Tzinos *et al. J Surveill Secur Saf* 2022;3:101-27
**DOI:** 10.20517/jsss.2022.15

**Journal of Surveillance, Security and Safety**

**Original Article**

**Open Access**



# Evaluating the performance of post-quantum secure algorithms in the TLS protocol

**Iraklis Tzinos[1], Konstantinos Limniotis[1,2,3], Nicholas Kolokotronis[4]**

[1]School of Pure and Applied Sciences, Open University of Cyprus, Latsia, Nicosia 2220, Cyprus.
[2]Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, Athens 15784, Greece.
[3]Department of Informatics and Computer Engineering, University of West Attica, Athens 12243, Greece.
[4]Department of Informatics and Telecommunications, University of the Peloponnese, Tripolis 22100, Greece.

**Correspondence to:** Dr. Konstantinos Limniotis, School of Pure and Applied Sciences, Open University of Cyprus, Latsia, Nicosia 2220, Cyprus. E-mail: konstantinos.limniotis@ouc.ac.cy; ORCID: 0000-0002-7663-7169

**How to cite this article:** Tzinos I, Limniotis K, Kolokotronis N. Evaluating the performance of post-quantum secure algorithms in the TLS protocol. *J Surveill Secur Saf* 2022;3:101-27. http://dx.doi.org/10.20517/jsss.2022.15

**Received:** 3 May 2022 **First Decision:** 5 Aug 2022 **Revised:** 26 Aug 2022 **Accepted:** 19 Sep 2022 **Published:** 29 Sep 2022

**Academic Editor:** Rongmao Chen **Copy Editor:** Jia-Xin Zhang **Production Editor:** Jia-Xin Zhang

## Abstract

**Aim:** The imminent advent of large-scale quantum computers within the next years is expected to highly affect the security of several cryptosystems that are now considered secure; this mainly holds for classical, long-established, public key cryptographic algorithms such as RSA and elliptic curve cryptography. Apparently, any security protocol that relies on such ciphers, including the transport layer security (TLS) protocol which constitutes a somewhat de facto standard for the security on the web, will not be considered secure in the post-quantum era. To alleviate the security risks stemming from quantum computing, several proposals have been submitted to the relevant procedure initiated by NIST towards evaluating and standardizing one or more quantum-resistant public-key cryptographic algorithms. This paper focuses on embedding post-quantum secure cryptographic algorithms into the TLS protocol to analyze its performance. More precisely, the paper aims to analyze whether this transition to post-quantum secure algorithms will have a significant impact on the user experience due to the possible increase of client–server communication times.

**Methods:** Having as the starting point several important works in the field, several experiments were carried out, using combinations of cloud and local virtual machines per case and considering all the post-quantum cryptographic algorithm finalists for key exchange from the third round of the ongoing NIST process, for various cryptographic as well as network parameters.

**Results:** Our results exhibit that, for key exchange in TLS, the best performance among the post-quantum secure ciphers is achieved by the Saber and CRYSTAL-Kyber variants for all security levels, regardless of the underlying computing power. The performance is comparable to that of the corresponding one achieved by a classical elliptic curve algorithm for key exchange for both RTT and packet loss ratio — i.e., the network parameters seem to have the same effect on post-quantum secure algorithms as in the case of a conventional elliptic curve algorithm. However, the effect of the network parameters on the performance is more crucial than the effect of the underlying chosen ciphers.

**Conclusion:** According to the experiments, we conclude that there exist very promising algorithms that could be utilized in TLS in the near future, which may behave even better than the conventional elliptic curve algorithms for key exchange. It should also be pointed out that NIST announced on 5 July 2022 (i.e., after the completion of our research experiments) that, for general encryption used when we access secure websites, the CRYSTALS-Kyber algorithm has been selected, having as one of its advantages the speed of operation. Hence, the results of our paper are fully in line with the progress of the NIST process. Taking into account that the NIST process is still ongoing (now in its fourth round) with the aim to select more algorithms, as well as that some algorithms may be standardized outside NIST, it becomes evident that our results provide very useful insights on performance aspects of the post-quantum secure algorithms.

**Keywords:** Performance, post-quantum cryptography, public-key cryptography, transport layer security protocol

## 1. INTRODUCTION

Cryptography is a main information security mechanism, providing services to achieve several security goals such as confidentiality, data and entity authentication, and non-repudiation; however, it actually goes far beyond these goals and is able to provide solutions in terms of fulfilling legal requirements with respect to personal data protection and privacy[1]. To this end, cryptographic algorithms constitute core elements in network security protocols, including the prominent transport layer security (TLS) protocol[2], which constitutes a somewhat de facto standard for web security[3]. Indeed, TLS ensures: (i) entity authentication through digital certificates that are digitally signed (via a public key digital signature algorithm) by trusted certification authorities; (ii) confidentiality through encrypting (via the use of symmetric ciphers) the content of the communications, while the symmetric key for encryption/decryption is being securely exchanged via public key (i.e., asymmetric) cryptographic techniques; and (iii) data integrity, via ensuring that the encryption is authenticated (via message authentication codes or suitable modes of operations allowing for authenticated encryption). Any weakness in cryptographic algorithms affects the overall security of the protocol (see, e.g.,[4] for a survey on such cryptographic threats for TLS).

The imminent advent of quantum computers will highly change the situation with regard to which cryptographic algorithms should be considered secure. Indeed, having large-scale quantum computers will allow executing algorithms that can efficiently solve difficult problems that cannot be solved today by contemporary conventional computing systems. More precisely, due to a quantum algorithm proposed by Peter Shor in 1994[5], all commonly used public-key systems (including RSA, elliptic curve cryptography, and the Diffie–Hellman algorithm that is being used in the TLS protocol) will no longer be secure. Symmetric cryptography is also affected, but not to the same extent: there is a known quantum algorithm developed by Grover in 1996[6] that suffices to decrease the security level of symmetric algorithms by up to half, which means that contemporary symmetric cryptographic primitives may still provide security to the post-quantum era by doubling, if needed, the key sizes (for symmetric ciphers) or the sizes of the message digests (for cryptographic hash functions).

Post-quantum cryptography refers to cryptographic algorithms which are secure under the assumption that the attacker has a quantum computer. Although the quantum computers that (are known to) exist currently are not large enough to violate the security of contemporary cryptography, it is essential to start considering the implementation of post-quantum cryptographic algorithms. The basic idea is to develop public-key algorithms whose security relies on a difficult mathematical problem that will remain difficult even if large-scale quantum computers become a reality. Hence, the US National Institute of Standards and Technology (NIST) launched in 2017 a process to standardize one or more quantum-resistant public-key cryptographic algorithms by collecting and evaluating submissions from the cryptographic community around the world[7]. This evaluation process is still ongoing, being in its third round of evaluation when the present research was conducted (and since July 2022, during the review phase of this paper, a fourth round has been initiated). The NIST process aims to find post-quantum secure public key algorithms that can be used either for digital signatures or to provide confidentiality, which in turn also incorporate secure key exchange (KEX) techniques as well as key encapsulation mechanisms (KEMs).

NIST evaluates the security strength of post-quantum secure algorithms on the basis of five categories which are characterized in terms of the equivalent strength of a symmetric primitive. In particular, according to NIST, a separate category for each of the following security requirements is defined (from the lowest strength to the highest strength):

- Level 1 (L1): Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 128-bit key (e.g., AES128).
- Level 2 (L2): Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 256-bit hash function (e.g., SHA256/SHA3-256).
- Level 3 (L3): Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 192-bit key (e.g., AES192).
- Level 4 (L4): Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 384-bit hash function (e.g., SHA384/SHA3-384).
- Level 5 (L5): Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 256-bit key (e.g., AES 256).

Currently, the NIST competition is in the fourth round, as subsequently described.

During these years, the research community has also started exploring whether known public-key post-quantum secure cryptographic algorithms can be implemented in contemporary systems to enrich current security protocols by post-quantum secure ciphers. The actual motivation is that it is essential to start deploying quantum-safe solutions even before large-scale quantum computers become available. This is nicely explained by the famous Mosca equation (see, e.g.,[8]): if $x$ denotes how long we need our cryptographic keys to be to remain secure, $y$ denotes how long it will take to deploy a set of tools that are quantum-safe (i.e., the migration time), and $z$ denotes the so-called collapsed time, i.e. the time needed to have a quantum computer, or some other method, that will break the currently deployed public-key cryptographic algorithms, then we have a serious problem if $x + y > z$. Moreover, with respect to the time $z$, Mosca estimated since 2015[8] that there is a 1/7 chance of breaking RSA-2048 by 2026 and a 1/2 chance by 2031. Therefore, incorporating post-quantum ciphers in the TLS protocol is currently a significant research field (see, e.g.,[9–14]).

This paper focuses on the embedding of post-quantum secure cryptographic algorithms into the TLS protocol. More precisely, in this study, we performed a comprehensive set of experiments towards examining all possible post-quantum cryptographic algorithms for key exchange that are being analyzed by NIST, in terms of how efficiently they can be implemented into the TLS 1.3 protocol. More precisely, we studied all the finalists of the third round of the NIST competition, which was ongoing when this research was conducted. For our experiments, we used combinations of cloud and local virtual machines per case. The implementations of the algorithms were based on the Open Quantum Safe project[15] and our experiments constituted a more extended set of experiments with respect to those presented in[10], which formed the main basis for our research. Our ultimate goal was to derive conclusions on whether the transition to post-quantum secure algorithms will have a significant impact on the user experience due to the possible increase of client–server handshake communication times, for various network types that are being investigated — and this for each possible post-quantum secure cipher. Our results confirm that, in terms of performance, there are some very promising algorithms that could be utilized in the near future.

The paper is organized as follows. The basic background, with respect to both post-quantum cryptography and the TLS protocol, is given in Section 2. A presentation of relative previous work in the field is given in Section 3. The description of how the experimental environment was set up, based on previous relevant works, is given in Section 4, along with a discussion on the motivation for these experiments and their added value compared to previous works, whereas the results of our experiments are presented in Section 5. A discussion on the results, stating the main conclusions derived, is given in Section 6. Finally, concluding remarks and suggestions for future research steps are given in Section 7.

## 2. BACKGROUND

### 2.1. Post-quantum cryptography

The post-quantum public key cryptographic algorithms are mainly classified into one of the following categories:

- Code-based cryptography includes cryptographic algorithms whose security rests with the difficult problem of decoding an erroneous codeword that has been generated through an unknown error correcting code.
- Lattice-based cryptography includes cryptographic algorithms whose security relies on the difficulty of specific mathematical problems in the field of lattices. Such problems are the shortest vector problem (SVP), being NP-hard, which is related to the finding of the shortest non-zero vector within a lattice, as well as other similar lattice-based difficult problems such as the closest vector problem (CVP) and the shortest integer solution (SIS). An important lattice-based problem is the "learning with errors" (LWE) problem[16], which has security reductions to variants of SVP.
- Multivariate cryptography includes cryptographic algorithms whose security relies on the complexity of solving systems of multivariate equations, which have been demonstrated to be either NP-hard or NP-complete. Some of the most promising multivariate-based schemes are based on hidden field equations (HFE) (for a generic survey of mathematical problems in the field of multivariate cryptography, see[17]).
- Hash-based cryptography includes digital signature cryptographic algorithms whose security is based on known properties of cryptographic hash functions, such as pre-image resistance, second-order pre-image resistance, and collision resistance.
- Supersingular elliptic curve isogeny cryptography includes cryptographic algorithms whose security relies on the isogeny protocol for ordinary elliptic curves presented in[18] but enhanced to withstand the quantum attack detailed in[19].

In addition, there exist a few algorithms that are based on the security of zero-knowledge proofs. Such post-quantum cryptographic schemes are generalizations of hash-based cryptographic schemes, enriched by nice cryptographic properties of symmetric ciphers towards constructing zero-knowledge proofs.

The NIST standardization process for post-quantum public key cryptography provided its first outcomes at the end of its in third round in July 2022. In this round, seven algorithms, being called finalists, were reviewed for consideration for standardization. Four of them are being considered for encryption, key exchange, and key encapsulation mechanisms — namely Crystals-Kyber, NTRU, Saber (which are lattice-based cryptographic algorithms), and McEliece (which is code-based) — while the remaining three are being considered for digital signatures — namely Crystals-Dilithium and Falcon (which are lattice-based cryptographic algorithms) and Rainbow (which is based on multivariate cryptography). Moreover, during the third round, there were still eight alternates, spanning all possible categories of post-quantum cryptography, for which NIST stated that *they may still potentially be standardized, although that most likely will not occur at the end of the third round. NIST expects to have a fourth round of evaluation for some of the candidates on this track. Several of these alternate candidates have worse performance than the finalists but might be selected for standardization based on high confidence in their security. Other candidates have acceptable performance but require additional analysis or work to inspire sufficient confidence in their security or security rationale. In addition, some alternates were selected based on NIST's desire for a broader range of hardness assumptions in future post-quantum security standards, their suitability for targeted use cases, or their potential for further improvement.*

During the research conducted for this work and the drafting of this paper, the NIST process was in its third round, and thus, as subsequently described in detail, all the aforementioned finalists for key exchange and KEM were considered for our analysis. However, on 5 July 2022, NIST announced, at the end of this round, the first four quantum-resistant cryptographic algorithms — i.e., the "winners" of this round. These are:

- For general encryption, used when we access secure websites, the CRYSTALS-Kyber algorithm was selected.
- For digital signatures, often used when there is a need to verify identities during a digital transaction or to sign a document remotely, the CRYSTALS-Dilithium, FALCON, and SPHINCS+ (the last one is from the list of the alternates) were selected.

At the same time, NIST announced candidates for a fourth round of analysis — i.e., new algorithms are also expected to be selected for public key encryption and key encapsulation mechanism, in addition to the already chosen CRYSTALS-Kyber. The fourth round of the NIST process analyzes McEliece, BIKE, HQC, and SIKE (the last three had been alternatives during the third round). One reason that NIST intends to standardize some more algorithms is to increase the diversity in security assumptions in the case there is a breakthrough in attacks on structured lattices on which Kyber is based.

### 2.2. The TLS protocol

The TLS protocol, aims to ensure confidentiality as well as data and entity authentication. The latest version of the protocol is 1.3 (RFC 8446), being approved by the Internet Engineering Task Force (IETF) in March 2018[2].

The main procedures that the TLS protocol follows can be simply described by the following two phases: the first one is the connection setup (known as the handshake protocol), which is followed by steady-state communication (known as the record protocol). During the handshake protocol, the client and server negotiate to commonly decide on a number of parameters, such as the cryptographic algorithms that are to be used, as well as the relevant secret information from which the secret symmetric keys are being computed. After the setup phase, communication begins (record protocol), which is encrypted and authenticated through symmetric cryptographic primitives. The public key encryption is present in TLS at the handshake phase, since: (i) the client authenticates the server through its digital certificate, signed by a certificate authority; and (ii) it is being used so that the client and the server will commonly securely agree on the secret parameters for the symmetric authenticated encryption that is to be used in their communication that will follow.

There are no known practical weaknesses to TLS 1.3; all earlier versions of the protocol (including TLS 1.2) have some weaknesses, which are either inherent to the protocol's design (for some old versions) or may occur in the case of misconfigurations of the protocol (see [4] for a survey on these weaknesses). All versions, however, are not post-quantum secure, due to the existence of public-key ciphers such as RSA and elliptic curve (EC) cryptography.

## 3. RELEVANT PREVIOUS WORK

Embedding post-quantum secure ciphers in the TLS protocol has already been studied by many researchers, due to its high importance. Our research heavily relied on the work presented in [10], which presents a framework for running relevant experiments in TLS by emulating network conditions; more precisely, the testbed developed therein allows controlling variables such as link latency and packet loss rate, and then examining the performance impact of various post-quantum ciphers, both for key establishment and for digital signatures, based on the implementations from the Open Quantum Safe project [15]. As illustrated by the work in [10], the network latency hides most of the impact from algorithms with slow performance, while, for some of the algorithms studied therein, a packet loss rate above 3–5% seems to have an impact on the performance.

In [12], an assessment, through relative experiments, of the concurrent use of quantum-resistant key exchange and authentication in TLS 1.3, as well as SSH protocols, under realistic network conditions, is carried out. It is shown that there exist combinations of algorithms that offer handshake performance close to the current standards (a minimum slowdown of about 1% has been monitored). It is interesting to point out that these "nice" combinations include the lattice-based Kyber cipher, which has been subsequently selected by NIST as the first post-quantum secure standard for public key encryption and KEM. A similar approach is also followed in [13] but for post-quantum digital signature algorithms. The performance of post-quantum digital signature algorithms is also studied in [20], and a security comparison of these algorithms is also performed therein.

In parallel with our work, a nice study on the performance of the TLS based on post-quantum secure algorithms is presented in [21]; this work utilizes the liboqs software library [22] that was also used in our experiments, as subsequently described. A main outcome of this work is that Saber or CRYSTALS-KYBER for key exchange together with the FALCON signature seems to be a right combination for achieving the best performance, while in general lattice-based cryptography can be compared to RSA and elliptic curve cryptography, outperforming these classical schemes at higher security levels. The work in [21], however, does not take into account network parameters.

Another relative work in the field is found in [14], which focuses explicitly on the Google-Cloudflare CECPQ2 experiment for integrating post-quantum key-exchange algorithm into TLS 1.3 for developing a solution achieving higher performance; however, since this experiment utilizes a variant of one of the algorithms in the NTRU proposal, the proposed solution is also based on NTRU. Finally, an integration of the post-quantum KEM scheme Kyber for key establishment and the post-quantum signature scheme SPHINCS+ into the embedded TLS library (mbed TLS) is presented in [11], illustrating that embedded systems can (at least) act as post-quantum secure TLS clients, for those studied algorithms.

## 4. THE TESTING ENVIRONMENT

This seciton describes the experiments that were carried out to evaluate the performance of TLS 1.3 (under several configuration parameters) if its public key algorithms for symmetric key exchange are being replaced by post-quantum secure ciphers — namely, by the finalists in the third round of the NIST evaluation process.

The testing environment consisted of one Google cloud device (Intel Xeon Cascade Lake n2-custom, with 8 vCPUs and 16 GB memory at 2.8 GHz) and two local devices, being executed as virtual devices through the Oracle Virtual Box (version 6.1). The first one was running over a desktop PC with Intel Core i-7 6700k at 4

GHz, whereas the second was running over a laptop with Intel Core i5-8250U at 1.6*G*Hz. Each virtual device was assigned with 2 Gb memory and a single-core processor. For all virtual devices (i.e., the two local devices and the cloud device), the operating system was Ubuntu 18.04.5 LTS (Bionic Beaver). All processors made use of Advanced Vector Extensions 2 (AVX2), an extension of AVX, which was first introduced in Intel Haswell family of processors; this is an important feature since many of the algorithms that were being studied in this experiment take advantage of this technology to improve their efficiency. It should be pointed out that the utilization of processors with varying processing capabilities allowed conducting experiments to see how the processor power affects the performance of post-quantum TLS.

To implement simulations that resemble realistic scenarios with regard to client–server connections, Linux network namespaces were used with the aim to develop different network entities, which in turn can be interconnected through virtual Ethernet. A network emulator was used to perform experiments for several probabilities of packet loss and for several round-trip times (RTTs).

The experiments are based on the following:

1. On a fork of the pq-tls-benchmark [23] which contains code and associated data for benchmarking post-quantum cryptography in TLS 1.3, appropriately adapted to fit our context; this fork constitutes a companion to the work presented in [10], which forms the basis for our work.
2. On liboqs, an open source C library for quantum-resistant cryptographic algorithms from the Open Quantum Safe (OQS) Project [15], which provides an open-source implementation of the post-quantum secure algorithms for the TLS 1.3, either from the PQClean project or directly from their submissions to the NIST. This library is available for research purposes.

More precisely, the aforementioned fork was used for the first two types of experiments, while for the third experiment, we used liboqs [22].

Our experiments included all the post-quantum secure ciphers for key exchange that were analyzed in the third round of the NIST evaluation procedure for all possible security levels; an exemption was the McEliece cipher for the first two experiments due to the large delay that occurred. Indeed, the McEliece cipher, as stated in the NIST Status Report on the Second Round of the Post-Quantum Cryptography Standardization Process [24], has a very large public key and, thus, does not fit well with Internet protocols as they are currently specified (although it is still an appealing choice for standardization, since it achieves the smallest ciphertext among alls KEMs and, thus, is preferable for some applications). We also examined hybrid versions of these ciphers — i.e., being combined with a classic elliptic curve cipher. Such versions are provided by the OQS project, such as, if quantum-safe public-key algorithms are used in conjunction with traditional public key algorithms, the derived implementation is *at least no less secure than existing traditional cryptography* [15]. More information on hybrid implementation for key exchange in TLS 1.3 can be bound in [10].

The ciphers (for the key exchange) examined for the first two experiments, which utilize simulation of TLS connections, are shown in Table 1. Each cipher has several versions depending on its parameters to achieve a specific security level according to the NIST requirements; as it can be seen, a classical elliptic curve (EC) algorithm for key exchange was also considered — namely, the elliptic curve Diffie–Hellman (ECDH) algorithm, with the NIST Curve P-256.

In all cases, the most recent version, TLS 1.3, of the protocol was used, whereas the data exchanged were encrypted by AES-256 GCM (Galois/Counter Mode). The server's authentication was based on the ECDSA certificate, signed with ECDSA P-256 with SHA-384.

We also executed a third experiment focusing explicitly on the post-quantum algorithms without incorporating

**Table 1. The key exchange algorithms that were considered for the first two experiments**

| Algorithm | Security level |
|---|---|
| Kyber | |
| Kyber512 | L1 |
| Kyber512-90s | L1 |
| Kyber768 | L3 |
| Kyber768-90s | L3 |
| Kyber1024 | L5 |
| Kyber1024-90s | L5 |
| p256_kyber512 | Hybrid |
| p256_kyber512-90s | Hybrid |
| p384_kyber768 | Hybrid |
| p384_kyber768-90s | Hybrid |
| p521_kyber1024 | Hybrid |
| p521_kyber1024-90s | Hybrid |
| NTRU | |
| NTRU-HPS-2048-509 | L1 |
| NTRU-HPS-2048-677 | L3 |
| NTRU-HRSS-701 | L3 |
| NTRU-HPS-4096-821 | L5 |
| p256_ntru_hps2048-509 | Hybrid |
| p384_ntru_hps2048-677 | Hybrid |
| p521_ntru_hps4096-821 | Hybrid |
| p384_ntru_hrss701 | Hybrid |
| Saber | |
| LightSaber | L1 |
| Saber | L3 |
| FireSaber | L5 |
| p256_lightsaber | Hybrid |
| p384_saber | Hybrid |
| p521_firesaber | Hybrid |
| ECDH NIST P-256 | |
| prime256v1 | Non post-quantum |

them into a TLS implementation. In this experiment, the McEliece variants were also taken into account.

### 4.1. Motivation for this work and relationships with similar works

This study aimed to exhaustively check all the finalists of the third round of the NIST competition for post-quantum ciphers with respect to their performance in TLS, focusing on key exchange, under varying network parameters and different underlying computing powers. To this end, as stated above, we mainly utilized the benchmark used in [10], which is considered a nice option for our experiments. Our analysis extended the analysis in [10] as follows:

- All the finalists for key exchange, for all possible security levels, were examined in our experiment, while in [10] the analysis focuses on only three instantiates for key exchange (SIKE p434, Kyber512-90s, and FrodoKEM-640-AES, i.e. instantiates of one finalist and two alternates).
- We additionally examined how the processing power affects the performance for fixed (optimal) network parameters. We also checked, as an additional aspect, the raw performance of each algorithm on different computing devices without using the TLS protocol.

## 5. RESULTS

This sections presents the results from our range of experiments that took place.

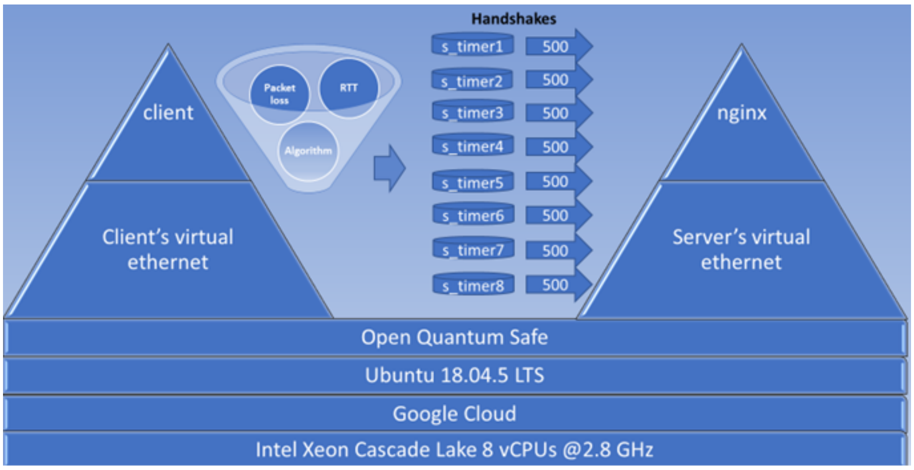


**Figure 1.** The setup of the first experiment.

### 5.1. First experiment: Analysis for several network parameters

The first experiment aimed to study the time needed for a complete TLS handshake for several network parameters. To this end, based on the approach in[10], we created a pair of virtual Ethernets for client–server. In the client's network, a variation of the performance timing program `s_timer` of the OpenSSL was used to measure the performance as follows: (i) a prescribed number of TLS handshakes was executed, where the relevant post-quantum cipher was embedded each time; and (ii) the session was terminated, storing the time duration that was needed. On the server's side, an Nginx server was executed, which utilized the Open Quantum Safe project's OpenSSL.

We subsequently set several RTTs, depending on the distance assumed between the client and server. Our hypotheses on the RTTs were based on those in[10]; as stated therein, four RTTs suffice to illustrate several realistic scenarios, from the optimum one (i.e., the smallest distance) to the worst one (i.e., with the largest distance). These four values of RTTs were 5.368 (best), 30.916 (moderate), 78.448 (bad), and 195.46 ms (worst).

Additionally, we set several values for the packet loss ratio, from 0% to 15%, which seemed to be realistic assumptions according to the information that can be obtained from work in[25]. For each cipher, eight different timers (through the `s_timer` utility) were used, each of them initiating 500 handshakes with the Nginx server — i.e., a total of 4000 connections for each scenario. The device used as a server was the Google cloud. Our experiments were based on the code available in[26], which is also a companion to the work presented in[10]. The whole setup of this experiment is illustrated in Figure 1.

For the cases of ciphers at the highest security level according to the NIST's classification, Figures 2–5 illustrate the diagrams for the time needed to complete the TLS handshakes, for all possible RTTs that were examined (from the best to the worst) and for each possible post-quantum key exchange algorithm. All results from all the experiments, for all security levels, are analytically presented in Figures 13–20 in the Appendix. From these results, we can get the following outcomes:

- The NTRU, Saber, and Kyber variants at the security level L1 behave better than the classical elliptic curve key exchange and their hybrid versions. Even for the few cases that they do not behave better, they are still very close to them, since the worst case that was monitored is a slow down by 2.5%.
- For all security levels, the aforementioned variants seem to behave generally better than their hybrid versions, regardless of the RTT or packet loss ratio.

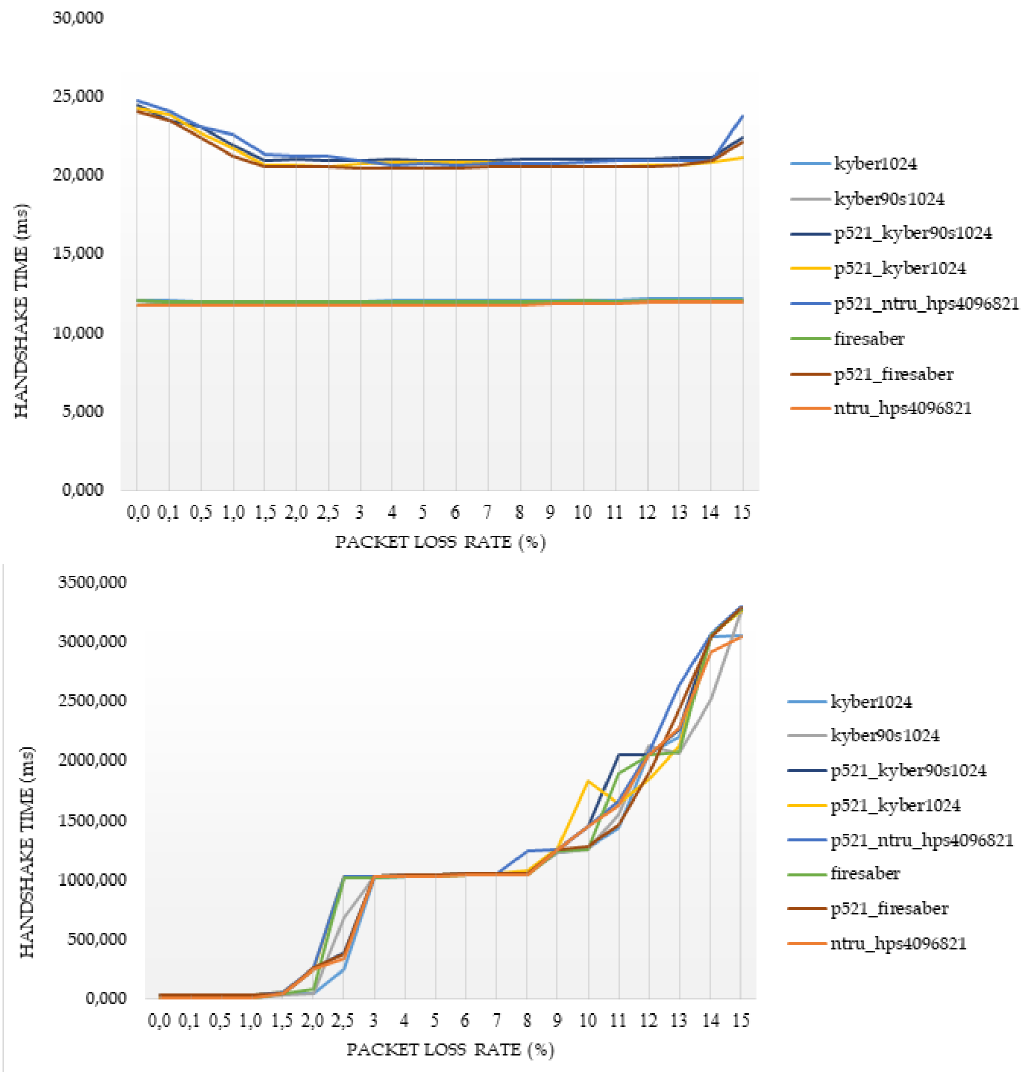


**Figure 2.** Results of the time to complete the TLS handshake, for post-quantum ciphers at the highest security level L5, in conjunction with hybrid implementations as well as with a conventional implementation with elliptic curve Diffie–Hellman key exchange with curve P-256. The first figure indicates the medians and the second the 95th percentile, for the optimal RTT.

.

- A packet loss ratio at 2% or beyond this value highly affects the overall handshake completion time, regardless of the underlying cipher; such a delay is expected, due to packet re-transmissions resulting from packet losses. As becomes clear from the subsequent experiments, the overall time for the handshake completion is much higher than the time of a pure cryptographic execution, and thus, this experiment is more relevant for assessing the effect of the network rather than the effect of the cipher; the latter was studied in the second experiment.
- The increase of packet loss ratio affects the ciphers at higher security levels L3 and L5 more than the ciphers at the L1 security level.
- For large values of RTT, which correspond to large distances between the client and server, we get that this large distance predominates with respect to the overall performance of completion of the handshake.

In principle, lightsaber seems to achieve the best performance for all network settings, but both Kyber and NTRU are also very close. This comparison was further examined by the subsequent experiments, which focused explicitly on the cryptographic procedure without considering network parameters.

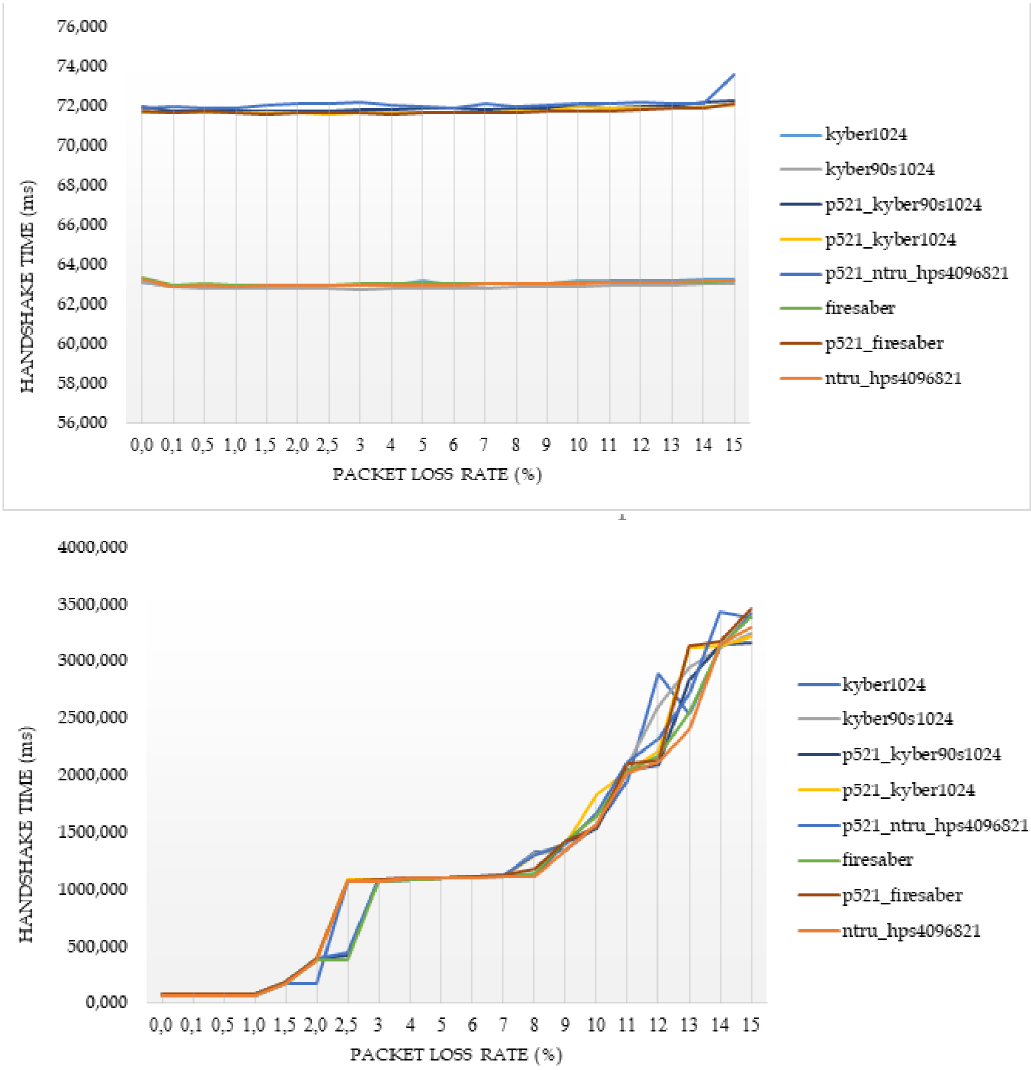


**Figure 3.** Results of the time to complete the TLS handshake, for post-quantum ciphers at the highest security level L5, in conjunction with hybrid implementations as well as with a conventional implementation with elliptic curve Diffie–Hellman key exchange with curve P-256. The first figure indicates the medians and the second the 95th percentile, for the moderate RTT.

### 5.2. Second experiment: Comparative study for two different devices under an optimum network

For our second experiment, we fixed the values of RTT and packet loss ratio to zero — i.e., to assume an ideal case with no network delays at all (an optimal network). Our aim was to evaluate the performance of the post-quantum ciphers for different devices with different computing capabilities — i.e., one *high_core* at 4 GHz (the Google machine) and one *low_core* at 1.6 GHz (the local machine). The same code as in the first experiment was used, but for each TLS implementation with different post-quantum cipher, we set one timer through the `s_timer` utility, which initiates 4000 handshakes with the Nginx server. The two local devices were used for the client execution to perform the comparative study. We also examined conventional elliptic curve algorithms to have a comparative study with such contemporary algorithms.

The setup of this experiment is shown in Figure 6.

The results are presented in a similar manner as in the first experiments — namely, we computed the medians

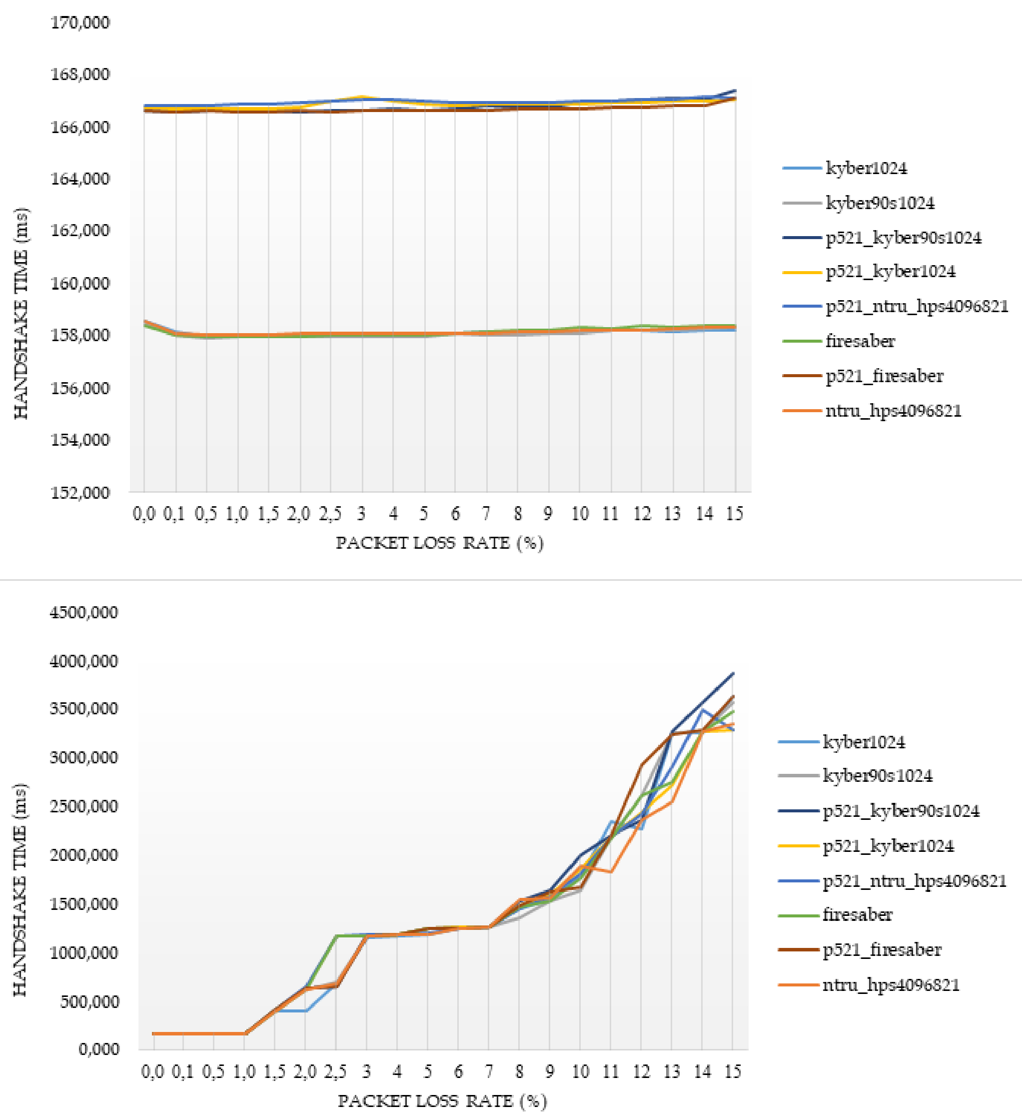


**Figure 4.** Results of the time to complete the TLS handshake, for post-quantum ciphers at the highest security level L5, in conjunction with hybrid implementations as well as with a conventional implementation with elliptic curve Diffie–Hellman key exchange with curve P-256. The first figure indicates the medians and the second the 95th percentile, for the bad RTT.

.

for the handshake completion time as well the 95th percentile. These measurements took place for all key exchange ciphers with security levels L1, L3, or L5. The results are shown in Figures 7 and 8 for L1 ciphers, Figures 9 and 10 for L3 ciphers, and Figures 11 and 12 for L5 ciphers.

Focusing on the L1 ciphers, we get that the lightsaber seems to be the faster cipher for the key exchange, whereas — as was also apparent in the first experiment, when several network parameters were varied — it seems to be faster even from conventional elliptic curve algorithms with no post-quantum resistance. Moreover, kyber90s512 seems also to have a nice performance. On the contrary, NTRU, as well as its hybrid implementation, seems to have the worst performance, being about 5 times slower than lightsaber and 3.5 times slower than Kyber90s512; in general, the differences in performance become greater in the high core machine.

Examining, for each post-quantum cipher, how the underlying computing power affects its performance, we

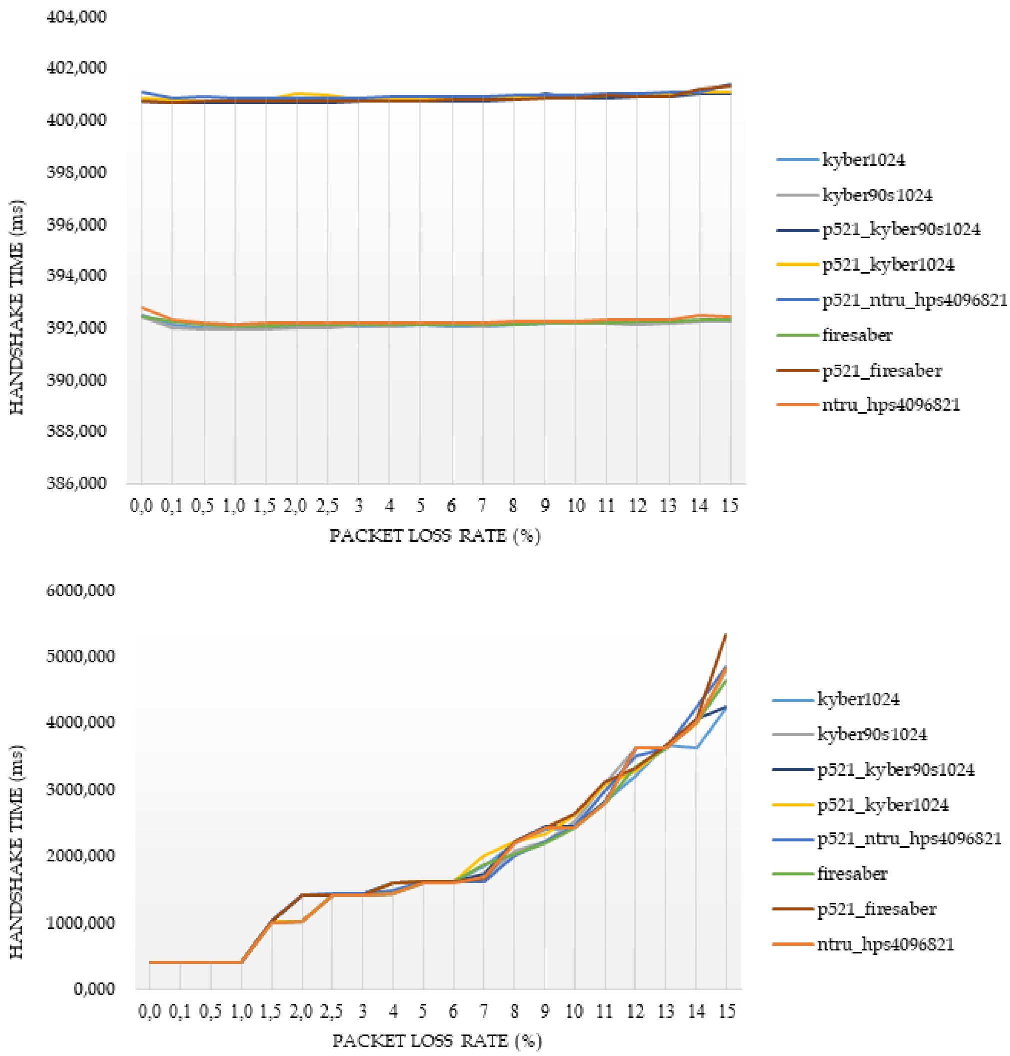


**Figure 5.** Results of the time to complete the TLS handshake, for post-quantum ciphers at the highest security level L5, in conjunction with hybrid implementations as well as with a conventional implementation with elliptic curve Diffie–Hellman key exchange with curve P-256. The first figure indicates the medians and the second the 95th percentile, for the worst RTT.

get that, moving from the high core to the low core machine, NTRU becomes slower by about 25%, Saber becomes slower by about 42%, and Kyber becomes slower by about 62%, while this decrease in performance for the conventional elliptic curve is about 30%.

Similar conclusions also hold for the L3 ciphers; in this case, however, the hybrid versions of lightsaber and kyber90s512 seem to be much more slower than in the case of the L1 ciphers. NTRU is 7.5 times slower than Saber and 6 times slower than Kyber768 (for the high core machine). Moreover, examining how the underlying computing power affects the performance, we get that, moving from the high core to the low core machine, NTRU becomes slower by about 45%, Saber becomes slower by about 33%, and Kyber becomes slower by about 27%, while this decrease in performance for the conventional elliptic curve is about 20%.

The L5 ciphers also have similar behavior and the above conclusions are much more clear; here, Firesaber is about 95% faster than the elliptic curve algorithm cipher with key length 256 bits. Good performance is also achieved by kyber1024 and kyber90s1024, which is also better than the performance of the conventional

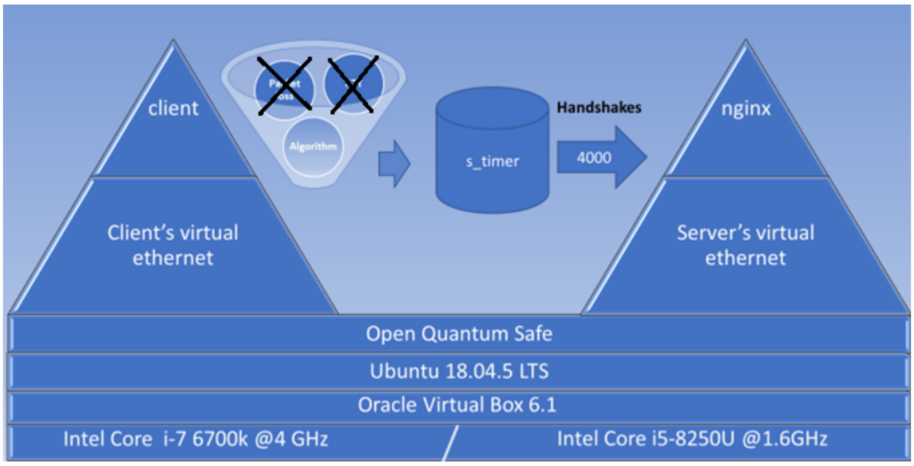


**Figure 6.** The setup of the second experiment.

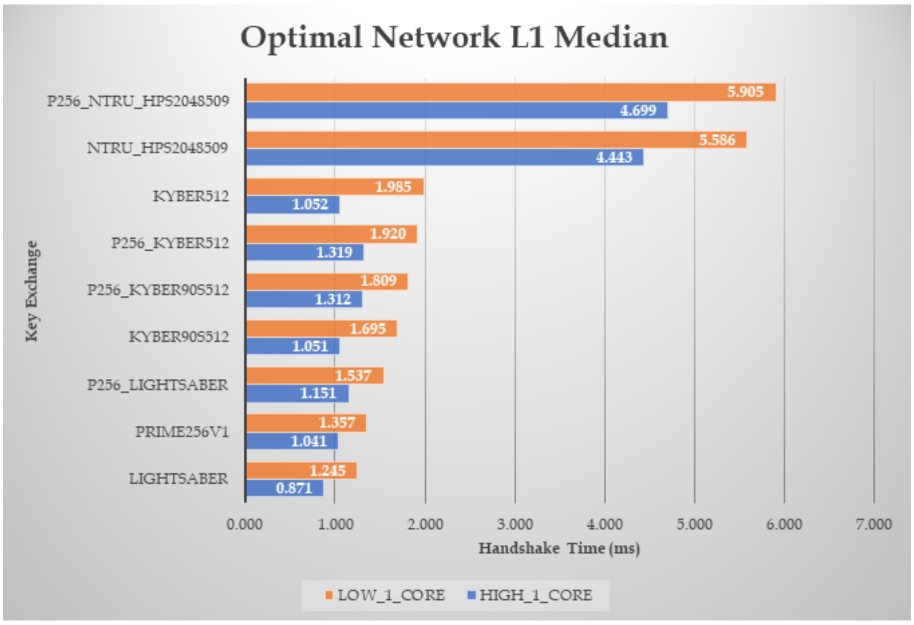


**Figure 7.** Results of the handshake time, with zero RTT and packet loss ratio, for ciphers at L1 security level (the median time in ms).

elliptic curve algorithm as well as their hybrid versions. Checking NTRU with respect to Saber and Kyber, we get that NTRU is about 9.3 times slower than Firesaber and about 7 times slower than Kyber1024 (at the high core machine). Moreover, examining how the underlying computing power affects the performance, we get that, moving from the high core to the low core machine, NTRU becomes slower by about 31%, Saber becomes slower by about 28%, and Kyber becomes slower by about 33%, while this decrease in performance for the conventional elliptic curve is about 24%.

For all security levels, and regardless of the underlying computing power (from those two that were used in our experiments), we get that the post-quantum algorithms are faster than their corresponding hybrid versions.

### 5.3. Third experiment: Raw performance

Our third experiment aimed to check the performance (execution time) of the key encapsulation ciphers based on measurements on the same device. Both local devices were also used to see the effect of the underlying com-

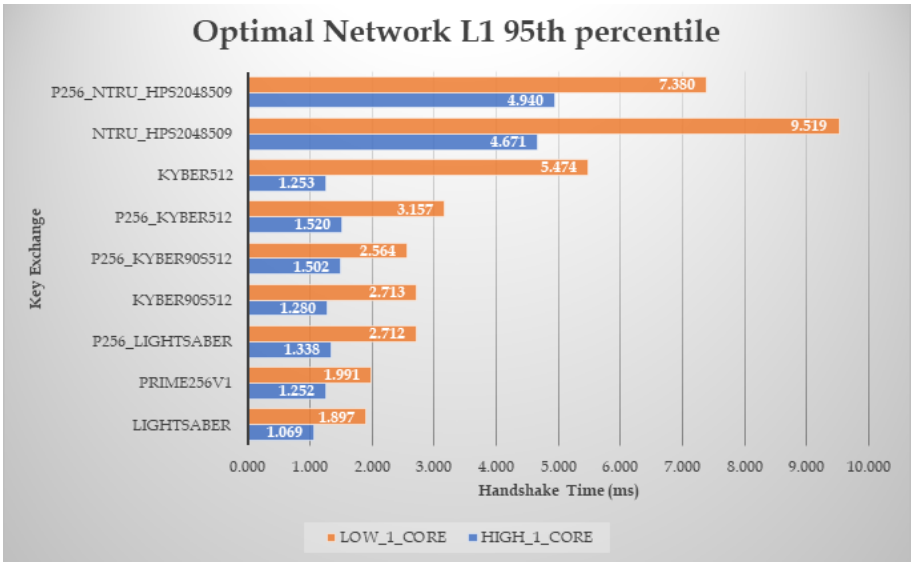


**Figure 8.** Results of the handshake time, with zero RTT and packet loss ratio, for ciphers at L1 security level (the 95th percentile — time in ms).

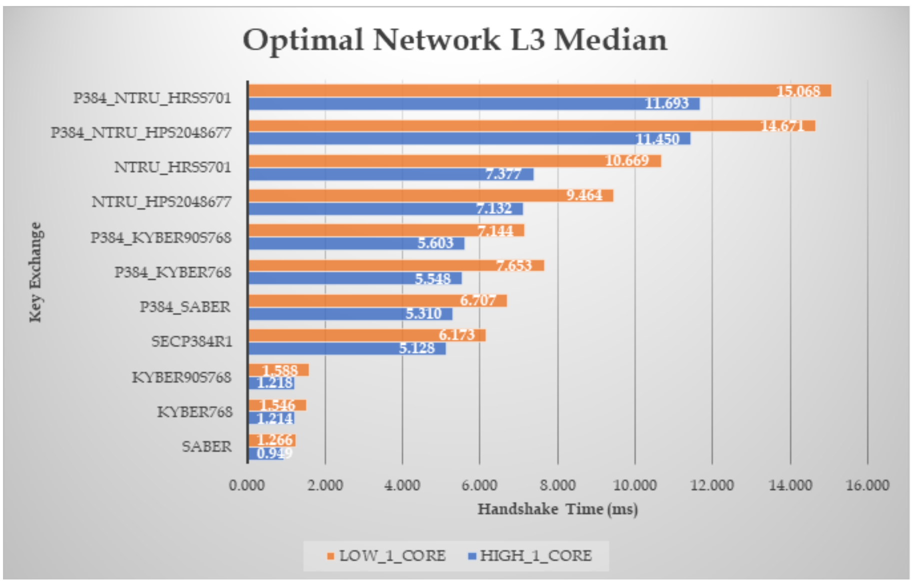


**Figure 9.** Results of the handshake time, with zero RTT and packet loss ratio, for ciphers at L3 security level (the median time in ms).

puting power on the performance of each cipher. For the experiments, we utilized the application speed_kem lying in the repository of liboqs. More precisely, each application was run for 10s, and at the end, we collected the time measurements.

Any such post-quantum cipher actually implements a key encapsulation mechanism (KEM), which consists of three algorithms: the keygen function, which generates a public encapsulation key $p_k$ and a private decapsulation key $s_k$; the encaps function, which has as input an encapsulation key $p_k$ and produces at its output a ciphertext $c$ and a symmetric key $k$; and the decaps function, which has as input a decapsulation key $s_k$ and a ciphertext $c$ and produces a symmetric key $k$ (or a decapsulation failure). The main concept in KEMs is that encapsulating with the public key and decapsulating with the corresponding private key produce the same

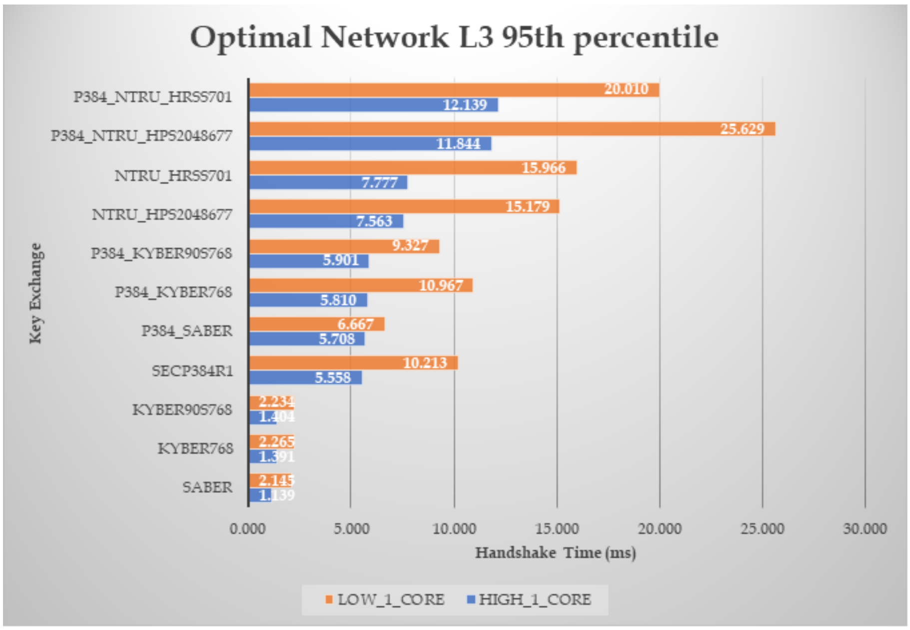


**Figure 10.** Results of the handshake time, with zero RTT and packet loss ratio, for ciphers at L3 security level (the 95th percentile — time in ms).

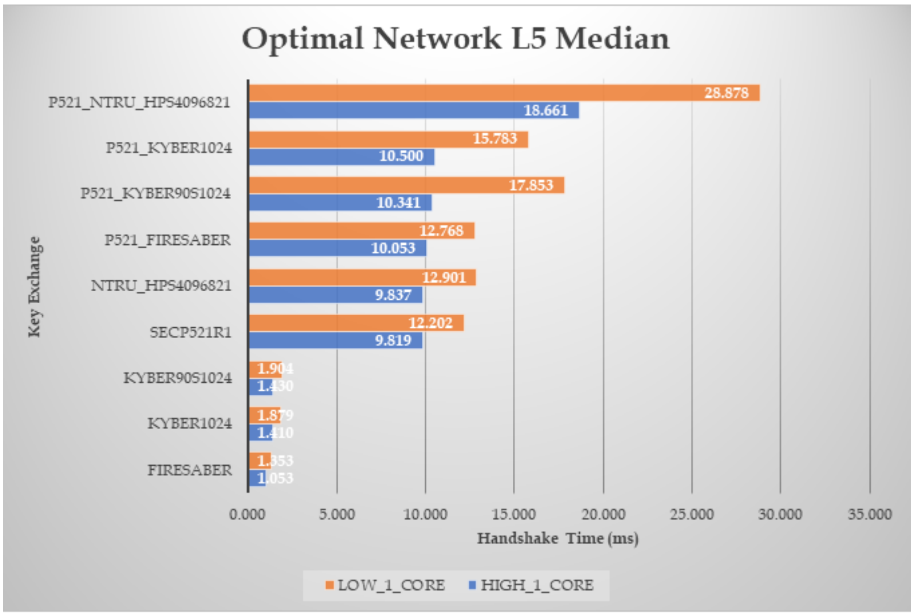


**Figure 11.** Results of the handshake time, with zero RTT and packet loss ratio, for ciphers at L5 security level (the median time in ms).

shared secret key, when the encapsulated ciphertext is given as input to the decapsulate function.

All the results from this experiment are shown in Table 2. All the algorithms for security levels L1, L3, and L5 were tested on both devices, whereas the execution times were computed separately for the keygen function, the encaps function, and the decaps function; the mean values of these times are shown in Table 2 for the McEliece variants, Table 3 for the Kyber variants, Table 4 for the NTRU variants, and Table 5 for the Saber variants. Note that, in this experiment, contrary to the previous two, we also tested all the variants of the

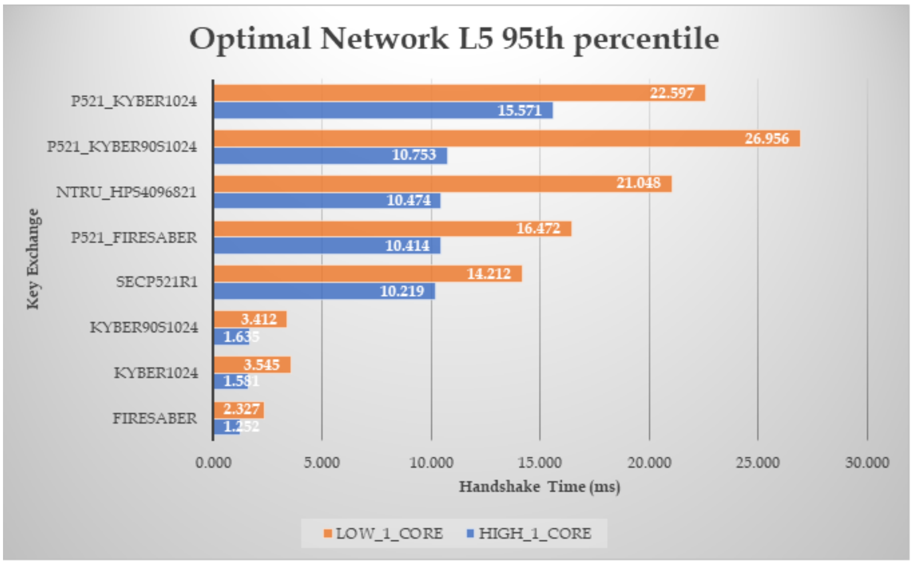


**Figure 12.** Results of the handshake time, with zero RTT and packet loss ratio, for ciphers at L5 security level (the 95th percentile — time in ms).

McEliece cipher, which is one of the finalists in the ongoing NIST standardization process. All parameters for each variant are also shown in the tables, and, for all cases, the size of the shared secret is 32 bytes.

The results in Tables 2–5 illustrate the importance of the underlying computing power, in terms of measuring the performance of a cryptographic algorithm, since gains from about 42% to about 50% are generally observed when we move to a more powerful device. Additionally, this gain in performance becomes more prevalent when the key sizes increase.

Moreover, these measurements confirm the outcomes from the first two experiments, illustrating that Saber and Kyber achieve better performance than the remaining algorithms (with the light version of the Saber, at security level L1, being the fastest), whereas we can also verify that the McEliece variants do not behave well with respect to performance, as was expected.

## 6. DISCUSSION

Combining the above results, it becomes evident that — as expected — the sizes of the key and the ciphertext highly affect the overall performance of a cipher and, thus, a higher security level of the cipher yields degradation in performance. This is particularly obvious for the McEliece cipher, which is an observation that was also pointed out by NIST. More precisely, the McEliece cipher seems to be not an option for classical contemporary systems. Moreover, the NTRU variants seem to also have not as good behavior as Saber and Kyber in terms of performance, even though the relevant key and ciphertext sizes are comparable with those of the other post-quantum secure ciphers.

Moreover, the results also verify that the network parameters also affect the overall performance to a high extent — and, actually, it is a more decisive factor for the overall performance than the underlying cryptographic algorithms that are being used.

In any case, we can conclude that there are several promising solutions for post-quantum key exchange algorithms that can be used in network security protocols such as the TLS, even in conventional contemporary systems. Such ciphers have comparable or, in some cases, even better performance than classical elliptic curve

**Table 2. Time measurements for post-quantum KEM ciphers (the McEliece variants)**

| Algorithm | Mean time (ms) (Intel Core i7- 6700k @4 GHz) | Mean time (ms) (Intel Core i5-82500k @1.6 GHz) | Percentage difference between the two systems |
|---|---|---|---|
| Classic-McEliece-348864 (L1) Sizes (in bytes): Public key: 261120, Secret key: 6452, ciphertext: 128 | | | |
| keygen | 124.698 | 173.083 | 38.80% |
| encaps | 0.311 | 0.432 | 38.90% |
| decaps | 0.190 | 0.269 | 41.80% |
| Classic-McEliece-348864f (L1) Sizes (in bytes): Public key: 261120, Secret key: 6452, ciphertext: 128 | | | |
| keygen | 99.878 | 146.610 | 46.79% |
| encaps | 0.308 | 0.446 | 44.81% |
| decaps | 0.192 | 0.276 | 43.68% |
| Classic-McEliece-460896 (L3) Sizes (in bytes): Public key: 524160, Secret key: 13568, ciphertext: 188 | | | |
| keygen | 370.397 | 607.631 | 64.05% |
| encaps | 0.633 | 0.901 | 42.39% |
| decaps | 0.431 | 0.618 | 43.49% |
| Classic-McEliece-460896f (L3) Sizes (in bytes): Public key: 524160, Secret key: 13568, ciphertext: 188 | | | |
| keygen | 298.691 | 441.286 | 47.74% |
| encaps | 0.613 | 0.881 | 43.69% |
| decaps | 0.431 | 0.649 | 50.48% |
| Classic-McEliece-6688128 (L5) Sizes (in bytes): Public key: 1044992, Secret key: 13892, ciphertext: 240 | | | |
| keygen | 547.710 | 974.409 | 77.91% |
| encaps | 1.203 | 1.763 | 46.52% |
| decaps | 0.484 | 0.706 | 45.96% |
| Classic-McEliece-6688128f (L5) Sizes (in bytes): Public key: 1044992, Secret key: 13892, ciphertext: 240 | | | |
| keygen | 401.450 | 616.208 | 53.50% |
| encaps | 1.208 | 1.787 | 47.95% |
| decaps | 0.485 | 0.708 | 45.93% |
| Classic-McEliece-6960119 (L5) Sizes (in bytes): Public key: 1047319, Secret key: 13908, ciphertext: 226 | | | |
| keygen | 542.884 | 906.688 | 67.01% |
| encaps | 1.225 | 1.767 | 44.26% |
| decaps | 0.464 | 0.683 | 47.20% |
| Classic-McEliece-6960119f (L5) Sizes (in bytes): Public key: 1047319, Secret key: 13908, ciphertext: 226 | | | |
| keygen | 383.001 | 586.975 | 53.26% |
| encaps | 1.247 | 1.813 | 45.39% |
| decaps | 0.463 | 0.687 | 48.29% |
| Classic-McEliece-8192128 (L5) Sizes (in bytes): Public key: 1357824, Secret key: 14080, ciphertext: 240 | | | |
| keygen | 545.983 | 843.698 | 54.53% |
| encaps | 1.643 | 2.368 | 44.13% |
| decaps | 0.481 | 0.705 | 46.61% |
| Classic-McEliece-8192128f (L5) Sizes (in bytes): Public key: 1357824, Secret key: 14080, ciphertext: 240 | | | |
| keygen | 418.616 | 645.955 | 54.31% |
| encaps | 1.620 | 2.344 | 44.71% |
| decaps | 0.483 | 0.700 | 45.00% |

public key algorithms; interestingly, it seems that adopting a hybrid solution does not provide much gain in terms of performance compared to a fully post-quantum secure solution.

**Table 3. Time measurements for post-quantum KEM ciphers (the Kyber variants)**

| Algorithm | Mean time (ms) (Intel Core i7- 6700k @4 GHz) | Mean time (ms) (Intel Core i5-82500k @1.6 GHz) | Percentage difference between the two systems |
|---|---|---|---|
| Kyber512 (L1)<br>Sizes (in bytes): Public key: 800, Secret key: 1632, ciphertext: 736 | | | |
| keygen | 0.065 | 0.094 | 43.86% |
| encaps | 0.088 | 0.128 | 45.02% |
| decaps | 0.112 | 0.159 | 42.38% |
| Kyber512-90s (L1)<br>Sizes (in bytes): Public key: 800, Secret key: 1632, ciphertext: 736 | | | |
| keygen | 0.068 | 0.101 | 48.50% |
| encaps | 0.090 | 0.129 | 43.27% |
| decaps | 0.115 | 0.168 | 45.77% |
| Kyber768 (L3)<br>Sizes (in bytes): Public key: 1184, Secret key: 2400, ciphertext: 1088 | | | |
| keygen | 0.112 | 0.161 | 43.64% |
| encaps | 0.140 | 0.201 | 43.52% |
| decaps | 0.172 | 0.248 | 43.98% |
| Kyber768-90s (L3)<br>Sizes (in bytes): Public key: 1184, Secret key: 2400, ciphertext: 1088 | | | |
| keygen | 0.120 | 0.172 | 43.23% |
| encaps | 0.145 | 0.211 | 45.80% |
| decaps | 0.178 | 0.256 | 43.98% |
| Kyber1024 (L5)<br>Sizes (in bytes): Public key: 1568, Secret key: 3168, ciphertext: 1568 | | | |
| keygen | 0.171 | 0.245 | 43.07% |
| encaps | 0.202 | 0.293 | 44.81% |
| decaps | 0.242 | 0.347 43.39% | |
| Kyber1024-90s (L5)<br>Sizes (in bytes): Public key: 1568, Secret key: 3168, ciphertext: 1568 | | | |
| keygen | 0.181 | 0.259 | 43.00% |
| encaps | 0.213 | 0.303 | 42.16% |
| decaps | 0.251 | 0.361 | 43.84% |

As a general conclusion, we can state that all the Saber variants — namely lightsaber, saber, and firesaber — as well as some variants of the Kyber — namely, kyber768, kyber90s768, kyber1024, and kyber90s1024 — could possibly be considered in terms of performance for adoption even for today's computing systems, since they exhibited nice performance properties for all sets of experiments that were carried out. It seems that there is also no need, from the performance point of view, to focus on hybrid implementations, since pure post-quantum secure ciphers seem to have better behavior. This general conclusion seems to remain valid regardless of the underlying computing power.

During the review phase of this paper, NIST completed its third round, as stated above. According to the relative status report that NIST issued[27], *both KYBER and Saber are suitable for use on constrained devices, as each of these can be implemented (at least without protections against side-channel attacks) using less than* 4 *kB of RAM with less than 20 kB of storage for the code*, while the overall performance of NTRU, Saber, and CRYSTALS-Kyber as KEMs would be acceptable for general-use applications, although *NTRU is not quite as good as KYBER or Saber as a result of its slower key generation and somewhat larger public keys and ciphertexts*. In the same report, NIST points out that *while Saber has the lowest total cost due to its smaller public keys and ciphertexts, the cost difference between KYBER and Saber was not large enough to be considered significant*. The algorithm that has been chosen by NIST, as described above, is the CRYSTALS-Kyber. As stated in[27], deciding between KYBER, NTRU, and Saber was a difficult choice, since *most applications would be able to use any of them without significant performance penalties*. Since NIST intended to standardize only one of these finalists, as all three were based on lattices, the final choice was CRYSTALS-Kyber, since NIST found that the

**Table 4. Time measurements for post-quantum KEM ciphers (the NTRU variants).**

| Algorithm | Mean time (ms) (Intel Core i7- 6700k @4 GHz) | Mean time (ms) (Intel Core i5-82500k @1.6 GHz) | Percentage difference between the two systems |
|---|---|---|---|
| NTRU-HPS-2048-509 (L1) Sizes (in bytes): Public key: 699, Secret key: 935, ciphertext: 699 | | | |
| keygen | 2.965 | 4.287 | 44.60% |
| encaps | 0.181 | 0.264 | 46.07% |
| decaps | 0.469 | 0.691 | 47.27% |
| NTRU-HPS-2048-677 (L3) Sizes (in bytes): Public key: 930, Secret key: 1234, ciphertext: 930 | | | |
| keygen | 5.168 | 7.490 | 44.94% |
| encaps | 0.305 | 0.449 | 47.28% |
| decaps | 0.814 | 1.201 | 47.57% |
| NTRU-HRSS-701 (L3) Sizes (in bytes): Public key: 1138, Secret key: 1450, ciphertext: 1138 | | | |
| keygen | 5.526 | 8.043 | 45.55% |
| encaps | 0.304 | 0.447 | 46.95% |
| decaps | 0.883 | 1.289 | 45.97% |
| NTRU-HPS-4096-821 (L5) Sizes (in bytes): Public key: 1230, Secret key: 1590, ciphertext: 1230 | | | |
| keygen | 7.596 | 11.363 | 49.60% |
| encaps | 0.438 | 0.649 | 48.12% |
| decaps | 1.196 | 1.768 | 47.83% |

**Table 5. Time measurements for post-quantum KEM ciphers (the Saber variants)**

| Algorithm | Mean time (ms) (Intel Core i7- 6700k @4 GHz) | Mean time (ms) (Intel Core i5-82500k @1.6 GHz) | Percentage difference between the two systems |
|---|---|---|---|
| LightSaber-KEM (L1) Sizes (in bytes): Public key: 672, Secret key: 1568, ciphertext: 736 | | | |
| keygen | 0.028 | 0.042 | 48.91% |
| encaps | 0.033 | 0.049 | 48.44% |
| decaps | 0.035 | 0.052 | 49.74% |
| Saber-KEM (L3) Sizes (in bytes): Public key: 992, Secret key: 2304, ciphertext: 1088 | | | |
| keygen | 0.049 | 0.074 | 51.88% |
| encaps | 0.058 | 0.083 | 43.68% |
| decaps | 0.061 | 0.101 | 65.79% |
| FireSaber-KEM (L5) Sizes (in bytes): Public key: 1312, Secret key: 3040, ciphertext: 1472 | | | |
| keygen | 0.075 | 0.118 | 56.96% |
| encaps | 0.087 | 0.137 | 57.98% |
| decaps | 0.095 | 0.143 | 50.35% |

security assumption upon which CRYSTALS-Kyber is based is marginally more convincing than the security assumptions of NTRU and Saber, whereas *with regard to performance, KYBER was near the top (if not the top) in most benchmarks*.

The conclusions derived from the present research are fully in line with the final output of the third round of the NIST competition, since indeed the CRYSTALS-Kyber algorithm chosen by NIST illustrated in our work very good performance (either the best or almost the best) for key exchange in the TLS protocol, whereas the performance benefits of Saber — as pointed out by NIST — are also clear. Moreover, the performance achieved by the CRYSTALS-Kyber is comparable with the classical contemporary public key implementations for the TLS protocol, and this comparison is not actually affected by network parameters.

## 7. CONCLUSIONS AND FUTURE RESEARCH

This study focused on analyzing the performance of public-key post-quantum algorithms in light of their possible use for key exchange in the prominent TLS protocol. Based on known results and existing software that has already been developed for research purposes, we carry out a more extended set of experiments, taking into account the list of third round finalists of the NIST's standardization process. The main outcome is that there exist differences among the various finalists with respect to their performance, and the main conclusion with regard to the fastest algorithms are in line with the final choice of NIST at the end of this round — namely the choice of CRYSTALS-Kyber as a standard. Moreover, starting from now, employing post-quantum secure solutions into contemporary applications and network security protocols seems to be a viable option. However, even for those algorithms that have not been standardized—i.e. they are not being evaluated anymore in the current fourth round of the NIST evaluation — the results are of importance, taking into account that it cannot be excluded that some of these schemes might be standardized outside the NIST, especially those for which NIST pointed out that they have low "cost" and do not raise (to our current knowledge) security issues. In this regard, it is interesting to recall that Chacha20, which is a secure symmetric cipher supported by TLS 1.3 for encrypting communication data, is not officially standardized by NIST.

This is a highly evolving research field; one should carefully monitor the progress in the NIST evaluation procedure and the related research. Indeed, at the beginning of August 2022, it was announced in a research paper (a pre-print version is currently public[28]) that SIKE, which is one of the four algorithms that are currently evaluated by NIST in the fourth round of evaluation (being one of the alternated algorithms in the third round), was cracked by using a computer running Intel Xeon CPU in 1 h.

It should be pointed out that our work focuses only on performance in the handshake phase of the TLS, having post-quantum secure algorithms for key exchange. Although known values of the sizes of the produced ciphertexts and keys are also being presented to allow a comparative study of these factors, we do not explicitly study relevant important parameters such as the bandwidth consumed by communication or the memory required. This could also be considered in future work, taking into account the relevant results announced by NIST. Moreover, the post-quantum digital signature algorithms should also be considered in the same context ]such studies have already been performed, for some such algorithms, in several works (e.g., [10]), as described in Section 3].

Another important aspect that needs to be considered in future research is to determine the behavior of post-quantum secure TLS implementations in restricted environments in terms of computing power and memory; to this end, it is important to focus on cases of IoT applications (e.g., on mobile devices, a Raspberry Pi, etc.) The current research illustrated that the differences in performance gains — among several post-quantum ciphers — seem to increase with the computing power, but such restricted environments have not been examined. Such research efforts have recently been started (see, e.g., [11]).

When dealing with an evaluation of ciphers' performance, it is also of importance to identify which underlying processes/computations are more "heavy", so as to focus appropriately on them in future research for algorithms optimization. This aspect was not studied here, and it constitutes an open research field.

Additionally, focusing on embedding post-quantum secure algorithms in other security protocols residing in lower network architecture levels, such as the IPsec, is also an interesting research area (see, e.g., [29]). More generally, focusing on post-quantum solutions in several existing protocols and infrastructures, such as the blockchain ecosystem[30], becomes an essential issue in ensuring the appropriate safeguards for long-term data protection.

## ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers for their very useful comments and suggestions, as well as for drawing our attention to some very recent research papers in the field, that helped to significantly improve the paper.

## DECLARATIONS

### Authors' contributions

Made substantial contributions to conception and design of the study: Tzinos I, Limniotis K, Kolokotronis N
Set up simulation environments, performed simulations and provided figures and tables with results: Tzinos I
Data analysis and interpretation: Tzinos I, Limniotis K, Kolokotronis N
Writing the paper: Tzinos I, Limniotis K, Kolokotronis N

### Availability of data and materials

Not applicable.

### Financial support and sponsorship

None.

### Conflicts of interest

All authors declared that there are no conflicts of interest.

### Ethical approval and consent to participate

Not applicable.

### Consent for publication

Not applicable.



## REFERENCES

1. Limniotis K. Cryptography as the Means to Protect Fundamental Human Rights. *Cryptogr* 2021;5:34. DOI
2. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3.; 2018. Available from: https://datatracker.ietf.org/doc/html/rfc8446.
3. Felt AP, Barnes R, King A, et al. Measuring HTTPS adoption on the web. In: Kirda E, Ristenpart T, editors. 26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16-18, 2017. USENIX Association; 2017. pp. 1323–38. Available from: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/felt.
4. Limniotis K, Kolokotronis N. Cryptography threats. In: Kolokotronis N, Shiaeles S, editors. Cyber-Secur. Threat. Actors, Dyn. Mitigation. Boca Raton, FL, USA: CRC Press; 2021. pp. 123–59. DOI
5. Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: 35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994. IEEE Computer Society; 1994. pp. 124–34. DOI
6. Grover LK. A Fast Quantum Mechanical Algorithm for Database Search. In: Miller GL, editor. Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996. ACM; 1996. pp. 212–19. DOI
7. NIST. Post-Quantum Cryptography. Available from: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
8. Mosca M. Cybersecurity in an era with quantum computers: will we be ready?; 2015. https://ia.cr/2015/1075. Cryptology ePrint Archive, Report 2015/1075.
9. Bos JW, Costello C, Naehrig M, Stebila D. Post-quantum key exchange for the tls protocol from the ring learning with errors problem. In: 2015 IEEE Symposium on Security and Privacy; 2015. pp. 553–70. DOI
10. Paquin C, Stebila D, Tamvada G. Benchmarking Post-Quantum Cryptography in TLS; 2019. https://ia.cr/2019/1447. Cryptology ePrint Archive, Report 2019/1447.
11. Bürstinghaus-Steinbach K, Krauß C, Niederhagen R, Schneider M. Post-quantum TLS on embedded systems: integrating and evaluating

kyber and SPHINCS+ with mbed TLS. In: Sun H, Shieh S, Gu G, Ateniese G, editors. ASIA CCS '20: The 15th ACM Asia Conference on Computer and Communications Security, Taipei, Taiwan, October 5-9, 2020. ACM; 2020. pp. 841–52. DOI

12. Sikeridis D, Kampanakis P, Devetsikiotis M. Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH. In: Han D, Feldmann A, editors. CoNEXT '20: The 16th International Conference on emerging Networking EXperiments and Technologies, Barcelona, Spain, December, 2020. ACM; 2020. pp. 149–56. DOI
13. Sikeridis D, Kampanakis P, Devetsikiotis M. Post-quantum authentication in TLS 1.3: A performance study. In: 27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23-26, 2020. The Internet Society; 2020. Available from: https://www.ndss-symposium.org/ndss-paper/post-quantum-authentication-in-tls-1-3-a-performance-study/.
14. Bernstein DJ, Brumley BB, Chen MS, Tuveri N. OpenSSLNTRU: Faster post-quantum TLS key exchange; 2021. https://ia.cr/2021/826. Cryptology ePrint Archive, Report 2021/826.
15. Stebila D, Mosca M. Avanzi R, Heys HM, editors. Post-quantum key exchange for the Internet and the Open Quantum Safe project. Springer; 2016. Available from: https://openquantumsafe.org.
16. Regev O. On lattices, learning with errors, random linear codes, and cryptography. In: Gabow HN, Fagin R, editors. Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005. ACM; 2005. pp. 84–93. DOI
17. Ding J, Yang BY. Multivariate public key cryptography. In: Bernstein DJ, Buchmann J, Dahmen E, editors. Post-Quantum Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg; 2009. pp. 193–241. DOI
18. Rostovtsev A, Stolbunov A. Public-key cryptosystem based on isogenies; 2006. https://ia.cr/2006/145. Cryptology ePrint Archive, Report 2006/145.
19. Childs AM, Jao D, Soukharev V. Constructing elliptic curve isogenies in quantum subexponential time. *J Math Cryptol* 2014;8:1–29. DOI
20. Raavi M, Wuthier S, Chandramouli P, et al. Security comparisons and performance analyses of post-quantum signature algorithms. In: Sako K, Tippenhauer NO, editors. Applied Cryptography and Network Security - 19th International Conference, ACNS 2021, Kamakura, Japan, June 21-24, 2021, Proceedings, Part II. vol. 12727 of Lecture Notes in Computer Science. Springer; 2021. pp. 424–47. DOI
21. Döring R, Geitz M. Post-quantum cryptography in use: empirical analysis of the TLS handshake performance. In: 2022 IEEE/IFIP Network Operations and Management Symposium, NOMS 2022, Budapest, Hungary, April 25-29, 2022. IEEE; 2022. pp. 1–5.
22. Github. liboqs; 2019. Available from: https://github.com/open-quantum-safe/liboqs.
23. Github. pq-tls-benchmark; 2019. Available from: https://github.com/xvzcf/pq-tls-benchmark.
24. NIST. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process; 202O. NISTIR 8309. Available from: https://csrc.nist.gov/publications/detail/nistir/8309/final.
25. Mozilla. The telemetry portal; 2022. Available from: https://telemetry.mozilla.org/.
26. Github. pq-tls-benchmark; 2020. Available from: https://github.com/kalhas/pq-tls-benchmark.
27. NIST. Status report on the third round of the nist post-quantum cryptography standardization proces; 2022. NISTIR 8413. Available from: https://csrc.nist.gov/publications/detail/nistir/8413/final.
28. Castryck W, Decru T. An efficient key recovery attack on SIDH (preliminary version); 2022. https://eprint.iacr.org/2022/975. Cryptology ePrint Archive, Paper 2022/975. Available from: https://eprint.iacr.org/2022/975.
29. Gazdag S, Grundner-Culemann S, Guggemos T, Heider T, Loebenberger D. A formal analysis of IKEv2's post-quantum extension. In: ACSAC '21: Annual Computer Security Applications Conference, Virtual Event, USA, December 6 - 10, 2021. ACM; 2021. pp. 91–105. DOI
30. Brotsis S, Kolokotronis N, Limniotis K. Towards post-quantum blockchain platforms. In: Sargsyan G, Kavallieros D, Kolokotronis N, editors. Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation. Netherlands: Now Publishers; 2022. pp. 106–30. DOI

## APPENDIX

All the results obtained from the first experiment are given in Figures 13–20.

| | 0.0% | 0.1% | 0.5% | 1% | 1.5% | 2% | 2.5% | 3% | 4% | 5% | 6% | 7% | 8% | 9% | 10% | 11% | 12% | 13% | 14% | 15% |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ntru_hps2048509 | 11.62 | 11.59 | 11.59 | 11.63 | 11.59 | 11.59 | 11.58 | 11.58 | 11.60 | 11.62 | 11.62 | 11.62 | 11.66 | 11.66 | 11.69 | 11.72 | 11.73 | 11.78 | 11.77 | 11.82 |
| lightsaber | 11.63 | 11.53 | 11.52 | 11.54 | 11.52 | 11.53 | 11.53 | 11.54 | 11.57 | 11.58 | 11.60 | 11.61 | 11.63 | 11.66 | 11.68 | 11.70 | 11.71 | 11.73 | 11.75 | 11.81 |
| saber | 11.69 | 11.62 | 11.62 | 11.62 | 11.62 | 11.62 | 11.64 | 11.63 | 11.66 | 11.67 | 11.69 | 11.70 | 11.75 | 11.76 | 11.78 | 11.81 | 11.82 | 11.84 | 11.99 | 11.98 |
| ntru_hps2048677 | 11.71 | 11.69 | 11.66 | 11.64 | 11.66 | 11.65 | 11.67 | 11.70 | 11.68 | 11.69 | 11.70 | 11.71 | 11.73 | 11.75 | 11.76 | 11.79 | 11.81 | 11.88 | 12.09 | 11.95 |
| prime256v1 | 11.74 | 11.66 | 11.64 | 11.65 | 11.73 | 11.70 | 11.69 | 11.74 | 11.77 | 11.79 | 11.78 | 11.79 | 11.81 | 11.82 | 11.84 | 11.85 | 11.87 | 11.88 | 11.91 | 12.00 |
| ntru_hrss701 | 11.74 | 11.75 | 11.70 | 11.68 | 11.69 | 11.70 | 11.70 | 11.71 | 11.70 | 11.82 | 11.77 | 11.76 | 11.77 | 11.79 | 11.77 | 11.83 | 11.85 | 11.86 | 11.91 | 11.98 |
| ntru_hps4096821 | 11.77 | 11.77 | 11.71 | 11.70 | 11.71 | 11.72 | 11.71 | 11.72 | 11.72 | 11.73 | 11.75 | 11.75 | 11.78 | 11.81 | 11.83 | 11.85 | 11.90 | 11.93 | 11.97 | 11.98 |
| kyber90s512 | 11.84 | 11.80 | 11.78 | 11.79 | 11.84 | 11.88 | 11.84 | 11.87 | 11.86 | 11.89 | 11.90 | 11.93 | 11.91 | 11.94 | 11.95 | 11.94 | 11.97 | 11.98 | 12.00 | 12.02 |
| kyber1024 | 12.03 | 11.99 | 11.93 | 11.94 | 11.94 | 11.94 | 11.98 | 11.96 | 12.00 | 12.04 | 12.02 | 12.00 | 12.02 | 12.05 | 12.06 | 12.07 | 12.10 | 12.11 | 12.14 | 12.16 |
| kyber512 | 12.05 | 11.85 | 11.92 | 11.87 | 11.85 | 11.87 | 11.88 | 11.89 | 11.88 | 11.93 | 11.96 | 11.98 | 11.98 | 11.99 | 11.99 | 12.01 | 12.02 | 12.03 | 12.08 | 12.08 |
| firesaber | 12.05 | 11.89 | 11.89 | 11.90 | 11.89 | 11.89 | 11.90 | 11.92 | 11.93 | 11.92 | 11.92 | 11.94 | 11.93 | 11.97 | 11.99 | 11.98 | 12.00 | 12.01 | 12.03 | 12.04 |
| kyber90s768 | 12.05 | 11.87 | 11.81 | 11.91 | 11.85 | 11.88 | 11.90 | 11.87 | 11.87 | 11.92 | 11.92 | 11.92 | 11.93 | 11.94 | 11.94 | 11.95 | 11.97 | 12.01 | 12.05 | 12.06 |
| kyber90s1024 | 12.08 | 11.87 | 11.81 | 11.84 | 11.80 | 11.85 | 11.83 | 11.84 | 11.85 | 11.88 | 11.91 | 11.91 | 11.93 | 11.93 | 11.94 | 11.97 | 11.97 | 11.97 | 11.98 | 12.01 |
| kyber768 | 12.16 | 11.90 | 11.88 | 11.89 | 11.85 | 11.89 | 11.91 | 11.94 | 11.90 | 11.96 | 11.97 | 12.00 | 11.98 | 11.99 | 12.01 | 12.04 | 12.06 | 12.08 | 12.07 | 12.13 |
| p256_kyber90s512 | 12.17 | 12.08 | 12.08 | 12.10 | 12.11 | 12.12 | 12.14 | 12.14 | 12.18 | 12.16 | 12.17 | 12.21 | 12.19 | 12.23 | 12.24 | 12.24 | 12.24 | 12.26 | 12.27 | 12.31 |
| p256_lightsaber | 12.18 | 11.99 | 11.96 | 12.04 | 12.02 | 12.04 | 12.07 | 12.12 | 12.11 | 12.14 | 12.13 | 12.17 | 12.16 | 12.19 | 12.17 | 12.18 | 12.24 | 12.24 | 12.26 | 12.30 |
| p256_kyber512 | 12.21 | 12.08 | 12.06 | 12.07 | 12.08 | 12.06 | 12.11 | 12.13 | 12.14 | 12.15 | 12.15 | 12.16 | 12.18 | 12.17 | 12.22 | 12.22 | 12.22 | 12.24 | 12.25 | 12.32 |
| p256_ntru_hps2048509 | 12.52 | 12.28 | 12.30 | 12.26 | 12.31 | 12.27 | 12.32 | 12.29 | 12.32 | 12.32 | 12.34 | 12.37 | 12.38 | 12.37 | 12.37 | 12.40 | 12.41 | 12.40 | 12.34 | 12.45 |
| p384_saber | 16.50 | 16.26 | 15.65 | 15.60 | 15.56 | 15.57 | 15.57 | 15.55 | 15.58 | 15.58 | 15.57 | 15.57 | 15.60 | 15.60 | 15.62 | 15.61 | 15.56 | 15.65 | 15.61 | 15.73 |
| p384_ntru_hrss701 | 16.77 | 16.51 | 15.93 | 15.71 | 15.77 | 15.74 | 15.70 | 15.67 | 15.65 | 15.70 | 15.68 | 15.71 | 15.70 | 15.75 | 15.77 | 15.77 | 15.80 | 15.83 | 15.87 | 15.92 |
| p384_kyber768 | 16.81 | 16.61 | 16.10 | 15.92 | 15.92 | 15.93 | 15.93 | 15.94 | 15.93 | 15.92 | 15.97 | 15.92 | 15.95 | 15.95 | 15.96 | 16.01 | 15.99 | 16.03 | 16.07 | 16.12 |
| p384_kyber90s768 | 16.87 | 16.50 | 16.06 | 15.88 | 15.91 | 15.96 | 15.91 | 15.94 | 15.88 | 15.91 | 15.88 | 15.92 | 15.92 | 15.93 | 15.94 | 15.96 | 15.98 | 15.95 | 16.04 | 16.03 |
| p384_ntru_hps2048677 | 16.94 | 16.80 | 16.07 | 16.05 | 15.95 | 15.94 | 15.99 | 15.98 | 15.98 | 16.00 | 16.02 | 16.05 | 16.09 | 16.03 | 16.09 | 16.07 | 16.06 | 16.11 | 16.14 | 16.72 |
| p521_firesaber | 24.03 | 23.47 | 22.36 | 21.20 | 20.55 | 20.51 | 20.48 | 20.44 | 20.45 | 20.45 | 20.46 | 20.48 | 20.48 | 20.52 | 20.53 | 20.54 | 20.56 | 20.62 | 20.92 | 22.13 |
| p521_kyber1024 | 24.19 | 23.83 | 22.64 | 21.66 | 20.60 | 20.62 | 20.53 | 20.70 | 20.86 | 20.86 | 20.84 | 20.80 | 20.62 | 20.57 | 20.56 | 20.57 | 20.61 | 20.66 | 20.84 | 21.12 |
| p521_kyber90s1024 | 24.45 | 23.42 | 23.02 | 21.91 | 20.95 | 20.98 | 20.93 | 20.95 | 20.97 | 20.95 | 20.95 | 20.95 | 20.98 | 20.98 | 20.99 | 20.98 | 21.01 | 21.08 | 21.07 | 22.37 |
| p521_ntru_hps4096821 | 24.73 | 24.08 | 23.06 | 22.59 | 21.26 | 21.16 | 21.16 | 20.95 | 20.63 | 20.67 | 20.67 | 20.73 | 20.70 | 20.75 | 20.86 | 20.87 | 20.87 | 20.95 | 20.94 | 23.77 |

**Figure 13.** Results of the handshake time for the best RTT scenario (the median time in ms).

| | 0.0% | 0.1% | 0.5% | 1% | 1.5% | 2% | 2.5% | 3% | 4% | 5% | 6% | 7% | 8% | 9% | 10% | 11% | 12% | 13% | 14% | 15% |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| kyber512 | 12.3 | 12.2 | 12.3 | 12.2 | 218.2 | 224.6 | 1012.3 | 1018 | 1022 | 1030 | 1034 | 1036 | 1038 | 1044 | 1236 | 1246 | 2035 | 2048 | 2253 | 3037 |
| kyber768 | 12.4 | 12.2 | 12.2 | 12.3 | 39.0 | 223.1 | 1013.4 | 1018 | 1024 | 1030 | 1036 | 1041 | 1046 | 1234 | 1245 | 1281 | 1706 | 2051 | 2454 | 3040 |
| kyber1024 | 12.4 | 12.3 | 12.3 | 12.4 | 39.7 | 45.3 | 246.5 | 1016 | 1026 | 1035 | 1040 | 1042 | 1068 | 1233 | 1264 | 1434 | 2061 | 2194 | 3046 | 3058 |
| kyber90s512 | 12.2 | 12.1 | 12.1 | 12.0 | 220.0 | 225.3 | 1012.5 | 1019 | 1023 | 1029 | 1035 | 1037 | 1039 | 1041 | 1240 | 1256 | 1936 | 2325 | 3040 | 3040 |
| kyber90s768 | 12.3 | 12.2 | 12.2 | 12.3 | 41.1 | 224.9 | 1013.6 | 1019 | 1027 | 1032 | 1039 | 1039 | 1044 | 1237 | 1248 | 1421 | 1696 | 2059 | 3033 | 3043 |
| kyber90s1024 | 12.3 | 12.2 | 12.1 | 12.2 | 37.9 | 41.1 | 682.9 | 1023 | 1024 | 1034 | 1039 | 1040 | 1057 | 1232 | 1250 | 1553 | 2122 | 2060 | 2523 | 3253 |
| p256_kyber512 | 12.6 | 12.5 | 12.4 | 12.6 | 216.7 | 223.0 | 265.9 | 1017 | 1028 | 1031 | 1040 | 1042 | 1044 | 1241 | 1256 | 1258 | 2063 | 2059 | 2053 | 3038 |
| p384_kyber768 | 18.9 | 18.8 | 18.7 | 18.7 | 46.4 | 251.9 | 256.6 | 1023 | 1035 | 1040 | 1041 | 1046 | 1060 | 1235 | 1269 | 1705 | 2049 | 2099 | 3040 | 3051 |
| p256_kyber90s512 | 12.6 | 12.5 | 12.5 | 12.7 | 217.1 | 227.2 | 250.6 | 1019 | 1028 | 1032 | 1037 | 1043 | 1224 | 1242 | 1257 | 1275 | 2012 | 2045 | 2063 | 3037 |
| p384_kyber90s768 | 19.0 | 18.8 | 18.5 | 18.3 | 44.5 | 256.0 | 707.0 | 1024 | 1033 | 1039 | 1042 | 1044 | 1075 | 1247 | 1260 | 1541 | 2054 | 2299 | 3053 | 3051 |
| p521_kyber90s1024 | 27.9 | 27.7 | 28.0 | 28.7 | 49.8 | 254.9 | 384.6 | 1027 | 1039 | 1041 | 1049 | 1050 | 1053 | 1262 | 1452 | 2048 | 2051 | 2258 | 3053 | 3269 |
| p521_kyber1024 | 27.6 | 27.5 | 27.1 | 27.9 | 52.7 | 253.5 | 1022.2 | 1026 | 1037 | 1041 | 1048 | 1050 | 1073 | 1269 | 1831 | 1636 | 1845 | 2118 | 3048 | 3261 |
| p256_ntru_hps2048509 | 13.0 | 12.7 | 12.8 | 12.8 | 38.6 | 226.4 | 248.6 | 1021 | 1027 | 1030 | 1040 | 1040 | 1046 | 1239 | 1248 | 1258 | 1444 | 2034 | 2613 | 3040 |
| p384_ntru_hps2048677 | 19.1 | 19.2 | 18.4 | 19.8 | 224.1 | 228.0 | 1016.7 | 1024 | 1029 | 1038 | 1039 | 1041 | 1046 | 1242 | 1248 | 1260 | 1952 | 2050 | 3038 | 3058 |
| p521_ntru_hps4096821 | 28.2 | 28.2 | 28.1 | 28.5 | 53.4 | 260.6 | 1025.2 | 1029 | 1037 | 1043 | 1051 | 1053 | 1237 | 1251 | 1444 | 1664 | 2065 | 2630 | 3059 | 3294 |
| p384_ntru_hrss701 | 18.9 | 18.8 | 18.3 | 18.3 | 246.8 | 251.4 | 1017.3 | 1025 | 1031 | 1040 | 1042 | 1046 | 1115 | 1252 | 1305 | 1879 | 2045 | 2816 | 3040 | 3246 |
| lightsaber | 11.9 | 11.8 | 11.8 | 11.9 | 220.4 | 225.0 | 1012.2 | 1017 | 1021 | 1027 | 1032 | 1035 | 1036 | 1224 | 1238 | 1243 | 1450 | 2048 | 2259 | 2857 |
| saber | 12.0 | 11.9 | 11.8 | 11.9 | 13.6 | 244.6 | 1017.8 | 1012 | 1024 | 1032 | 1037 | 1038 | 1054 | 1235 | 1253 | 1545 | 2034 | 2057 | 3036 | 3043 |
| firesaber | 12.4 | 12.3 | 12.2 | 12.4 | 38.8 | 84.5 | 1015.0 | 1020 | 1026 | 1032 | 1037 | 1042 | 1045 | 1244 | 1259 | 1890 | 2043 | 2065 | 3053 | 3267 |
| p256_lightsaber | 12.7 | 12.3 | 12.4 | 12.5 | 217.3 | 224.6 | 249.2 | 1020 | 1027 | 1032 | 1040 | 1041 | 1044 | 1232 | 1252 | 1464 | 1894 | 2045 | 2834 | 3045 |
| p384_saber | 18.4 | 18.5 | 17.7 | 18.9 | 227.5 | 251.4 | 271.1 | 1022 | 1030 | 1034 | 1040 | 1044 | 1046 | 1239 | 1258 | 1254 | 1820 | 2280 | 2389 | 3038 |
| p521_firesaber | 27.5 | 27.2 | 27.3 | 27.7 | 51.1 | 258.2 | 372.7 | 1025 | 1038 | 1040 | 1049 | 1050 | 1055 | 1262 | 1275 | 1463 | 1887 | 2422 | 3044 | 3286 |
| ntru_hrss701 | 12.1 | 12.0 | 12.1 | 12.1 | 216.0 | 227.3 | 253.3 | 1020 | 1025 | 1032 | 1035 | 1042 | 1043 | 1239 | 1241 | 1341 | 2040 | 1823 | 2063 | 3046 |
| ntru_hps4096821 | 12.1 | 12.1 | 12.1 | 12.1 | 39.9 | 243.9 | 333.8 | 1022 | 1027 | 1032 | 1039 | 1042 | 1044 | 1250 | 1448 | 1622 | 2051 | 2275 | 2912 | 3044 |
| ntru_hps2048509 | 11.9 | 11.9 | 11.8 | 12.0 | 220.7 | 225.7 | 227.4 | 1017 | 1023 | 1028 | 1032 | 1034 | 1037 | 1042 | 1240 | 1248 | 1250 | 2304 | 2458 | 3035 |
| ntru_hps2048677 | 12.0 | 12.0 | 12.0 | 12.0 | 220.9 | 243.8 | 1012.3 | 1020 | 1026 | 1032 | 1037 | 1041 | 1043 | 1228 | 1241 | 1257 | 2047 | 2054 | 2398 | 3035 |
| prime256v1 | 12.0 | 11.9 | 12.0 | 12.0 | 221.4 | 222.9 | 1012.4 | 1015 | 1026 | 1027 | 1033 | 1035 | 1035 | 1044 | 1227 | 1244 | 1441 | 2034 | 3031 | 3043 |

**Figure 14.** Results of the handshake for the best RTT scenario (the 95th percentile — time in ms).

| | 0.0% | 0.1% | 0.5% | 1% | 1.5% | 2% | 2.5% | 3% | 4% | 5% | 6% | 7% | 8% | 9% | 10% | 11% | 12% | 13% | 14% | 15% |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| lightsaber | 62.9 | 62.7 | 62.7 | 62.7 | 62.7 | 62.7 | 62.7 | 62.7 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.9 | 62.8 | 62.9 | 62.9 | 62.9 |
| saber | 62.9 | 62.7 | 62.7 | 62.7 | 62.7 | 62.8 | 62.9 | 63.0 | 62.9 | 63.1 | 63.0 | 63.0 | 62.9 | 62.9 | 62.9 | 62.9 | 62.9 | 63.0 | 63.0 | 63.0 |
| p256_kyber512 | 63.0 | 62.9 | 62.9 | 62.9 | 62.9 | 62.9 | 62.9 | 63.0 | 63.0 | 63.0 | 63.0 | 63.0 | 63.1 | 63.1 | 63.1 | 63.1 | 63.1 | 63.2 | 63.2 | 63.2 |
| kyber512 | 63.0 | 62.8 | 62.7 | 62.7 | 62.7 | 62.7 | 62.7 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.9 | 62.8 | 62.9 | 62.9 | 62.9 | 63.0 | 63.2 |
| kyber90s768 | 63.0 | 62.7 | 62.7 | 62.7 | 62.7 | 62.7 | 62.8 | 62.8 | 62.8 | 62.9 | 62.8 | 62.9 | 62.8 | 62.9 | 62.9 | 62.9 | 62.9 | 62.9 | 62.9 | 63.0 |
| ntru_hps2048509 | 63.0 | 62.8 | 62.7 | 62.7 | 62.7 | 62.7 | 62.7 | 62.7 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.9 | 62.9 | 62.9 | 62.9 | 63.0 | 63.0 |
| kyber768 | 63.0 | 62.8 | 62.7 | 62.7 | 62.7 | 62.7 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.9 | 62.9 | 62.9 | 63.0 | 63.0 | 63.2 | 63.2 | 63.1 |
| kyber90s512 | 63.0 | 62.8 | 62.7 | 62.7 | 62.7 | 62.7 | 62.7 | 62.7 | 62.7 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.9 | 62.9 | 62.9 | 62.9 | 63.0 |
| kyber1024 | 63.1 | 62.9 | 62.8 | 62.8 | 62.8 | 62.9 | 62.9 | 62.9 | 62.9 | 63.1 | 63.0 | 63.0 | 63.0 | 63.0 | 63.1 | 63.1 | 63.1 | 63.1 | 63.2 | 63.3 |
| ntru_hps2048677 | 63.1 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.9 | 62.9 | 62.9 | 62.9 | 63.0 | 63.0 | 63.0 | 63.0 | 63.0 | 63.1 |
| kyber90s1024 | 63.1 | 62.9 | 62.8 | 62.8 | 62.8 | 62.8 | 62.7 | 62.7 | 62.7 | 62.8 | 62.8 | 62.8 | 62.8 | 62.9 | 62.9 | 62.9 | 62.9 | 62.9 | 63.0 | 63.0 |
| ntru_hrss701 | 63.2 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.8 | 62.9 | 62.9 | 62.9 | 62.9 | 62.9 | 63.0 | 63.0 | 63.0 | 63.0 | 63.1 | 63.2 | 63.2 |
| ntru_hps4096821 | 63.2 | 62.9 | 62.9 | 62.9 | 62.9 | 62.9 | 62.9 | 62.9 | 62.9 | 62.9 | 63.0 | 63.0 | 63.0 | 63.0 | 63.0 | 63.1 | 63.1 | 63.1 | 63.1 | 63.2 |
| firesaber | 63.3 | 62.9 | 63.0 | 62.9 | 62.9 | 62.9 | 63.0 | 63.0 | 63.0 | 63.0 | 63.0 | 63.0 | 63.0 | 63.0 | 63.1 | 63.1 | 63.1 | 63.1 | 63.1 | 63.1 |
| prime256v1 | 63.5 | 63.2 | 63.1 | 63.1 | 63.1 | 63.2 | 63.2 | 63.1 | 63.2 | 63.2 | 63.3 | 63.3 | 63.3 | 63.3 | 63.3 | 63.3 | 63.3 | 63.4 | 63.4 | 63.4 |
| p256_kyber90s512 | 63.6 | 63.5 | 63.4 | 63.4 | 63.4 | 63.4 | 63.4 | 63.4 | 63.4 | 63.4 | 63.5 | 63.5 | 63.5 | 63.5 | 63.5 | 63.5 | 63.5 | 63.5 | 63.5 | 63.6 |
| p256_lightsaber | 63.6 | 63.4 | 63.4 | 63.3 | 63.3 | 63.3 | 63.3 | 63.3 | 63.4 | 63.4 | 63.4 | 63.4 | 63.4 | 63.4 | 63.5 | 63.5 | 63.5 | 63.6 | 63.6 | 63.6 |
| p256_ntru_hps2048509 | 63.8 | 63.5 | 63.4 | 63.4 | 63.5 | 63.5 | 63.5 | 63.5 | 63.5 | 63.5 | 63.6 | 63.6 | 63.5 | 63.6 | 63.6 | 63.6 | 63.6 | 63.6 | 63.7 | 63.7 |
| p384_saber | 66.5 | 66.5 | 66.5 | 66.5 | 66.5 | 66.5 | 66.5 | 66.5 | 66.5 | 66.6 | 66.6 | 66.6 | 66.7 | 66.8 | 66.8 | 66.7 | 66.7 | 66.7 | 66.7 | 67.0 |
| p384_kyber768 | 66.6 | 66.6 | 66.6 | 66.6 | 66.6 | 66.6 | 66.6 | 66.6 | 66.6 | 66.6 | 66.7 | 66.7 | 66.7 | 66.7 | 66.8 | 66.8 | 66.8 | 66.8 | 66.9 | 66.9 |
| p384_kyber90s768 | 66.7 | 66.7 | 66.7 | 66.7 | 66.7 | 66.7 | 66.8 | 66.9 | 66.9 | 66.9 | 66.8 | 66.8 | 66.9 | 66.8 | 66.8 | 67.0 | 67.0 | 66.9 | 67.0 | 67.1 |
| p384_ntru_hrss701 | 66.8 | 66.8 | 66.8 | 66.8 | 66.8 | 66.8 | 66.8 | 66.8 | 66.8 | 66.9 | 66.9 | 66.9 | 66.9 | 67.0 | 67.0 | 67.0 | 67.0 | 67.1 | 67.1 | 67.1 |
| p384_ntru_hps2048677 | 67.0 | 67.0 | 67.0 | 67.0 | 66.9 | 66.8 | 66.8 | 66.8 | 66.8 | 66.9 | 66.9 | 66.9 | 66.9 | 67.0 | 67.1 | 67.0 | 67.0 | 67.2 | 67.1 | 67.1 |
| p521_kyber1024 | 71.6 | 71.6 | 71.6 | 71.6 | 71.6 | 71.6 | 71.6 | 71.6 | 71.6 | 71.6 | 71.6 | 71.6 | 71.7 | 71.7 | 71.9 | 71.8 | 71.9 | 71.8 | 71.9 | 72.0 |
| p521_firesaber | 71.7 | 71.6 | 71.7 | 71.6 | 71.6 | 71.6 | 71.6 | 71.6 | 71.6 | 71.6 | 71.6 | 71.6 | 71.6 | 71.7 | 71.7 | 71.7 | 71.7 | 71.8 | 71.8 | 72.1 |
| p521_ntru_hps4096821 | 71.8 | 71.9 | 71.9 | 71.8 | 72.0 | 72.1 | 72.1 | 72.1 | 72.0 | 71.9 | 71.9 | 72.0 | 71.9 | 72.0 | 72.1 | 72.1 | 72.1 | 72.1 | 72.1 | 73.5 |
| p521_kyber90s1024 | 71.9 | 71.7 | 71.7 | 71.7 | 71.7 | 71.7 | 71.7 | 71.8 | 71.8 | 71.8 | 71.8 | 71.8 | 71.8 | 71.9 | 72.0 | 71.8 | 71.9 | 71.9 | 72.1 | 72.2 |

**Figure 15.** Results of the handshake time for the moderate RTT scenario (the median time in ms).

| | 0.0% | 0.1% | 0.5% | 1% | 1.5% | 2% | 2.5% | 3% | 4% | 5% | 6% | 7% | 8% | 9% | 10% | 11% | 12% | 13% | 14% | 15% |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| kyber512 | 63.3 | 63.2 | 62.9 | 63.1 | 297 | 297 | 566 | 1069 | 1074 | 1076 | 1081 | 1088 | 1089 | 1264 | 1299 | 1377 | 1818 | 2102 | 2257 | 3090 |
| kyber768 | 63.3 | 63.2 | 63.1 | 63.1 | 291 | 351 | 1066 | 1069 | 1088 | 1088 | 1094 | 1106 | 1108 | 1306 | 1384 | 2022 | 2081 | 2305 | 2384 | 3104 |
| kyber1024 | 63.4 | 63.4 | 63.2 | 63.2 | 167 | 170 | 1066 | 1072 | 1079 | 1089 | 1102 | 1103 | 1329 | 1338 | 1550 | 1943 | 2883 | 2532 | 3121 | 3408 |
| kyber90s512 | 63.3 | 63.1 | 63.1 | 63.1 | 296 | 298 | 1065 | 1071 | 1073 | 1076 | 1080 | 1088 | 1092 | 1095 | 1311 | 1378 | 2080 | 2099 | 3087 | 3087 |
| kyber90s768 | 63.3 | 63.0 | 63.1 | 62.9 | 168 | 358 | 1066 | 1072 | 1082 | 1090 | 1098 | 1103 | 1109 | 1328 | 1358 | 1623 | 2083 | 2103 | 3088 | 3103 |
| kyber90s1024 | 63.4 | 63.2 | 63.1 | 63.1 | 168 | 372 | 1064 | 1066 | 1078 | 1090 | 1096 | 1104 | 1309 | 1337 | 1561 | 2090 | 2602 | 2941 | 3117 | 3244 |
| p256_kyber512 | 63.3 | 63.2 | 63.2 | 63.3 | 309 | 353 | 1064 | 1067 | 1079 | 1090 | 1099 | 1104 | 1106 | 1121 | 1381 | 1568 | 2075 | 2112 | 2497 | 3105 |
| p384_kyber768 | 68.0 | 67.9 | 67.8 | 68.5 | 174 | 377 | 452 | 1072 | 1079 | 1090 | 1098 | 1118 | 1301 | 1602 | 1834 | 2027 | 2110 | 2629 | 3130 | 3422 |
| p256_kyber90s512 | 64.1 | 63.8 | 63.7 | 63.9 | 169 | 305 | 1067 | 1070 | 1086 | 1090 | 1098 | 1103 | 1106 | 1304 | 1382 | 1507 | 2095 | 2115 | 2725 | 3104 |
| p384_kyber90s768 | 68.2 | 67.8 | 68.0 | 69.4 | 173 | 376 | 407 | 1073 | 1082 | 1089 | 1100 | 1108 | 1115 | 1338 | 1601 | 2079 | 2120 | 2323 | 3134 | 3491 |
| p521_kyber90s1024 | 75.7 | 75.5 | 75.7 | 77.2 | 178 | 383 | 417 | 1079 | 1085 | 1091 | 1104 | 1113 | 1123 | 1400 | 1528 | 2038 | 2089 | 2829 | 3146 | 3151 |
| p521_kyber1024 | 75.3 | 74.2 | 75.5 | 76.1 | 178 | 381 | 1075 | 1077 | 1085 | 1092 | 1106 | 1112 | 1299 | 1397 | 1826 | 2033 | 2209 | 3123 | 3128 | 3214 |
| p256_ntru_hps2048509 | 64.2 | 63.9 | 63.9 | 63.9 | 293 | 300 | 376 | 1073 | 1088 | 1094 | 1099 | 1105 | 1108 | 1168 | 1396 | 1384 | 2080 | 2097 | 3085 | 2626 |
| p384_ntru_hps2048677 | 68.5 | 68.6 | 68.9 | 69.0 | 299 | 377 | 419 | 1076 | 1082 | 1089 | 1099 | 1098 | 1108 | 1337 | 1377 | 1662 | 2082 | 2315 | 3089 | 3103 |
| p521_ntru_hps4096821 | 75.6 | 75.4 | 75.9 | 79.0 | 178 | 387 | 436 | 1076 | 1088 | 1097 | 1103 | 1116 | 1296 | 1391 | 1666 | 2112 | 2309 | 2712 | 3423 | 3380 |
| p384_ntru_hrss701 | 68.2 | 67.8 | 68.2 | 68.7 | 172 | 376 | 1068 | 1073 | 1085 | 1088 | 1099 | 1105 | 1179 | 1388 | 2046 | 2105 | 2288 | 2450 | 3135 | 3159 |
| lightsaber | 63.1 | 63.0 | 63.0 | 63.0 | 296 | 299 | 344 | 1067 | 1074 | 1077 | 1085 | 1089 | 1090 | 1093 | 1309 | 1328 | 1600 | 2083 | 2407 | 3104 |
| saber | 63.2 | 63.0 | 63.1 | 63.0 | 169 | 372 | 377 | 1065 | 1077 | 1092 | 1095 | 1103 | 1113 | 1334 | 1382 | 1400 | 2104 | 2521 | 3081 | 3088 |
| firesaber | 63.6 | 63.3 | 63.3 | 63.4 | 168 | 371 | 375 | 1067 | 1081 | 1092 | 1103 | 1107 | 1132 | 1417 | 1632 | 2033 | 2159 | 2550 | 3130 | 3394 |
| p256_lightsaber | 64.0 | 63.9 | 63.7 | 63.8 | 172 | 374 | 1064 | 1073 | 1080 | 1089 | 1103 | 1103 | 1105 | 1336 | 1350 | 1809 | 1860 | 2097 | 3088 | 3112 |
| p384_saber | 68.2 | 68.4 | 68.2 | 68.4 | 295 | 378 | 379 | 1069 | 1080 | 1087 | 1091 | 1102 | 1107 | 1360 | 1406 | 1870 | 2030 | 2100 | 3041 | 3101 |
| p521_firesaber | 75.3 | 75.5 | 75.2 | 78.3 | 177 | 384 | 1073 | 1081 | 1088 | 1096 | 1103 | 1115 | 1180 | 1417 | 1546 | 2097 | 2122 | 3126 | 3170 | 3454 |
| ntru_hrss701 | 63.5 | 63.3 | 63.0 | 63.2 | 295 | 371 | 1064 | 1068 | 1084 | 1088 | 1094 | 1106 | 1110 | 1360 | 1397 | 1505 | 1893 | 2112 | 3083 | 3097 |
| ntru_hps4096821 | 63.5 | 63.3 | 63.3 | 63.3 | 169 | 374 | 1064 | 1070 | 1088 | 1093 | 1100 | 1103 | 1111 | 1337 | 1572 | 2017 | 2112 | 2401 | 3141 | 3297 |
| ntru_hps2048509 | 63.3 | 63.1 | 62.9 | 63.1 | 294 | 302 | 358 | 1067 | 1071 | 1075 | 1083 | 1088 | 1089 | 1095 | 1312 | 1379 | 1562 | 2087 | 2465 | 3097 |
| ntru_hps2048677 | 63.4 | 63.2 | 63.1 | 63.2 | 330 | 372 | 403 | 1071 | 1075 | 1090 | 1102 | 1104 | 1106 | 1344 | 1376 | 1591 | 1816 | 2097 | 2405 | 3104 |
| prime256v1 | 63.8 | 63.6 | 63.5 | 63.5 | 295 | 339 | 1066 | 1065 | 1074 | 1075 | 1087 | 1088 | 1091 | 1304 | 1320 | 1362 | 2072 | 2316 | 2452 | 3091 |

**Figure 16.** Results of the handshake for the moderate RTT scenario (the 95th percentile — time in ms).

| | 0.0% | 0.1% | 0.5% | 1% | 1.5% | 2% | 2.5% | 3% | 4% | 5% | 6% | 7% | 8% | 9% | 10% | 11% | 12% | 13% | 14% | 15% |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| lightsaber | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 |
| kyber90s512 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 |
| kyber512 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 |
| ntru_hrss701 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 |
| ntru_hps2048509 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 |
| ntru_hps2048677 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 |
| firesaber | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 |
| kyber90s1024 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 |
| kyber768 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 |
| kyber90s768 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 |
| saber | 159 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 |
| kyber1024 | 159 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 |
| ntru_hps4096821 | 159 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 |
| p256_kyber512 | 159 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 159 | 158 | 159 |
| prime256v1 | 159 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 158 | 159 |
| p256_kyber90s512 | 159 | 159 | 158 | 158 | 159 | 158 | 158 | 159 | 158 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 |
| p256_lightsaber | 159 | 159 | 158 | 158 | 158 | 158 | 158 | 158 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 |
| p256_ntru_hps2048509 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 | 159 |
| p384_saber | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 |
| p384_kyber90s768 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 |
| p384_ntru_hrss701 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 |
| p384_ntru_hps2048677 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 163 |
| p384_kyber768 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 | 162 |
| p521_kyber90s1024 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 |
| p521_firesaber | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 |
| p521_kyber1024 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 |
| p521_ntru_hps4096821 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 | 167 |

**Figure 17.** Results of the handshake time for the bad RTT scenario (the median time in ms).

| | 0.0% | 0.1% | 0.5% | 1% | 1.5% | 2% | 2.5% | 3% | 4% | 5% | 6% | 7% | 8% | 9% | 10% | 11% | 12% | 13% | 14% | 15% |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| kyber512 | 158 | 158 | 158 | 158 | 439 | 458 | 1159 | 1163 | 1167 | 1174 | 1178 | 1181 | 1184 | 1187 | 1484 | 1547 | 2176 | 2536 | 3175 | 3182 |
| kyber768 | 159 | 159 | 158 | 158 | 444 | 612 | 1161 | 1164 | 1183 | 1238 | 1247 | 1252 | 1279 | 1536 | 1628 | 1638 | 2204 | 2417 | 3041 | 3200 |
| kyber1024 | 159 | 158 | 158 | 158 | 406 | 408 | 687 | 1161 | 1178 | 1188 | 1245 | 1257 | 1454 | 1543 | 1784 | 2340 | 2263 | 3254 | 3255 | 3638 |
| kyber90s512 | 158 | 158 | 158 | 158 | 443 | 467 | 1160 | 1163 | 1168 | 1173 | 1176 | 1181 | 1184 | 1186 | 1472 | 1747 | 2137 | 3175 | 2845 | 3188 |
| kyber90s768 | 159 | 159 | 159 | 158 | 450 | 545 | 1159 | 1169 | 1177 | 1236 | 1242 | 1253 | 1259 | 1530 | 1552 | 1672 | 2254 | 2593 | 3182 | 3265 |
| kyber90s1024 | 159 | 158 | 158 | 158 | 406 | 616 | 704 | 1165 | 1180 | 1244 | 1248 | 1258 | 1361 | 1533 | 1647 | 2191 | 2615 | 3254 | 3278 | 3573 |
| p256_kyber512 | 159 | 159 | 159 | 159 | 406 | 544 | 701 | 1162 | 1179 | 1239 | 1241 | 1254 | 1258 | 1530 | 1557 | 1635 | 2185 | 2258 | 3186 | 3193 |
| p384_kyber768 | 164 | 163 | 164 | 164 | 411 | 632 | 1163 | 1175 | 1187 | 1192 | 1253 | 1263 | 1432 | 1583 | 1855 | 2137 | 2207 | 2708 | 3303 | 3646 |
| p256_kyber90s512 | 159 | 159 | 159 | 159 | 408 | 467 | 621 | 1169 | 1185 | 1237 | 1246 | 1253 | 1259 | 1529 | 1794 | 1643 | 2193 | 2666 | 3182 | 3253 |
| p384_kyber90s768 | 163 | 163 | 162 | 165 | 411 | 640 | 1164 | 1171 | 1182 | 1240 | 1246 | 1375 | 1465 | 1547 | 1962 | 2257 | 2187 | 2792 | 3282 | 3440 |
| p521_kyber90s1024 | 169 | 169 | 170 | 170 | 415 | 631 | 646 | 1184 | 1192 | 1247 | 1260 | 1268 | 1536 | 1638 | 2000 | 2201 | 2369 | 3266 | 3566 | 3865 |
| p521_kyber1024 | 169 | 170 | 170 | 173 | 417 | 637 | 1170 | 1172 | 1190 | 1248 | 1259 | 1264 | 1478 | 1598 | 1865 | 2194 | 2437 | 2720 | 3278 | 3295 |
| p256_ntru_hps2048509 | 159 | 159 | 159 | 159 | 411 | 459 | 534 | 1165 | 1179 | 1239 | 1243 | 1254 | 1260 | 1543 | 1548 | 1648 | 2137 | 2353 | 3177 | 3190 |
| p384_ntru_hps2048677 | 163 | 163 | 163 | 164 | 410 | 626 | 963 | 1166 | 1187 | 1193 | 1247 | 1254 | 1257 | 1533 | 1552 | 1840 | 2202 | 3180 | 3181 | 3202 |
| p521_ntru_hps4096821 | 169 | 170 | 169 | 170 | 415 | 645 | 1170 | 1179 | 1193 | 1197 | 1256 | 1267 | 1457 | 1580 | 1817 | 2194 | 2431 | 2905 | 3486 | 3293 |
| p384_ntru_hrss701 | 163 | 163 | 163 | 164 | 411 | 783 | 1164 | 1167 | 1183 | 1224 | 1244 | 1263 | 1434 | 1627 | 1647 | 2147 | 2417 | 2696 | 3277 | 3549 |
| lightsaber | 158 | 158 | 158 | 158 | 455 | 468 | 1159 | 1163 | 1168 | 1172 | 1177 | 1181 | 1186 | 1188 | 1471 | 1544 | 2186 | 2187 | 2611 | 3183 |
| saber | 159 | 158 | 158 | 159 | 448 | 461 | 1158 | 1164 | 1178 | 1188 | 1250 | 1252 | 1436 | 1545 | 1553 | 1740 | 2194 | 2346 | 3178 | 3194 |
| firesaber | 159 | 159 | 158 | 158 | 406 | 628 | 1163 | 1168 | 1184 | 1243 | 1247 | 1257 | 1467 | 1538 | 1760 | 2176 | 2613 | 2748 | 3279 | 3475 |
| p256_lightsaber | 159 | 159 | 159 | 159 | 408 | 487 | 1159 | 1165 | 1185 | 1240 | 1247 | 1256 | 1257 | 1531 | 1545 | 1832 | 2185 | 3175 | 3183 | 3193 |
| p384_saber | 163 | 162 | 163 | 163 | 442 | 640 | 719 | 1166 | 1181 | 1189 | 1248 | 1252 | 1258 | 1546 | 1618 | 2024 | 1928 | 2445 | 3178 | 3194 |
| p521_firesaber | 170 | 169 | 170 | 170 | 416 | 631 | 647 | 1175 | 1190 | 1248 | 1255 | 1267 | 1477 | 1625 | 1677 | 2199 | 2923 | 3238 | 3291 | 3642 |
| ntru_hrss701 | 159 | 159 | 158 | 158 | 442 | 544 | 624 | 1167 | 1181 | 1189 | 1242 | 1253 | 1387 | 1481 | 1543 | 1670 | 2193 | 2434 | 3179 | 3200 |
| ntru_hps4096821 | 159 | 158 | 158 | 158 | 405 | 620 | 690 | 1169 | 1184 | 1188 | 1246 | 1259 | 1543 | 1557 | 1886 | 1832 | 2356 | 2549 | 3268 | 3357 |
| ntru_hps2048509 | 158 | 158 | 158 | 158 | 454 | 473 | 536 | 1161 | 1167 | 1173 | 1178 | 1181 | 1186 | 1461 | 1465 | 1540 | 2195 | 2201 | 2941 | 3184 |
| ntru_hps2048677 | 159 | 158 | 158 | 158 | 406 | 538 | 1160 | 1166 | 1186 | 1188 | 1246 | 1254 | 1259 | 1542 | 1556 | 1820 | 2183 | 2210 | 2980 | 3194 |
| prime256v1 | 159 | 159 | 159 | 159 | 448 | 537 | 529 | 1161 | 1169 | 1174 | 1179 | 1183 | 1186 | 1189 | 1482 | 1487 | 1597 | 2295 | 2772 | 3184 |

**Figure 18.** Results of the handshake for the bad RTT scenario (the 95th percentile — time in ms).

| | 0.0% | 0.1% | 0.5% | 1% | 1.5% | 2% | 2.5% | 3% | 4% | 5% | 6% | 7% | 8% | 9% | 10% | 11% | 12% | 13% | 14% | 15% |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| lightsaber | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 |
| saber | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 |
| kyber90s1024 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 |
| ntru_hps2048509 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 |
| firesaber | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 |
| kyber1024 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 |
| kyber90s512 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 |
| ntru_hps2048677 | 393 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 |
| kyber512 | 393 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 |
| kyber90s768 | 393 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 |
| ntru_hrss701 | 393 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 |
| kyber768 | 393 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 |
| p256_kyber512 | 393 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 393 | 392 |
| prime256v1 | 393 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 393 | 393 |
| ntru_hps4096821 | 393 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 |
| p256_lightsaber | 393 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 392 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 |
| p256_kyber90s512 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 |
| p256_ntru_hps2048509 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 | 393 |
| p384_saber | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 |
| p384_kyber90s768 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 |
| p384_kyber768 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 |
| p384_ntru_hps2048677 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 |
| p384_ntru_hrss701 | 397 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 | 396 |
| p521_kyber90s1024 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 |
| p521_firesaber | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 |
| p521_kyber1024 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 |
| p521_ntru_hps4096821 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 | 401 |

**Figure 19.** Results of the handshake time for the worst RTT scenario (the median time in ms).

| | 0.0% | 0.1% | 0.5% | 1% | 1.5% | 2% | 2.5% | 3% | 4% | 5% | 6% | 7% | 8% | 9% | 10% | 11% | 12% | 13% | 14% | 15% |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| kyber512 | 393 | 393 | 393 | 392 | 985 | 1005 | 1012 | 1399 | 1404 | 1409 | 1414 | 1415 | 1600 | 1607 | 2014 | 2023 | 2420 | 3030 | 3425 | 3428 |
| kyber768 | 393 | 393 | 392 | 393 | 995 | 1012 | 1404 | 1410 | 1426 | 1595 | 1602 | 1615 | 1656 | 2196 | 2240 | 2449 | 3198 | 3265 | 3609 | 4139 |
| kyber1024 | 393 | 393 | 392 | 392 | 1008 | 1013 | 1408 | 1412 | 1591 | 1603 | 1608 | 1845 | 2202 | 2412 | 2425 | 2820 | 3197 | 3678 | 3625 | 4221 |
| kyber90s512 | 393 | 392 | 392 | 393 | 988 | 1002 | 1395 | 1400 | 1406 | 1411 | 1414 | 1421 | 1594 | 1624 | 2012 | 2424 | 2432 | 2808 | 3424 | 3424 |
| kyber90s768 | 393 | 392 | 392 | 392 | 1002 | 1393 | 1411 | 1409 | 1423 | 1598 | 1598 | 1615 | 2010 | 2198 | 2415 | 2615 | 2810 | 3412 | 3447 | 3839 |
| kyber90s1024 | 393 | 392 | 392 | 392 | 990 | 1015 | 1406 | 1416 | 1431 | 1598 | 1606 | 1677 | 2087 | 2212 | 2519 | 3100 | 3611 | 3617 | 4008 | 4767 |
| p256_kyber512 | 393 | 393 | 393 | 392 | 997 | 1015 | 1405 | 1410 | 1427 | 1595 | 1607 | 1614 | 1998 | 2195 | 2416 | 2443 | 2811 | 3413 | 3508 | 3625 |
| p384_kyber768 | 398 | 397 | 397 | 397 | 998 | 1022 | 1404 | 1417 | 1552 | 1603 | 1617 | 1909 | 2222 | 2424 | 2636 | 2668 | 3224 | 3620 | 3634 | 4520 |
| p256_kyber90s512 | 393 | 393 | 393 | 393 | 991 | 1017 | 1394 | 1413 | 1419 | 1600 | 1609 | 1614 | 2004 | 2199 | 2424 | 2523 | 2609 | 3421 | 3638 | 4028 |
| p384_kyber90s768 | 398 | 397 | 397 | 397 | 1000 | 1399 | 1407 | 1418 | 1428 | 1603 | 1613 | 1634 | 2196 | 2335 | 2469 | 3284 | 3268 | 3619 | 4036 | 5114 |
| p521_kyber90s1024 | 403 | 403 | 403 | 407 | 1010 | 1406 | 1418 | 1427 | 1600 | 1612 | 1617 | 1726 | 2215 | 2437 | 2440 | 2806 | 3618 | 3620 | 4070 | 4235 |
| p521_kyber1024 | 404 | 403 | 403 | 405 | 1008 | 1027 | 1415 | 1420 | 1600 | 1615 | 1617 | 2001 | 2211 | 2337 | 2597 | 3076 | 3268 | 3636 | 3999 | 4832 |
| p256_ntru_hps2048509 | 393 | 393 | 393 | 393 | 984 | 1008 | 1017 | 1406 | 1432 | 1591 | 1603 | 1611 | 2010 | 2197 | 2225 | 2430 | 2783 | 3389 | 3456 | 3983 |
| p384_ntru_hps2048677 | 397 | 397 | 397 | 398 | 1004 | 1400 | 1407 | 1415 | 1428 | 1600 | 1605 | 1613 | 1951 | 2203 | 2430 | 2439 | 3415 | 3416 | 3436 | 3624 |
| p521_ntru_hps4096821 | 404 | 403 | 403 | 404 | 1022 | 1410 | 1421 | 1422 | 1469 | 1610 | 1620 | 1627 | 2016 | 2220 | 2452 | 2987 | 3500 | 3619 | 4249 | 4837 |
| p384_ntru_hrss701 | 398 | 397 | 397 | 398 | 1013 | 1398 | 1408 | 1421 | 1600 | 1604 | 1614 | 2012 | 2194 | 2432 | 2446 | 2989 | 3097 | 3640 | 4241 | 4236 |
| lightsaber | 393 | 392 | 392 | 392 | 986 | 1000 | 1014 | 1400 | 1405 | 1410 | 1414 | 1418 | 1420 | 1995 | 2014 | 2020 | 2620 | 2778 | 3400 | 3433 |
| saber | 393 | 392 | 392 | 392 | 984 | 1010 | 1398 | 1411 | 1428 | 1601 | 1603 | 1611 | 2008 | 2020 | 2222 | 2590 | 2804 | 3439 | 3427 | 4030 |
| firesaber | 393 | 393 | 392 | 392 | 1002 | 1012 | 1400 | 1418 | 1422 | 1599 | 1614 | 1877 | 2026 | 2204 | 2424 | 2788 | 3350 | 3619 | 4026 | 4628 |
| p256_lightsaber | 393 | 393 | 393 | 393 | 988 | 1394 | 1403 | 1414 | 1588 | 1596 | 1605 | 1613 | 2001 | 2207 | 2425 | 2436 | 3023 | 2800 | 3437 | 3744 |
| p384_saber | 397 | 397 | 397 | 398 | 989 | 1012 | 1401 | 1417 | 1444 | 1601 | 1606 | 1617 | 2016 | 2202 | 2206 | 2452 | 3056 | 3328 | 3436 | 3996 |
| p521_firesaber | 404 | 402 | 404 | 404 | 1020 | 1409 | 1419 | 1420 | 1598 | 1614 | 1621 | 1674 | 2211 | 2432 | 2621 | 3111 | 3318 | 3661 | 4065 | 5317 |
| ntru_hrss701 | 393 | 393 | 392 | 392 | 998 | 1009 | 1405 | 1409 | 1426 | 1593 | 1602 | 1613 | 1997 | 2013 | 2222 | 2600 | 2802 | 3426 | 3623 | 4028 |
| ntru_hps4096821 | 393 | 393 | 393 | 393 | 1004 | 1018 | 1400 | 1410 | 1426 | 1603 | 1605 | 1676 | 2194 | 2423 | 2430 | 2786 | 3614 | 3617 | 4017 | 4815 |
| ntru_hps2048509 | 393 | 392 | 392 | 392 | 392 | 1004 | 1393 | 1398 | 1408 | 1411 | 1413 | 1418 | 1422 | 1921 | 2016 | 2417 | 2434 | 2449 | 3423 | 3429 |
| ntru_hps2048677 | 393 | 392 | 392 | 392 | 988 | 1014 | 1401 | 1411 | 1438 | 1597 | 1603 | 1612 | 1998 | 2196 | 2420 | 2585 | 2790 | 3424 | 3429 | 3630 |
| prime256v1 | 393 | 393 | 393 | 393 | 986 | 1010 | 1395 | 1400 | 1409 | 1410 | 1414 | 1419 | 1421 | 1611 | 2010 | 2022 | 2444 | 2795 | 3409 | 3427 |

**Figure 20.** Results of the handshake for the worst RTT scenario (the 95th percentile — time in ms).