of the Yokogawa WT310 according to Equation 6.

$$W = \frac{1}{n}\sum_{i=1}^{n} W_i \quad (5)$$

$$\Delta W = \frac{1}{n}\sqrt{\sum_{i=1}^{n}(0.1\% * W_i + 0.0006 * W)^2} \quad (6)$$

The calculation of energy efficiency still requires the determination of throughput T_A, which the benchmark [8] defines in Equation 7 as the weighted number of performed actions A during a period t_p. We consider the throughput for one specific action at a time. In this equation, $|A|$ stands for the number of actions A performed and W_A for the weighting factor of action A. The benchmark defines W_A as follows: W_A is the number of decrypted or encrypted bits for decryption and encryption actions. For all other actions, we set W_A to the value 1. The error of T_A results from Equation 8 using Gaussian error propagation, where Δt_p stands for t_p's accuracy.

$$T_A = \frac{W_A * |A|}{t_p} \quad (7) \qquad \Delta T_A = \frac{W_A * |A| * \Delta t_p}{t_p^2} \quad (8)$$

E. Pre- and Post-quantum Schemes for Benchmarking

At first, it is necessary to determine which pre- and post-quantum schemes to consider. In selecting the pre-quantum schemes, we followed the approach presented in [8] and analogously selected the following schemes: $Boneh+$, $Nishat$ ([10], [11]), and $Baseline$. The $Baseline$, in the following referred to as $Base$, is a simple scheme chosen as a baseline scheme for all pre-quantum group encryption schemes. The Scheme $Boneh+$ consists of the two variants $Boneh+_{\text{Fat Client}}$ and $Boneh+_{\text{Thin Client}}$, which differ regarding workload distribution between the actors. We use the implementation that the benchmark [8] uses to realize the pre-quantum schemes.

We selected three post-quantum schemes. In doing so, we had to select 1-to-1 post-quantum encryption schemes in this selection and extend them to n-to-n post-quantum encryption schemes with SKDC since, for now, literature only proposes 1-to-1 post-quantum encryption schemes. Specifically, this comprises the $AJPS$ scheme [12], a promising new post-quantum cryptosystem that related works only analyzed for security. We aim to fill this gap in this paper by also analyzing its performance. Additionally, we compare the chosen schemes

TABLE I: Features of pre- and post-quantum group encryption schemes.

Features \ Schemes	$SKDC$ [9]	$Nishat$ [10], [11]	$Boneh$ Thin Client	$Boneh$ Fat Client
unlimited group size	✓	✗	✓	✗
backward secrecy	✓	✓	✓	✓
forward secrecy	✓	✓	✓	✓

(a) Features of the pre-quantum group encryption schemes $BASE$, $Nishat$, $Boneh{+}_{\text{Fat Client}}$ and $Boneh{+}_{\text{Thin Client}}$

Features \ Schemes	$AJPS$ [12]	$Saber$ [14]	$NTRU$ [13]
unlimited group size	✓	✓	✓
backward secrecy	✓	✓	✓
forward secrecy	✓	✓	✓

(b) Features of the post-quantum group encryption schemes $AJPS$, $Saber$ and $NTRU$.

to $NTRU$ [13] and $Saber$ [14], both finalists from the third Nist standardization round for post-quantum methods[1].

For the realization of the pre-quantum schemes, we use the existing implementation from [8]. We use the official implementations submitted for the third Nist round for the post-quantum procedures on the CI side for NTRU and Saber [14], [15]. On the member side, we use an adapted implementation for the ESP32 from [16], which the European Union Agency for Cybersecurity also refers to [17]. For NTRU, we had to create the group member implementation ourselves. For AJPS we use the implementation from [18].

IV. Feature- and Requirements-driven Analysis of Pre- and Post-Quantum Schemes

The benchmark proposed in [8] emphasizes that it is vital to consider the pure performance, the supported features, and the requirements to the environment for group encryption method selection. For this reason, in this section, we first compare the pre- and post-quantum schemes concerning their features and requirements.

Features: Tables Ia and Ib list the features of the pre-quantum and post-quantum schemes. All pre-quantum schemes (see Table Ia) provide forward and backward secrecy. However, only the schemes $BASE$ and $Boneh{+}_{\text{Thin Client}}$ allow group members to perform group management operations for arbitrarily large groups. The schemes $Nishat$ and $Boneh{+}_{\text{Fat Client}}$, on the other hand, limit the number of participants in a group.

All post-quantum schemes (see Table Ib) support forward and backward secrecy and perform group management operations for arbitrarily large groups. Concerning the features, in summary, post-quantum schemes do not pose restrictions since they fulfill all features in each case. However, when selecting pre-quantum schemes, one must pay close attention to the maximum size of the group.

Requirements: All post-quantum methods offer all features, but this also comes at a cost in some cases. For this purpose, we consider Tables IIa and IIb, which contain the corresponding requirements for the respective group management operations. Based on these tables, the pre- and post-quantum methods all have identical requirements in terms of confidentiality of communication. However, there are differences in the topology requirements. All post-quantum schemes send individualized messages for each group member, making broadcast inefficient, and unicast is preferable. On the other hand, the pre-quantum schemes $Nishat$ and $Boneh{+}_{\text{Fat Client}}$ can efficiently use broadcast. [2] However, $Nishat$ and $Boneh{+}_{\text{Fat Client}}$ achieve the efficient use of broadcast only because group members cannot perform group management operations for arbitrarily large groups in these schemes.

In summary, considering features and requirements, the choice between post- and pre-quantum schemes only matters if the use case does not require arbitrarily large groups. In this case, pre-quantum schemes may have the advantage of being able to use broadcast efficiently.

V. Performance Analysis

Due to space limitations, we cannot discuss all performance metrics and focus on computation times and energy efficiency. We start the performance analysis from the group members' perspective on computation times and energy efficiency, followed by the CI-side calculation times. A discussion of the results concludes this section.

A. Group Member Performance

We start the member-side performance analysis with the calculation times and follow with the energy efficiency.

1) Computation Times:: Figures 3a and 3b present the duration required to encrypt a message for other group members using post- and pre-quantum group encryption schemes. Here, we consider messages up 60 bytes for encryption since most messages in the IoT are small and often comprise less than 40 bytes [19]. The two graphs show that the pre-quantum schemes have quasi-constant encryption times in this range. The same applies to the post-quantum schemes, except for $AJPS$'s linearly increasing encryption time. We rank the schemes in ascending order by their encryption times for a message length between 10 bytes and 60 bytes: $Boneh{+}_{\text{Thin Client}}$, $Boneh{+}_{\text{Fat Client}}$, and $BASE < Saber < NTRU < Nishat < AJPS$. $Nishat$ sometimes swaps places with $AJPS$ in the ranking for message lengths smaller than 10 bytes. Here, $Boneh{+}_{\text{Thin Client}}$, $Boneh{+}_{\text{Fat Client}}$, and $BASE$ have the same encryption times since they all use AES. Pre-quantum schemes encrypt messages faster than post-quantum

[1]The US agency NIST has started the standardization process for post-quantum schemes, analogous to the standardization process for pre-quantum schemes. This standardization process comprises several rounds, which narrow down the final scheme. At this point in the standardization process for post-quantum schemes, NIST announced the finalists of the third round [7].

[2]The difference between unicast and broadcast is particularly important for IoT scenarios, since IoT communication protocols such as MQTT rely on multicast, creating an overhead when used for unicast messages.

TABLE II: Requirements of the group creation operation of the centralized group encryption schemes $BASE$, $Nishat$, $Boneh{+}_{\text{Fat Client}}$ and $Boneh{+}_{\text{Thin Client}}$.

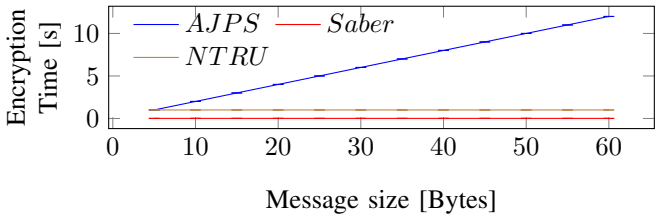
		$BASE$ [9]				$Nishat$ [10], [11]				$Boneh{+}_{\text{Fat Client}}$				$Boneh{+}_{\text{Thin Client}}$			
		Topology		Confi-dential		Topology		Confi-dential		Topology		Confi-dential		Topology		Confi-dential	
		uni-cast	broad-cast	yes	no	uni-cast	broad-cast	yes	no	uni-cast	broad-cast	yes	no	uni-cast	broad-cast	yes	no
Group Creation	Deployment	✗		✗		✗		✗		✗		✗		✗		✗	
	Operational	✗			✗		✗		✗		✗		✗	✗			✗
Member revocation		✗			✗		✗		✗		✗		✗	✗			✗
Member Addition	old	✗			✗		✗		✗		✗		✗	✗			✗
	new	✗			✗		✗		✗		✗		✗	✗			✗

(a) Requirements of the pre-quantum group encryption schemes $BASE$, $Nishat$, $Boneh{+}_{\text{Fat Client}}$ and $Boneh{+}_{\text{Thin Client}}$.

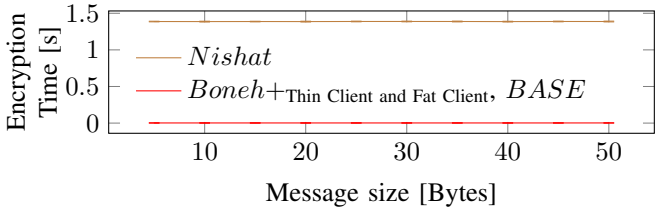
		$AJPS$ [12]				$Saber$ [14]				$NTRU$ [13]			
		Topology		Confi-dential		Topology		Confi-dential		Topology		Confi-dential	
		uni-cast	broad-cast	yes	no	uni-cast	broad-cast	yes	no	uni-cast	broad-cast	yes	no
Group Creation	Deployment	✗		✗		✗		✗		✗		✗	
	Operational	✗			✗	✗			✗	✗			✗
Member revocation		✗			✗	✗			✗	✗			✗
Member Addition	old	✗			✗	✗			✗	✗			✗
	new	✗			✗	✗			✗	✗			✗

(b) Requirements of the post-quantum group encryption schemes $AJPS$, $Saber$ and $NTRU$.

methods. However, this difference is marginal. Between one of the fastest pre-quantum schemes $Boneh{+}_{\text{Thin Client}}$, $Boneh{+}_{\text{Fat Client}}$, and $BASE$ and the fastest post-quantum scheme $Saber$ is less than 10 ms.



(a) Encryption times of post-quantum group encryption schemes.



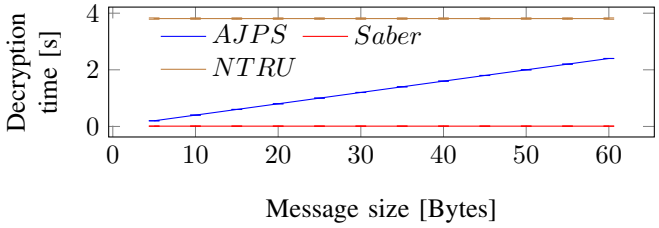
(b) Encryption times of pre-quantum group encryption schemes.

Fig. 3: Encryption times of pre- and post- quantum group encryption schemes.

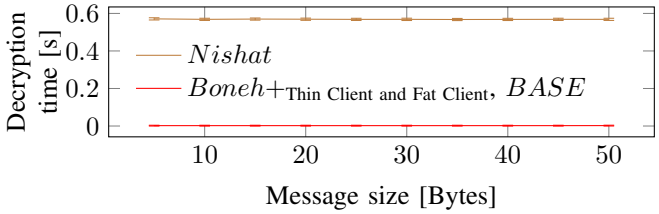
For the performance analysis of the decryption times, we chose the measurement range analogous to the encryption. Figures 4a and 4b illustrate the decryption times for post- and pre-quantum schemes. For the considered measurement range, all pre-quantum schemes and post-quantum schemes take constant time for message decryption, except for $AJPS$'s linearly increasing decryption time. We rank the schemes in ascending order by their decryption times for a message length between 15 bytes and 60 bytes: $Boneh{+}_{\text{Thin Client}}$, $Boneh{+}_{\text{Fat Client}}$, and $BASE < Saber < Nishat < AJPS < NTRU$. $Nishat$ sometimes swaps places with $AJPS$ in the ranking for message lengths smaller than 15 bytes. Again, $Boneh{+}_{\text{Thin Client}}$, $Boneh{+}_{\text{Fat Client}}$, and $BASE$ have the same decryption times since they all use AES. Also, in terms of decryption, the fastest pre-quantum schemes are faster than the fastest post-quantum scheme. However, the difference between the fastest post-quantum scheme $Saber$ and one of the fastest pre-quantum schemes is at most 10 ms.

The last computation time analysis considers the duration of group operations for pre- and post-quantum schemes. We only consider the operational phase for group members since the deployment phase consists only of storing parameters. Table III lists the respective times required for post-quantum schemes, and Figure 5 illustrates the times required for pre-quantum schemes. In analogy to the benchmark, we consider group sizes of up to 550 members. The table and graph allow us to assume that, except for scheme $Boneh{+}_{\text{Fat Client}}$, all pre- and post-quantum schemes require constant time to perform group management operations. For $Boneh{+}_{\text{Fat Client}}$, the time required for group management operations increases with the group size. We rank the schemes in ascending order by their group operation durations: $BASE < Saber < Nishat < Boneh{+}_{\text{Fat Client}} < Boneh{+}_{\text{Thin Client}} < NTRU < AJPS$. Furthermore, again, the best pre-quantum scheme $BASE$ is faster than the best post-quantum procedure. However, the difference between the two is once more marginal with a maximum of 2 ms.

2) Energy Efficiency:: For reasons of space, we only consider the energy efficiency of the encryption and decryption process in the following. Figures 6a and 6b



(a) Decryption times of post-quantum group encryption schemes.



(b) Decryption times of pre-quantum group encryption schemes.

Fig. 4: Decryption times of pre- and post- quantum group encryption schemes.

TABLE III: Computation times of group members during the group creation operation in the operational phase for post-quantum group encryption schemes. (Note that the notation of the values follows the following scheme: Value $\pm$ accuracy)

Post quantum scheme	Initial group joining time
AJPS [12]	(37.83 ± 0.65) seconds
Saber [14]	(10.13 ± 0.24) milliseconds
NTRU [13]	(3.81 ± 0.23) seconds

illustrate the energy efficiency of the encryption process of post- and pre-quantum schemes. These figures allow the statement that the efficiency for all schemes, except $AJPS$, increases with the message length. For AJPS, the efficiency decreases with increasing message length. The schemes can be ranked in terms of the energy efficiency of the encryption process as follows: $AJPS < NTRU < Nishat < Saber < Base, Boneh{+}_{\text{Fat Client}}, Boneh{+}_{\text{Thin Client}}$. Pre-quantum schemes $Base$, $Boneh{+}_{\text{Fat Client}}$, and $Boneh{+}_{\text{Thin Client}}$ are the most efficient schemes because they use AES to encrypt

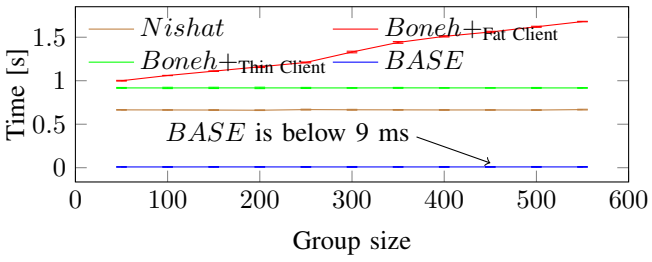
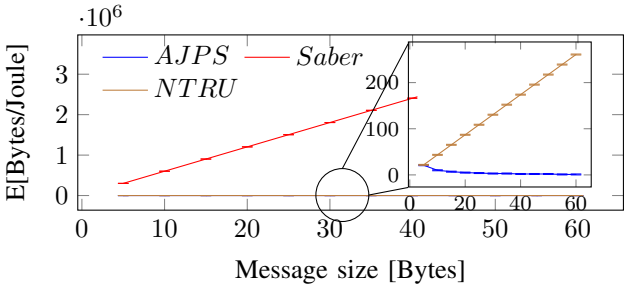
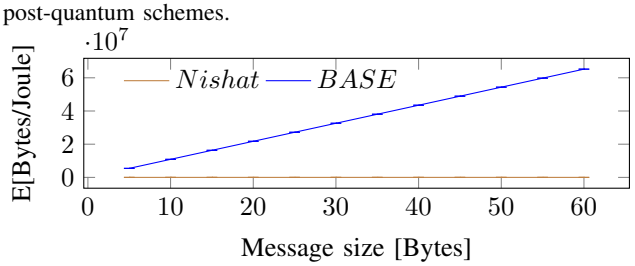


Fig. 5: Computation times of group members during the group creation operation in the operational phase for pre-quantum group encryption schemes.



(a) Energy efficiency of group member encryption process for post-quantum schemes.



(b) Energy efficiency of group member encryption process for pre-quantum schemes.

Fig. 6: Energy efficiency of group member encryption process for pre- and post-quantum schemes.

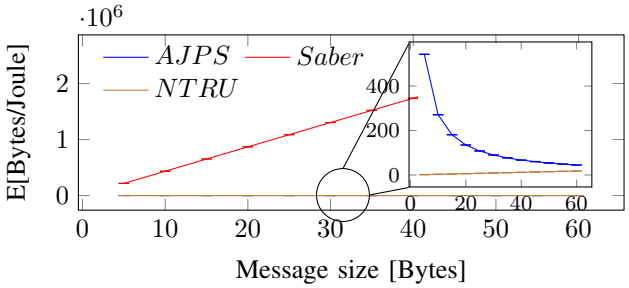
their messages. The difference between the most efficient post-quantum scheme Saber and one of the most efficient pre-quantum schemes like BASE is enormous since it is more than 18 times as efficient as Saber.

Figures 7a and 7b illustrate the energy efficiency of the decryption process. Apart from two differences, the same statements apply for the energy efficiency of the decryption process as for the encryption process. These two differences are in the ranking for the decryption process: $NTRU$ and $AJPS$ swap places, and BASE is not only 18 but even more than 25 times as efficient as Saber.

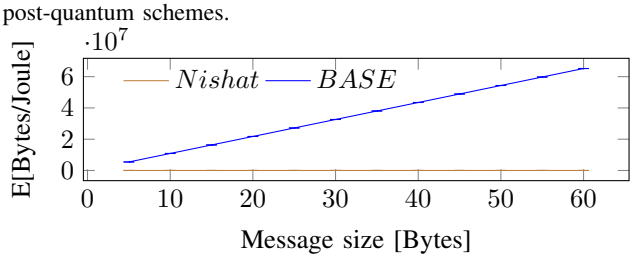
B. Central Instance Performance

For space reasons, we consider only the initial group creation time. Here, we distinguish between the deployment phase and the operational phase.

1) Deployment Phase:: Figures 8a and 8b illustrate the time required to compute the secret information, such as secret keys, delivered with the group members' IoT devices. As in the benchmark, we consider group sizes of up to 550 members. The two figures show that the time required for the deployment calculations increases linearly with the group size for all schemes. For the measurement range under consideration, we rank the pre- and post-quantum schemes in ascending order considering calculation time: $NTRU < Saber < BASE < Boneh{+}_{\text{Fat Client}}, Boneh{+}_{\text{Thin Client}} < AJPS < Nishat$. In the deployment phase, the fastest schemes, in contrast to encryption and decryption, are post-quantum schemes. Still, the difference between the fastest pre-quantum scheme $BASE$ and the second-fastest scheme, the post-quantum scheme

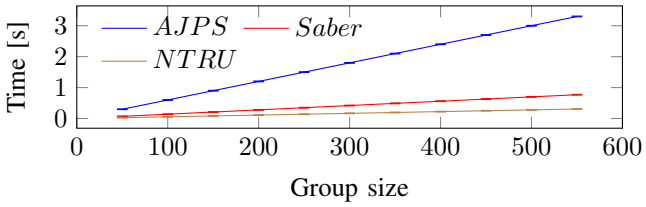


(a) Energy efficiency of group member decryption process for post-quantum schemes.

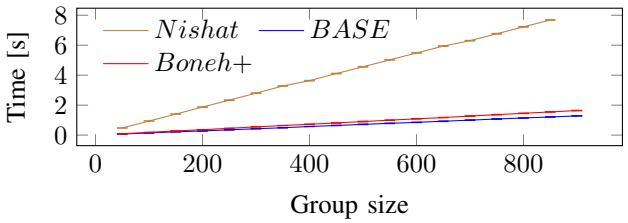


(b) Energy efficiency of group member decryption process for pre-quantum schemes.

Fig. 7: Energy efficiency of group member decryption process for pre- and post-quantum schemes.



(a) Computation times by CI during the group creation operation in the deployment phase for post-quantum group encryption schemes.

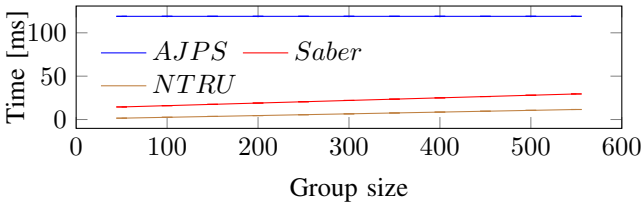


(b) Computation times by CI during the group creation operation in the deployment phase for pre-quantum group encryption schemes.

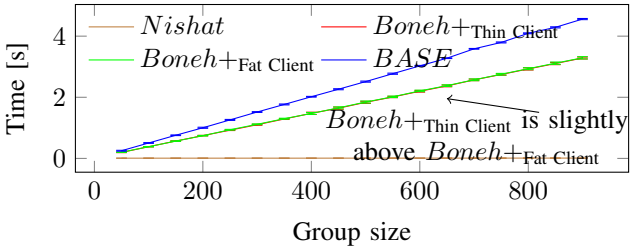
Fig. 8: Computation times by CI during the group creation operation in the deployment phase for pre- and post-quantum group encryption schemes.

Saber, does not exceed 15 ms in the measurement range under consideration.

2) Operational Phase:: Figures 9a and 9b show the time requiredto create a group using the secret information subsequently. Again, we consider group sizes with up to 550 members. The two figures show that for all schemes, the required



(a) Computation times by CI during the group creation operation in the operational phase for post-quantum group encryption schemes.



(b) Computation times by CI during the group creation operation in the operational phase for pre-quantum group encryption schemes.

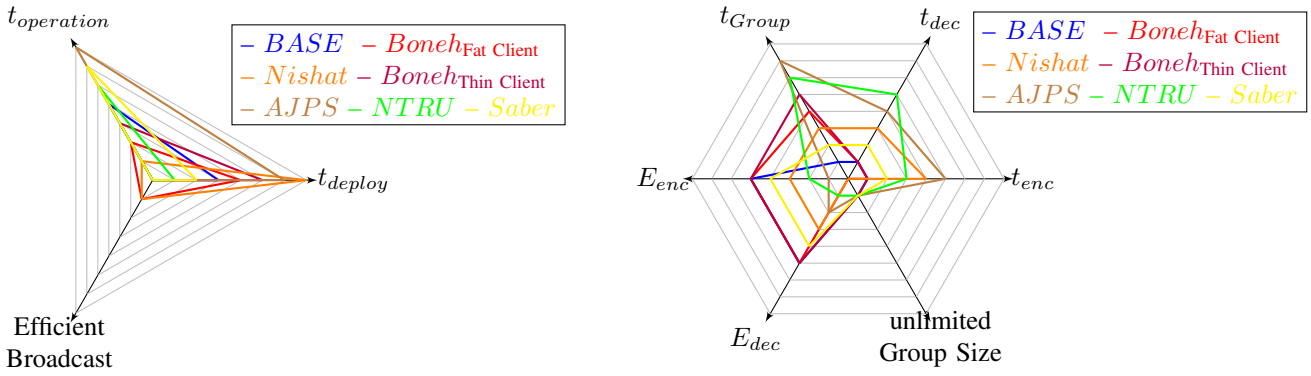
Fig. 9: Computation times by CI during the group creation operation in the operational phase for pre- and post-quantum group encryption schemes.

time increases linearly with the number of members. We rank the pre- and post-quantum schemes in ascending order considering the required time: $Nishat < Boneh+_{\text{Fat Client}} < Boneh+_{\text{Thin Client}} < BASE < NTRU < Saber < AJPS$. In contrast to the deployment phase, a pre-quantum scheme is the fastest scheme for the operational phase. The difference between the fastest pre-quantum and fastest post-quantum schemes is over 10 seconds, about four orders of magnitude more than differences mentioned earlier.

C. Discussion

After comparing the pre- and post-quantum schemes concerning individual aspects, we now perform a cross-aspect comparison. Thus, we illustrated the schemes in terms of their rank from CI and group member point of view in Figure 10. When the ranking was not identical for each measurement of a use case, the ranking applies to most measurements.

Figure 10a gives three take-aways for the CI: (1) no scheme performs best in all phases, (2) the schemes have their main effort in either the deployment or operational phase, and (3) no scheme category scores best in all dimensions. For example, in the deployment phase, the fastest scheme is a pre-quantum scheme. It is a post-quantum scheme in the operational phase, and only pre-quantum schemes can use efficient broadcast. Thereby, the difference between pre- and post-quantum schemes varies depending on the phase. In the deployment phase, the difference is limited to 15 ms, while in the operational phase, it extends to more than 10 seconds. However, when neglecting the difference in the deployment



(a) Ranking for the CI.

(b) Ranking for group members.

Fig. 10: Post- and pre-quantum scheme ranking.

phase, the pre-quantum schemes perform better than the post-quantum schemes.

From the point of view of a group member, the situation looks different (see Figure 10b). This figure allows the statement that pre-quantum schemes, or more precisely the scheme BASE, perform best with group members in all dimensions. The second-best scheme for group members is the post-quantum scheme Saber. Despite the clear ranking for first and second place, it is noteworthy that the difference between BASE and SABER in terms of calculation times is not very large, however, with a maximum of 10 ms. This difference can be negligible for use cases in which the ESP32 does not have a limited energy supply. For use cases in which the ESP32 has a limited power supply, this difference can be relevant since the ESP32 could encrypt 18 times more messages with BASE than with SABER and decrypt 25 times more messages.

Overall, our comparison of pre- and post-quantum group ciphers shows that pre-quantum schemes perform better than post-quantum schemes. However, our comparison also shows that the difference between pre- and post-quantum schemes is sometimes vanishingly slighty in specific dimensions. Post-quantum group ciphers are suitable for small IoT typical microcontrollers.

VI. Related Work

In this section, we review related work and highlight the novelty of our contribution. In [20], the authors evaluated the performance of different post-quantum cryptosystems on a Samsung Galaxy A5 smartphone. The metrics considered were computational time, required memory, and power consumption. We only consider the metrics of computation time and energy efficiency. However, for these, we consider (1) the accuracy of all results, (2) indicate how this accuracy was determined, and (3) the requirements and features of the schemes. Additionally, we consider a range of payload sizes for the decryption and encryption process rather than just one payload size. Furthermore, with the ESP32 microcontroller, we have chosen significantly weaker hardware than an Android phone and could thus prove the feasibility of a post-quantum cryptosystem for microcontrollers. Furthermore, we differ in that we use post-quantum schemes not only for 1-to-1 encryptions but for n-to-n encryptions and compare pre-quantum n-to-n encryption with post-quantum n-to-n encryption.

The authors of [21] also compare different post-quantum methods among each other and with pre-quantum methods. In terms of metrics, they only focus on storage requirements of keys and transmitted data, like ciphertext signatures. However, the paper does not show how they determined the storage space requirements in individual cases, and there are no statements about the accuracy of the data. We consider the metrics of computation times and energy efficiency and analyze the schemes according to a standardized benchmark that (1) includes the accuracy of the results, (2) clearly defines how to determine this accuracy, (3) considers requirements and features of the procedures. Furthermore, we consider not just 1-to-1 encryption but n-to-n encryption and analyze the suitability of post-quantum group encryption for resource-constrained microcontrollers.

In [22], the authors introduce a new post-quantum public cryptosystem called spLWE. In addition to presenting the method itself, they compare its performance with other post-quantum methods on a Macbook Pro in terms of memory requirements and computation times. Concerning to encryption and decryption, the evaluation restricts itself to messages with a fixed message size of 254 bits and omits information about the accuracy of the presented performance values. We differ from this work in that we (1) use computation times and energy efficiencies as metrics, (2) specify precisely how accurate the determined performance values are, (3) compare post-quantum schemes not only among each other but also with pre-quantum schemes, (4) consider different message sizes, and (5) use significantly more resource-constrained hardware with the ESP32 to evaluate the suitability of the methods for IoT. In addition, we analyze the performance of post-quantum schemes not only for 1-to-1 but n-to-n encryptions.

The authors of [23] compared the second NIST standardization round finalists' performance regarding computation times, memory requirements, and energy consumption on a Zynq-

7000. On the other hand, we measure the performance with the ESP32 on much weaker, IoT-typical hardware. We focus on the calculation times and the energy efficiency as metrics and specify the accuracy of all performance values. In addition, we compare post-quantum methods not only with each other but also with pre-quantum methods. Furthermore, we consider n-to-n communication.

VII. Conclusion

The increasing computing power of quantum computers can be an essential component accelerating many conventional applications. However, with their high computation power, quantum computers also support attacks on security guarantees provided by today's cryptographic systems. Besides security guarantees, it is also crucial that post-quantum cryptosystems have good performance and work on all devices, from powerful PCs to resource-constrained IoT devices. In addition, post-quantum encryption must support not only 1-to-1 communication but also IoT typical n-to-n communication in dynamic groups, so far mostly ignored in research. With this paper, we fill this gap and analyze post-quantum encryption schemes concerning their performance for n-to-n communication and compare their performance to traditional pre-quantum n-to-n encryption schemes. We chose an IoT use case as the evaluation scenario to evaluate the post-quantum schemes' suitability for resource-limited hardware. Our results show that the pre-quantum schemes perform better in terms of performance than the post-quantum schemes, but the differences are often only marginal. However, these marginal differences in computation times lead to the lower energy efficiency of the post-quantum schemes. In terms of features, there is no difference between pre- and post-quantum schemes. Concerning the requirements, post-quantum schemes require unicast, whereas some pre-quantum schemes support broadcast transmission increasing efficiency. Thus, the decision whether to use pre- or post-quantum schemes for n-to-n encryption in IoT use cases depends on (i) whether energy efficiency is critical - e.g., in the case of limited power supply - and (ii) whether unicast or broadcast is available.

As future work, we plan to extend our analysis in different network situations using the tools [24] and [25] and generalize the results to other domains besides IoT systems. Further, we plan to use the results in self-aware computing systems [26], which would switch the scheme according the environmental constraints and system parameters. This awareness enables an adaptive choice of the best fitting scheme.

Acknowledgment

This research has been funded by the Federal Ministry of Education and Research of Germany in the framework KMU-innovativ - Verbundprojekt: Secure Internet of Things Management Platform - SIMPL (project number 16KIS0852) [27].

References

[1] W. Roush, "The Google-IBM "quantum supremacy" feud," 2020, online available under https://www.technologyreview.com/2020/02/26/905777/google-ibm-quantum-supremacy-computing-feud, Accessed on 27.11.2020.

[2] F. Arute *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.

[3] K. Hartnett, "A New "Law" Suggests Quantum Supremacy Could Happen This Year," 2019, online available under https://www.scientificamerican.com/article/a-new-law-suggests-quantum-supremacy-could-happen-this-year/, Accessed on 27.11.2020.

[4] L. Tvede, "The Present And Future Of Quantum Computing Expansion," 2020, online available under https://https://www.forbes.com/sites/forbesbusinesscouncil/2020/07/14/the-present-and-future-of-quantum-computing-expansion/?sh=2d621a4443b9, Accessed on 27.11.2020.

[5] Y. Lee, M. G. Kim, S. Rho, D.-j. Kim, and Y.-k. Lim, "Friends in activity trackers: design opportunities and mediator issues in health products and services," *Proc. IASDR*, pp. 1206–1219, 2015.

[6] A. Polacco and K. Backes, "The amazon go concept: Implications, applications, and sustainability," *Journal of Business and Management*.

[7] N. I. of Standards and Technology, "NIST's Post-Quantum Cryptography Program Enters 'Selection Round'," 2020, online available under https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round, Accessed on 27.11.2020.

[8] T. Prantl *et al.*, "Towards a Group Encryption Scheme Benchmark: A View on Centralized Schemes with focus on IoT," in *2021 ACM/SPEC International Conference on Performance Engineering (ICPE)*, 2021.

[9] S.-Q. Li *et al.*, "A survey on key management for multicast," in *2010 Second International Conference on Information Technology and Computer Science*, 2010.

[10] K. Nishat *et al.*, "Group-oriented encryption for dynamic groups with constant rekeying cost," *Security and Communication Networks*.

[11] T. Prantl *et al.*, "Evaluating the Performance of a State-of-the-Art Group-oriented Encryption Scheme for Dynamic Groups in an IoT Scenario," in *MASCOTS*, ser. MASCOTS '20, November 2020.

[12] D. Aggarwal *et al.*, "A new public-key cryptosystem via Mersenne numbers," in *Annual International Cryptology Conference*. Springer.

[13] J. Hoffstein *et al.*, "NTRU: A ring-based public key cryptosystem," in *Algorithmic Number Theory*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 267–288.

[14] B. Wang *et al.*, "Saber on ESP32," in *Applied Cryptography and Network Security*. Cham: Springer International Publishing, 2020, pp. 421–440.

[15] T. Buktu *et al.*, "ntru Quantum-resistant cryptography," Tech. Rep., 2021.

[16] B. Wang *et al.*, "Saber on ESP32," in *Applied Cryptography and Network Security*. Cham: Springer International Publishing, 2020, pp. 421–440.

[17] B. Ward *et al.*, "POST-QUANTUM CRYPTOGRAPHY," Iraklio, Greece, Tech. Rep., 2021.

[18] T. Prantl *et al.*, "Performance Evaluation of a Post-Quantum Public-Key Cryptosystem," in *2021 IEEE 40th International Performance Computing and Communications Conference (IPCCC)*. IEEE, 2021.

[19] I. Management Association, *The Internet of Things: Breakthroughs in Research and Practice: Breakthroughs in Research and Practice*.

[20] N. Chikouche *et al.*, "Performance Evaluation of Post-quantum Public-Key Cryptography in Smart Mobile Devices," in *Challenges and Opportunities in the Digital Era*. Springer International Publishing.

[21] R. Niederhagen and M. Waidner, "Practical Post-Quantum Cryptography," *Fraunhofer SIT*, 2017.

[22] J. H. Cheon *et al.*, "A Practical Post-Quantum Public-Key Cryptosystem Based on spLWE."

[23] V. B. Dang *et al.*, "Implementation and Benchmarking of Round 2 Candidates in the NIST Post-Quantum Cryptography Standardization Process Using Hardware and Software/Hardware Co-design Approaches," Cryptology ePrint Archive, Report 2020/795, 2020, https://eprint.iacr.org/2020/795.

[24] S. Herrnleben *et al.*, "An IoT Network Emulator for Analyzing the Influence of Varying Network Quality," in *Simulation Tools and Techniques*. Cham: Springer International Publishing, 2021, pp. 580–599.

[25] S. Herrnleben, M. Leidinger *et al.*, "ComBench: A Benchmarking Framework for Publish/Subscribe Communication Protocols under Network Limitations," ser. VALUETOOLS '21. New York, NY, USA: Association for Computing Machinery, 2021.

[26] C. Krupitzer *et al.*, "An Overview of Design Patterns for Self-Adaptive Systems in the Context of the Internet of Things," *IEEE Access*, vol. 8, pp. 187 384–187 399, 2020.

[27] T. Prantl *et al.*, "SIMPL: Secure IoT Management Platform," in *ITG Workshop on IT Security (ITSec)*, 2020, doi:http://dx.doi.org/10.15496/publikation-41816.