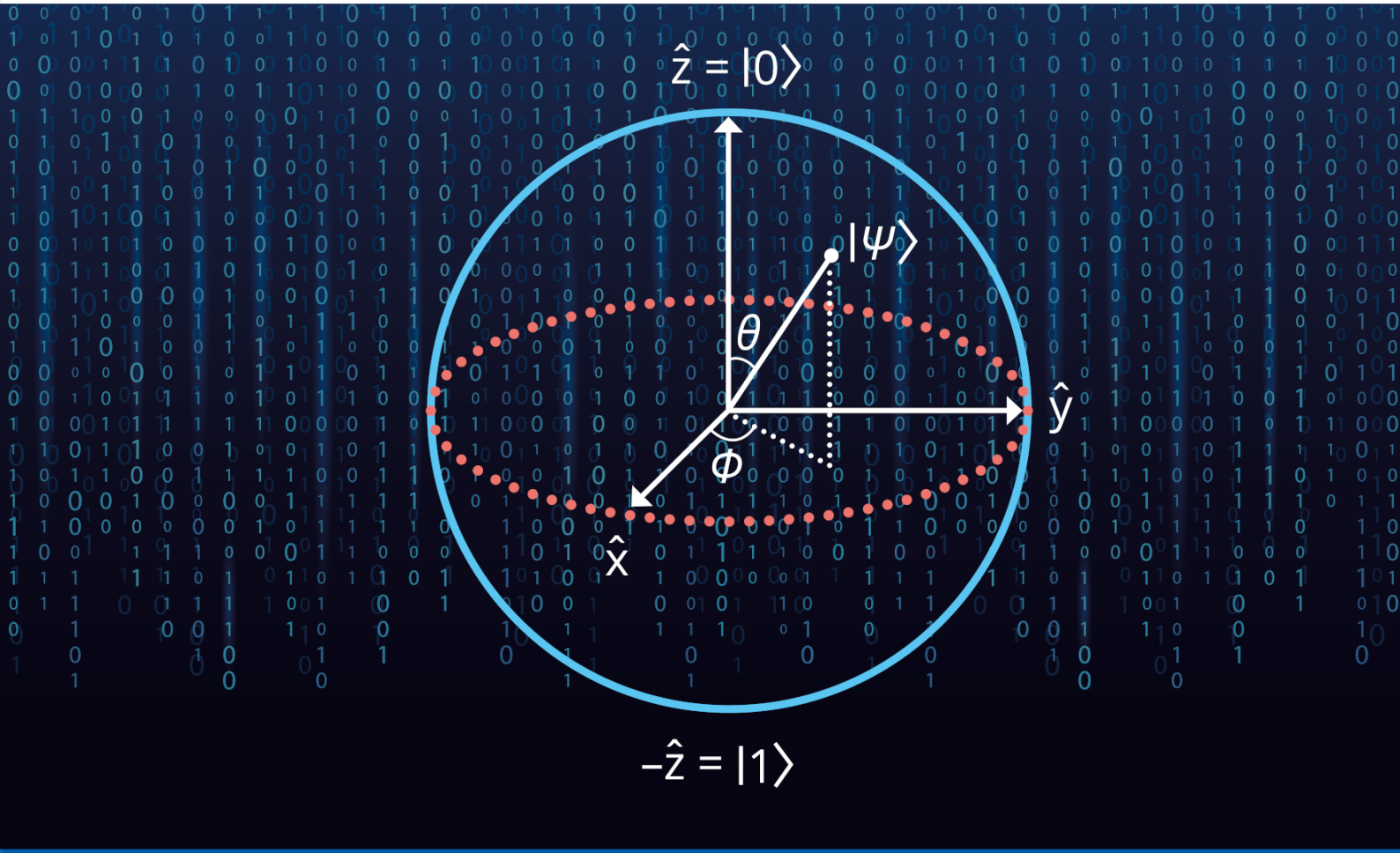
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



POST-QUANTUM CRYPTOGRAPHY

Integration study

OCTOBER 2022

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT
To contact the authors please use evangelos.rekleitis@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS
Daniel J. Bernstein, Ruhr University Bochum
Andreas Hülsing, Technische Universiteit Eindhoven
Tanja Lange, Technische Universiteit Eindhoven

FOR ENISA
Evangelos Rekleitis, ENISA

ACKNOWLEDGMENTS
Nikolaos Tantouris, ENISA
Radu Arcus, ENISA

ISBN: 978-92-9204-590-6. DOI: 10.2824/151162, Catalogue Number: TP-03-22-080-EN-N

CONTENTS

EXECUTIVE SUMMARY

With this report ENISA seeks to give insight on post-standardisation challenges. As a follow-up to ENISA's 2021 Post-Quantum Cryptography: Current state and quantum mitigation study[1], the new report elaborates on the topic to address the following points:

- Integrating post-quantum systems into existing protocols
- New protocols designed around post-quantum systems
- Double encryption and double signatures using post-quantum systems
- Seccurity proofs in the presence of quantum attackers
- Standardisation efforts for post-quantum enabled protocols

The 2021 study provided an overview of the current state of play on the standardisation process of Post-Quantum Cryptography (PQC)[2]. It introduced a framework for analysing existing PQC proposals, presented the five (5) main families of PQC algorithms[3], and the NIST Round 3 finalists for encryption and signature schemes[4]. It also sketched two proposals that proactive system owners can implement right now – before a standard is published – in order to protect the confidentiality of their data against a quantum capable attacker[5].

While agreeing on PQC cryptoalgorithms for encryption and signing is an important milestone [6], by itself it is not enough. Any new cryptoalgorithm will need to interplay with existing protocols or even require entirely new protocols to be designed and implemented. Furthermore, PQC proposals are a solution to a still unrealised vulnerability – there are currently no publicly known quantum computers, strong enough to break encryption, and not all scientists believe this will ever be the case[7]–. Whether we should implement protections against a threat that might not materialise would be a moot question if said implementations were cost free. However, PQC algorithms are often more costly, e.g. in terms of size and computations. In addition, changing to a new cryptographic paradigm might provide new opportunities for software bugs and our understanding of the security of the PQC algorithms is often less mature[8].

For each of the above open issues an overview of current developments is provided, along with future directions and identified gaps. Chapter 2 Integrating post-quantum systems into existing protocols provides an overview of the work done to integrate PQC proposals with current systems. It comments on the size and speed characteristics of the proposals, based on the benchmarks of the eBACS: ECRYPT Benchmarking of Cryptographic Systems project[9][11], and how they interplay with the Internet Protocol (IP) and security protocols

1 https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation, (accessed October 17, 2022).
2 e.g. NIST's https://csrc.nist.gov/Projects/post-quantum-cryptography, (accessed October 17, 2022).
3 code-based, isogeny-based, hash-based, lattice-based and multivariate-based
4 https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions, (accessed October 17, 2022).
5 viz. hybrid implementations that use a combination of pre-quantum and post-quantum schemes, and the mixing of pre-shared keys into all keys established via public-key cryptography.
6 While this report was being typeset and proofread NIST announced (July 2022) it had identified the four candidate algorithms for standardisation https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4 and https://csrc.nist.gov/publications/detail/nistir/8413/final, (accessed October 17, 2022).
7 See for example https://www.scientificamerican.com/article/will-quantum-computing-ever-live-up-to-its-hype/ and https://spectrum.ieee.org/the-case-against-quantum-computing, (accessed October 17, 2022).
8 As shown by the two recent cryptanalysis attacks against the Supersingular Isogeny Diffie-Hellman (SIDH) protocol – one by Wouter Castryck and Thomas Decru of KU Leuven and the other by Luciano Maino and Chloe Martindale of the University of Bristol. SIDH is at the core of the Post-Quantum key encapsulation mechanism SIKE (Supersingular Isogeny Key Encapsulation), which was selected to continue to round four of the NIST Post-Quantum Project for consideration of standardisation. https://eprint.iacr.org/2022/975, https://eprint.iacr.org/2022/1026 (accessed October 17, 2022).
9 https://bench.cr.yp.to/, (accessed October 17, 2022).

like TLS 1.3, VPN etc. As can be seen, not all use cases are created equal. For instance, in high-load cases, such as car2car communications, even apparently small differences between PQC proposals could have a significant impact by, for example, introducing latency or even incompatibility with existing communication protocols due to limits on message size. System designers will be required to understand the available options and make optimal choices for each use case, through calculated trade-offs.

A different approach would be to develop new protocols, taking into account the specifications of PQC systems from the design phase. The somewhat limited work done so far is mentioned in chapter 3 New protocols designed around post-quantum systems. The main outcome here is that existing work is promising but more research and deployment work is needed.

Chapter 4 Double encryption and double signatures takes on the veridical paradox that by striving for quantum resistance using a PQC system we might be lowering security overall. Actually, there is no guarantee that the post-quantum cryptosystems that survive the standardisation process are secure. So far cryptanalysts could have missed an important attack, perhaps even one that runs sufficiently quick on today's non-quantum computers. Furthermore, the complicated new ecosystem of post-quantum cryptographic software has a clear risk of introducing bugs. A solution to this might be to augment, instead of simply replacing, current modern cryptosystems with PQC systems. This can be done by adding an extra layer that also encrypts and/or signs using post-quantum cryptography, as already discussed in our 2021 study. Here we take a closer look at the details and caveats of such a construction. The take away is that if this is done *properly*, then any attack will require breaking the current cryptosystem (e.g. one based on elliptic-curves) and breaking the post-quantum system. So, even if there are vulnerabilities in the post-quantum cryptosystem or post-quantum software, there will be no damage to the security of the existing system. The perceptive reader will have guessed that once more further investigations are required, but standardisation bodies are already working on this, specifying suitable mechanisms.

Chapter 5 Security proofs in the presence of quantum attackers, deals with formal models and proofs an important part of the analysis of modern cryptographic systems. While we have known for decades Shor's and Grover's algorithms – the former breaking RSA and ECC public key cryptography and the latter reducing the security level of symmetric cryptography – ongoing research on quantum computing might yet reveal more attacks against schemes and protocols. This is why cryptologists are not only working on proofs for the new PQC systems and protocols, but are also revisiting existing proofs for widely used systems and protocols. When we aim for post-quantum security, i.e. security against adversaries making use of a quantum computer, we have to model the adversaries also as quantum algorithms. This requires changing models and deciding about the specific abilities of quantum adversaries. New proofs have to be written that take quantum adversaries into account. This process has been started and is progressing well for basic building blocks, especially those considered in the NIST competition. However, in many other areas, especially in the analysis of protocols, the process has not even begun.

Finally, chapter 6 Standardisation efforts for protocols briefly discusses the work done by standardisation bodies, going beyond NIST's seminal work, including ETSI, IETF and ISO, as well as recent reports by other European agencies, namely ANSSI and BSI. It is of interest to note that standardisation bodies continue to standardise protocols built using pre-quantum systems that will not withstand quantum attacks. In cases where significant developing investment has already been spent, one should consider applying the discussed concepts of double encryption, double signatures, etc. Otherwise the sensible thing is to consider post-quantum integration from the beginning when developing new standards.

1 INTRODUCTION

Cryptography is a crucial tool for the security of our digital society and is used virtually everywhere. For example, it secures our online communications, keeps the data on our devices secret even if we lose them, and protects the integrity and authenticity of digital records. The security of cryptographic solutions deployed today is threatened by the development of quantum computers. To counter this threat, the area of post-quantum cryptography was initiated. Post-quantum cryptography studies cryptosystems under the assumption that the attacker has access to a quantum computer, while the user is supposed to be a regular user of today's systems with no quantum capabilities. Several classes of problems exist that are conjectured to withstand even attacks using quantum computers. At this point the US National Institute for Standards and Technology (NIST) is running a selection process to select such systems for standardisation. Given the success of NIST standards in the area of cryptography, it is likely that the systems selected by NIST will become the international standard for large parts of the world, including the European Union. An overview of the process and the systems under consideration can be found in the recent Post-Quantum Cryptography: Current state and quantum mitigation study by ENISA[1].

In July 2022, NIST announced four candidates to be standardised, plus the four fourth round candidate Key-Establishment Mechanisms (KEMs)[2]. In addition, NIST plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022.

One might expect that with the end of this process, i.e. the publication of the standards, everything will have been solved. We simply replace the schemes that we are using today with the new systems and be done. This unfortunately is not the case at all. Many challenges need to be overcome before our data and our systems are secured against attacks using quantum computers.

One challenge is the size of the artifacts produced by post-quantum cryptography. The reason that today's cryptographic systems are so efficient is also the reason why they are vulnerable to quantum computers – these problems are highly structured. Systems secure against quantum attacks have far less structure and hence a less compact description. As a consequence, keys, ciphertexts and signatures are larger for post-quantum systems than for matching pre-quantum systems; see Chapter 2. This poses challenges to higher-level protocols. Protocol messages do not meet the size limitations of underlying protocols anymore, which at least leads to fragmentation, additional round-trips, and a more complicated state-machine if not treated carefully. As a consequence, latency and data traffic increase.

A related aspect is a decrease in the speed of some algorithms. This can significantly hurt the performance of protocols if not taken into consideration. Both aspects can be dealt with by designing new protocols that take the new performance characteristics into account. However, this comes of course with all the challenges of designing new cryptographic protocols from assessing their security to standardising them.

A last aspect that prevents the use of the new cryptographic systems as plug-in replacements is that the encryption systems have a different interface. The currently most widely used cryptographic tool to establish a shared secret is the Diffie-Hellman key exchange. This is the Swiss Army knife of cryptography. Again, what makes this system so versatile is what makes it vulnerable to quantum attacks: its structure. None of the candidates in the NIST competition matches the data flow and versatility of the Diffie-Hellman key ex-

[1] https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation, (accessed October 17, 2022).

[2] https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4 and https://csrc.nist.gov/publications/detail/nistir/8413/final, (accessed October 17, 2022).

change. Hence, protocols that currently use the Diffie-Hellman key exchange have to be changed to interface with the new cryptographic systems.

Aside from the challenges of adopting and deploying post-quantum systems, analysing their security requires a novel set of tools and techniques to take attackers equipped with quantum computers into account. This has far-reaching consequences for establishing confidence that new systems are safe to deploy and in what circumstances. New security models have to be defined, new proof techniques have to be developed, and tools such as automated theorem provers have to be changed to be applicable in this new setting. Constructions that cannot be proven secure need to be replaced.

Finally, especially in the short term, many institutions will require modes that combine conventional and post-quantum cryptographic solutions to meet compliance regulations. The risk of current post-quantum proposals being broken is high enough that such combinations are recommended even when they are not required. This of course amplifies the performance issues mentioned above, as two systems have to be used in place of one. Dedicated combined modes can potentially reduce the cost but they have to be developed and studied.

Of course, a practical overhead that applies to all developed solutions is that they have to be standardised and implemented. This causes a whole chain of standards to be updated that make use of the new cryptographic systems or the protocols developed on top of it.

This study discusses the state-of-the-art with regard to these challenges. It provides the existing answers and highlights where more work is necessary.

2 INTEGRATING POST-QUANTUM SYSTEMS INTO EXISTING PROTOCOLS

This chapter reports on work to use post-quantum systems in current protocols. It first presents data regarding size and performance of the NIST candidates, then reports on limits to sizes in Internet protocols and related experiments, and finally covers some case studies experimenting with integrating post-quantum cryptography.

For short explanations on the general functioning of these systems as well as details on the NIST round-3 candidates see the ENISA PQC study [13]. For more details see the chapters in standing document 8 (SD8) of ISO/IEC JTC 1/SC 27/WG 2 [25]. One of the authors, professor Lange, has developed an online course on post-quantum cryptography [49].

2.1 SIZE AND SPEED OF POST-QUANTUM CANDIDATES

It is often said that post-quantum systems are larger or slower than their pre-quantum counterparts. Elliptic-curve cryptography (ECC) is certainly remarkably compact, achieving 128-bit security with just 256-bit keys. This compactness along with efficient implementations is seeing ECC replace the older RSA system since the mid-2000s when cryptanalysts had become more comfortable with the security analysis, security requirements had generally moved from 80 bits to 96 or 128 bits, and cryptographers had improved the speed of implementations to show significant advantages over RSA. For comparison, RSA keys at the 128-bit security level have 3072 bits. Key sizes for systems using discrete logarithms in the multiplicative group of finite fields are similar to RSA key sizes.

For post-quantum systems there is no overall winner. For example, for post-quantum key-encapsulation mechanisms (KEMs), the smallest key sizes are again achieved by systems related to elliptic curves, namely those based on isogenies, while the shortest ciphertexts are achieved by systems based on error-correcting codes. While isogeny-based systems also have relatively small ciphertexts and thus are small overall, code-based systems have some of the largest sizes for public keys, while lattice-based systems have medium sizes for ciphertexts and keys. When it comes to speed, isogeny-based systems are the slowest while systems based on lattices or codes are much faster.

A similar picture appears for post-quantum signatures. Multivariate quadratic systems have the smallest signatures, but by far the largest public keys, while lattice-based systems have medium-sized keys and signatures. Hash-based signatures have small keys but signatures a bit bigger than lattice-based signatures. They come with fast verification and a bit slower signing speeds.[1] In general, the size increase compared to ECC and RSA is worse for signatures than for KEMs.

This means that in the world of post-quantum cryptography, protocol designers need to be aware of the possibility of different trade-offs and choose systems matching their application scenario, taking into account (1) how frequently public keys are sent relative to ciphertexts or signed messages using them and (2) how important computation speed is relative to bandwidth.

The following sections present detailed benchmarking information for post-quantum KEMs and for post-quantum signatures.

[1] An exception are stateful hash-based signatures such as LMS and XMSS. These already standardised schemes take a special role as they do not match the standard signature API because they require the secret key to be changed after every signature. However, their performance is similar to that of structured lattice-based schemes.

2.1.1 Benchmarking data for KEMs

Figure 2.1 visualises these trade-offs by plotting the space needed for a ciphertext against the space needed for the public key for all NIST Round 2 KEMs which are submitted to eBATS [11] for benchmarking. Note the code-based system Classic McEliece [2] far out on the bottom right, showing the smallest ciphertexts and the largest public keys among the systems. The smallest total size of one ciphertext and one public key, towards the bottom left in the figure, is from the isogeny-based system SIKE [43].

For size measurements the CPU of the benchmarking system does not matter, but for the subsequent graphs, showing speed measurements, it does. We have chosen to include results measured on an Intel Haswell CPU as that was designated by NIST as the benchmarking platform for their post-quantum project. For the most up-to-date measurements on the same machine see https://bench.cr.yp.to/results-kem.html#amd64-hiphop.

Figure 2.2 plots the ciphertext size against the time taken for decapsulating a KEM ciphertext. Lattice-based systems such as Threebears [37], Kyber [61], NTRU [24] and NTRU Prime [9] show the fastest decapsulation speeds (smallest x-values) but Classic McEliece features the smallest ciphertexts (smallest y-values) while being only marginally slower than the lattice-based candidates. SIKE also has smaller ciphertext sizes (y-values) than the lattice-based systems but has much slower decapsulation speeds (x-values) placing it on the right edge of the figure.

The last graph we present for KEMs plots the public-key size against the time taken to generate a public key. Figure 2.3 shows that some systems are optimised for one-time key usage with fast key-generation speed while others are more suitable for long-term or few-time usage. Note that the term 'ephemeral key' does not mean one-time key but rather expresses that it must not exist anymore after some time period has passed, hence IND-CCA2 security is relevant for these systems; see [13] for definitions.

2.1.2 Benchmarking data for signatures

Post-quantum signatures paint a similarly interesting picture when it comes to possible trade-offs. Figure 2.4 plots signature size, more precisely the space overhead for signed messages over the message size for signing a long message, against public-key size. This places systems roughly on the anti-diagonal, showing small public keys and larger signatures for hash-based signatures, such as SPHINCS+ [41], versus large public keys and small signatures for systems based on multivariate quadratics such as Rainbow [29] and GeMSS [23]. The lattice-based designs Falcon [58] and Dilithium [52] have medium-sized keys and signatures.

Signatures are typically verified multiple times, hence verification speeds matter. Figure 2.5 plots signature size, again meaning the space overhead for signed messages over the message size for signing a long message, against the time to generate a message given a signed message. Note that eBATS and NIST use the signed-message API, meaning that the verification algorithm takes a signed message as input and outputs the message or 'failure' depending on whether the signed message is valid or not, hence the verification step generates the message. Figure 2.6 plots public-key size against the time to generate a message given a signed message. These graphs show that designers will prefer different systems depending on whether public keys, i.e. certificates, are included or not. If public keys are included then systems based on lattices or hash functions have advantages over systems based on multivariate equations. The latter have very large public keys, making them attractive if public keys are rarely transmitted.

2.2 SIZE LIMITATIONS IN TYPICAL INTERNET PROTOCOLS

The Internet transmits data inside *IP packets*. Each packet is individually addressed and has a limited size, so intermediate Internet routers can quickly receive a packet, forward the packet, forget the packet, and then reuse the same packet-handling resources for the next packet.

The latest version of the Internet protocol, IPv6, requires every router to be able to handle packets as large as 1280 bytes. The previous version, IPv4, is widely deployed and in theory does not guarantee that 1280 bytes are safe, but 1280-byte packets appear to be delivered throughout the Internet today without trouble. Larger IP packets are not prohibited but require the complications of 'Path MTU discovery' or the fragility of 'frag-

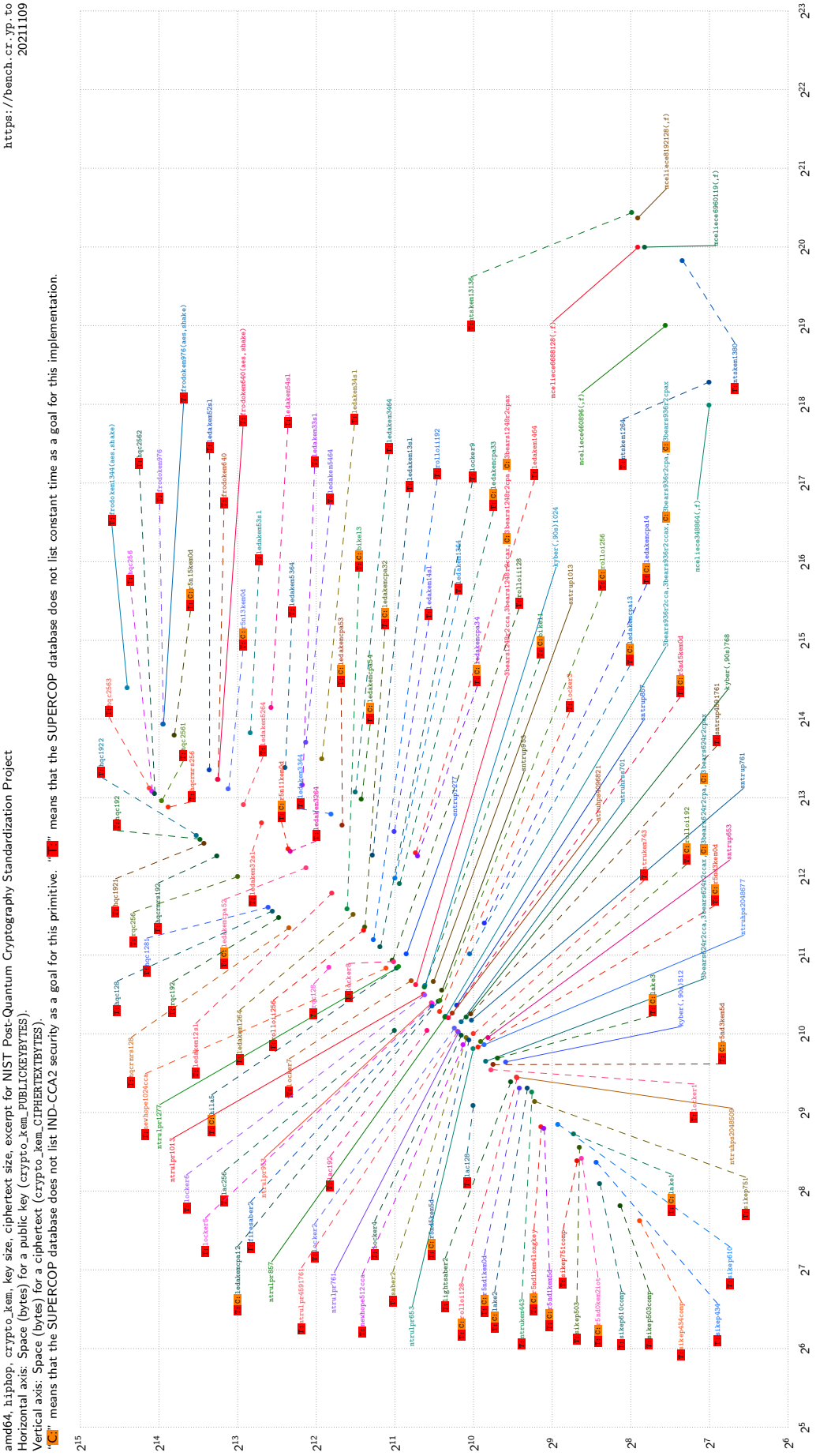


Figure 2.1: Horizontal axis: space in bytes for a KEM public key. Vertical axis: space in bytes for a KEM ciphertext. Figure taken from https://bench.cr.yp.to/graph/amd64-hiphop-kem-pkbytes,cbytes-nistpqc.pdf

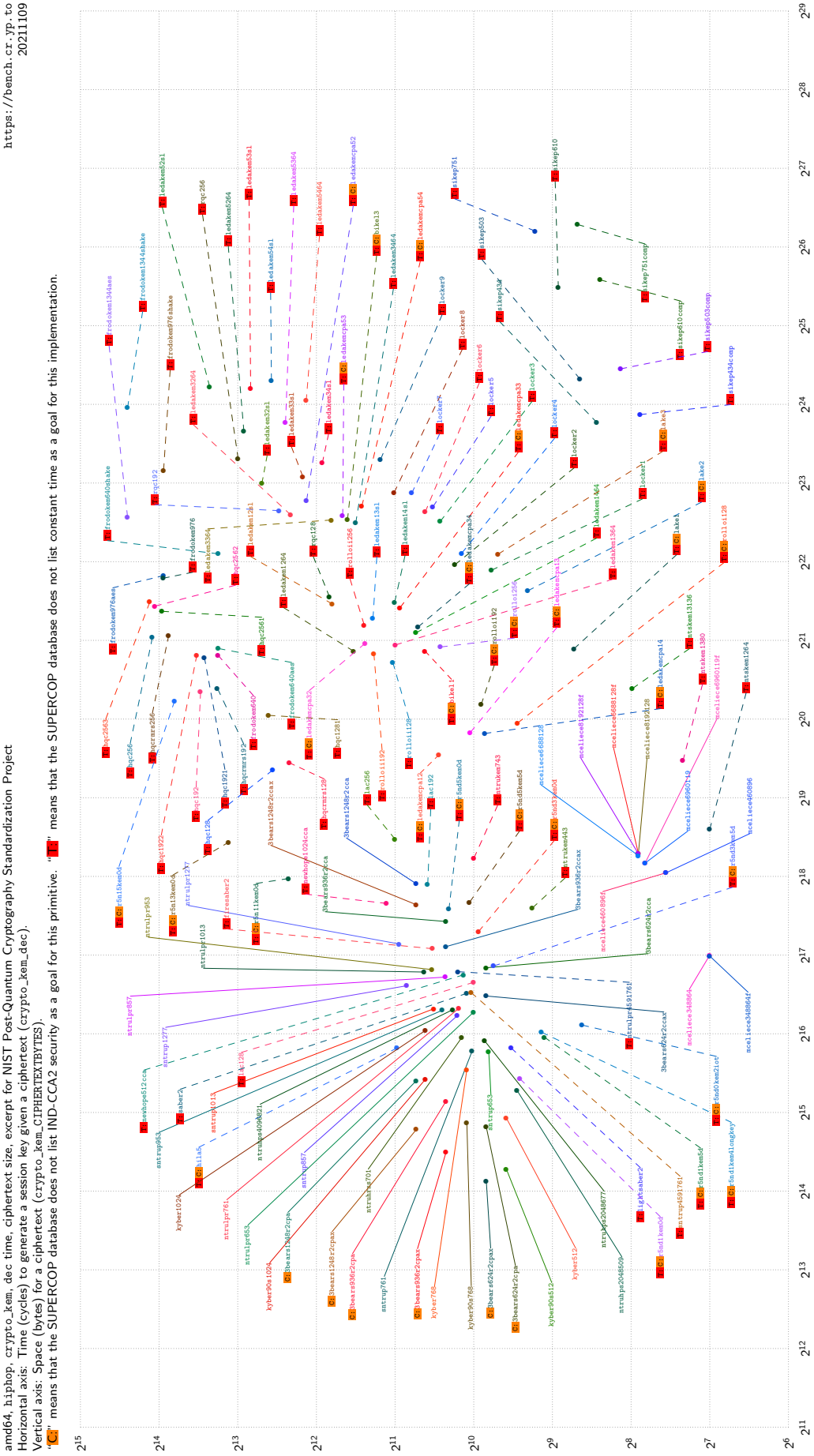


Figure 2.2: Horizontal axis: time in cycles to to generate a session key given a ciphertext. Vertical axis: space in bytes for a ciphertext. Figure taken from https://bench.cr.yp.to/graph/amd64-hiphop-kem-kcycles,cbytes-nistpqc.pdf.

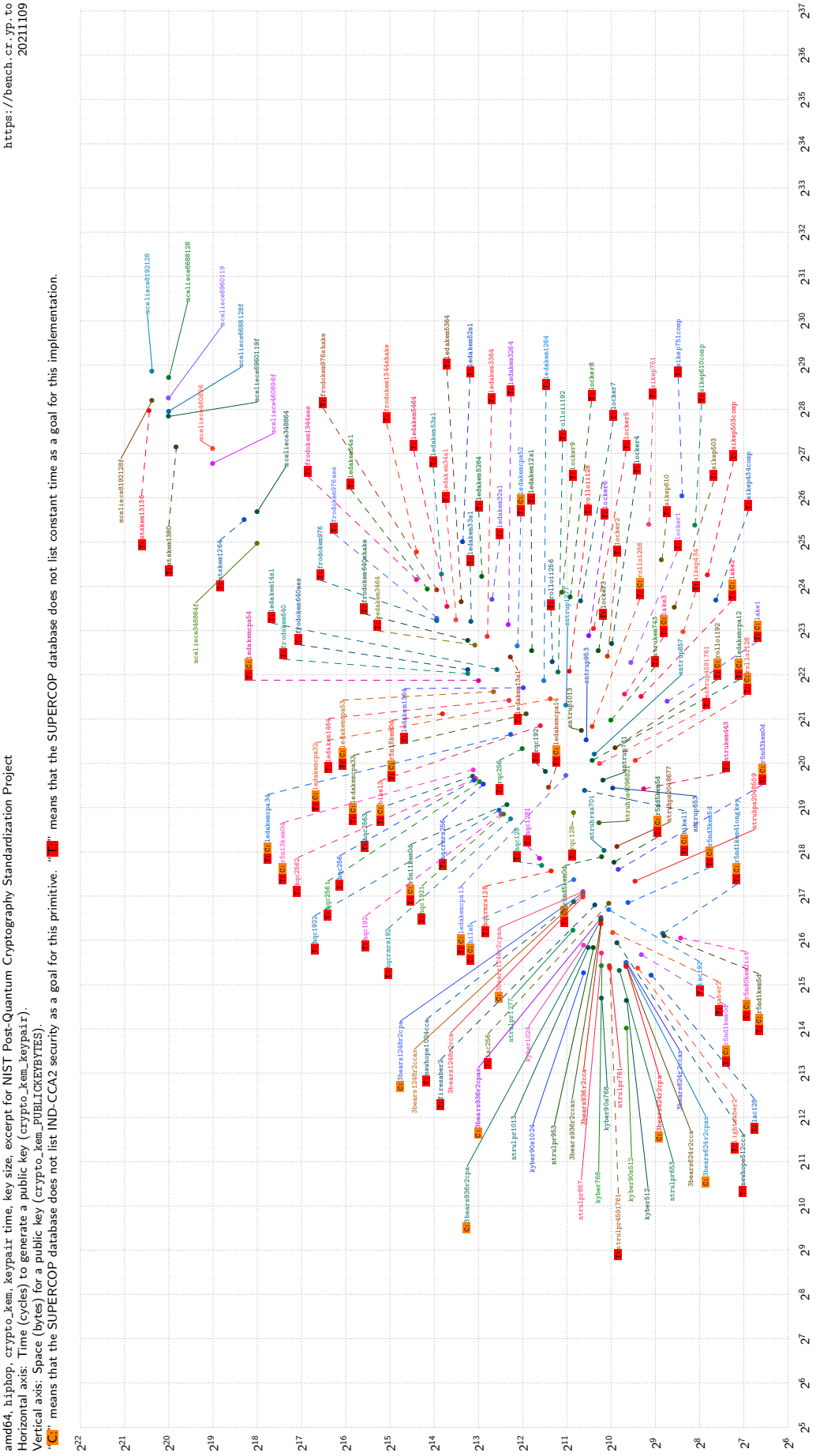


Figure 2.3: Horizontal axis: time in cycles to generate a KEM public key. Vertical axis: space in bytes for a KEM public key. Figure taken from https://bench.cr.yp.to/graph/amd64-hiphop-kem-pkcycles, pkbytes-nistpqc.pdf.

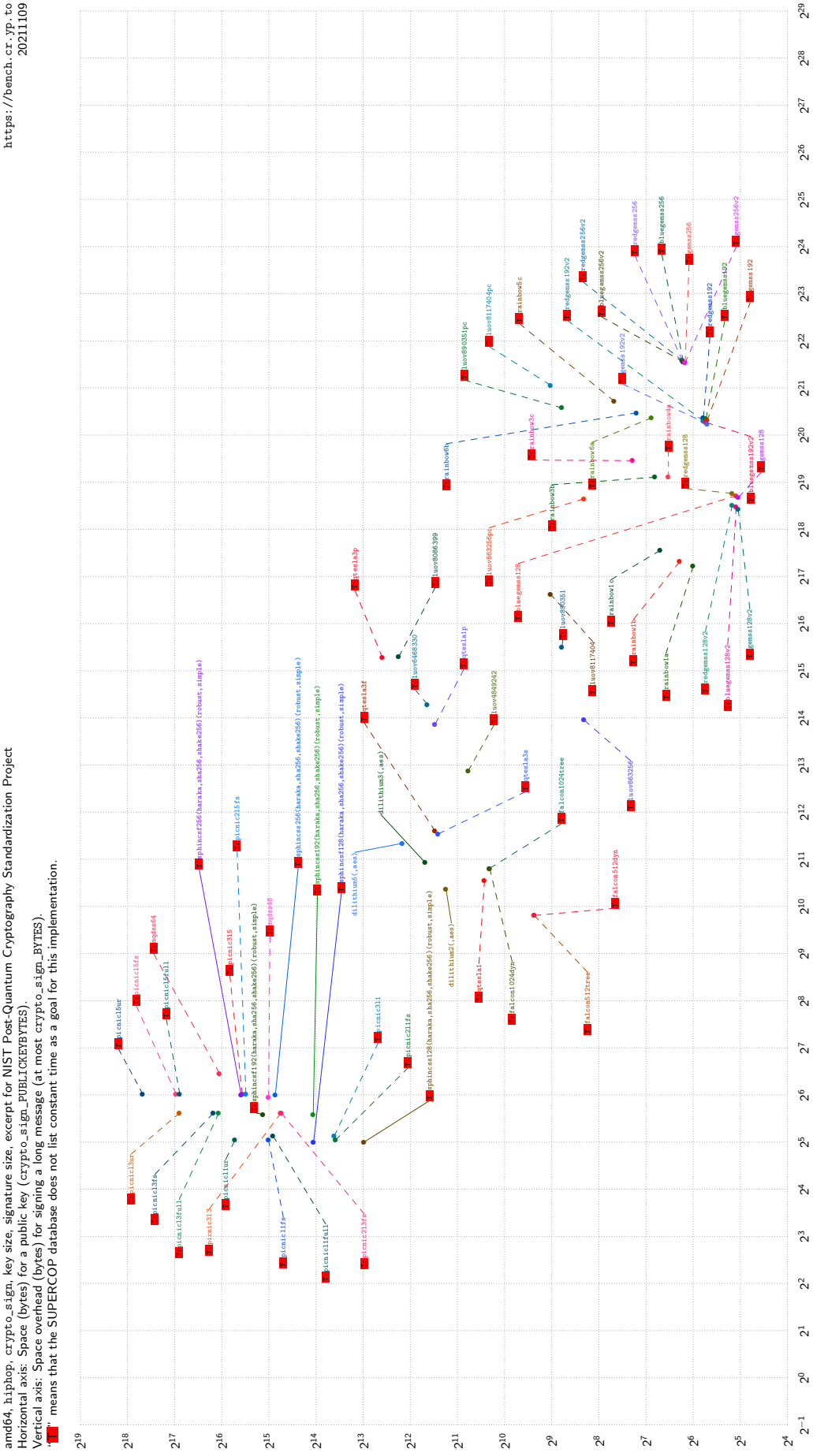


Figure 2.4: Horizontal axis: space in bytes for a public key. Vertical axis: space overhead in bytes for signing a long message. Figure taken from https://bench.cr.yp.to/graph/amd64-hiphop-sign-pkbytes, sbytes-nistpqc.pdf.

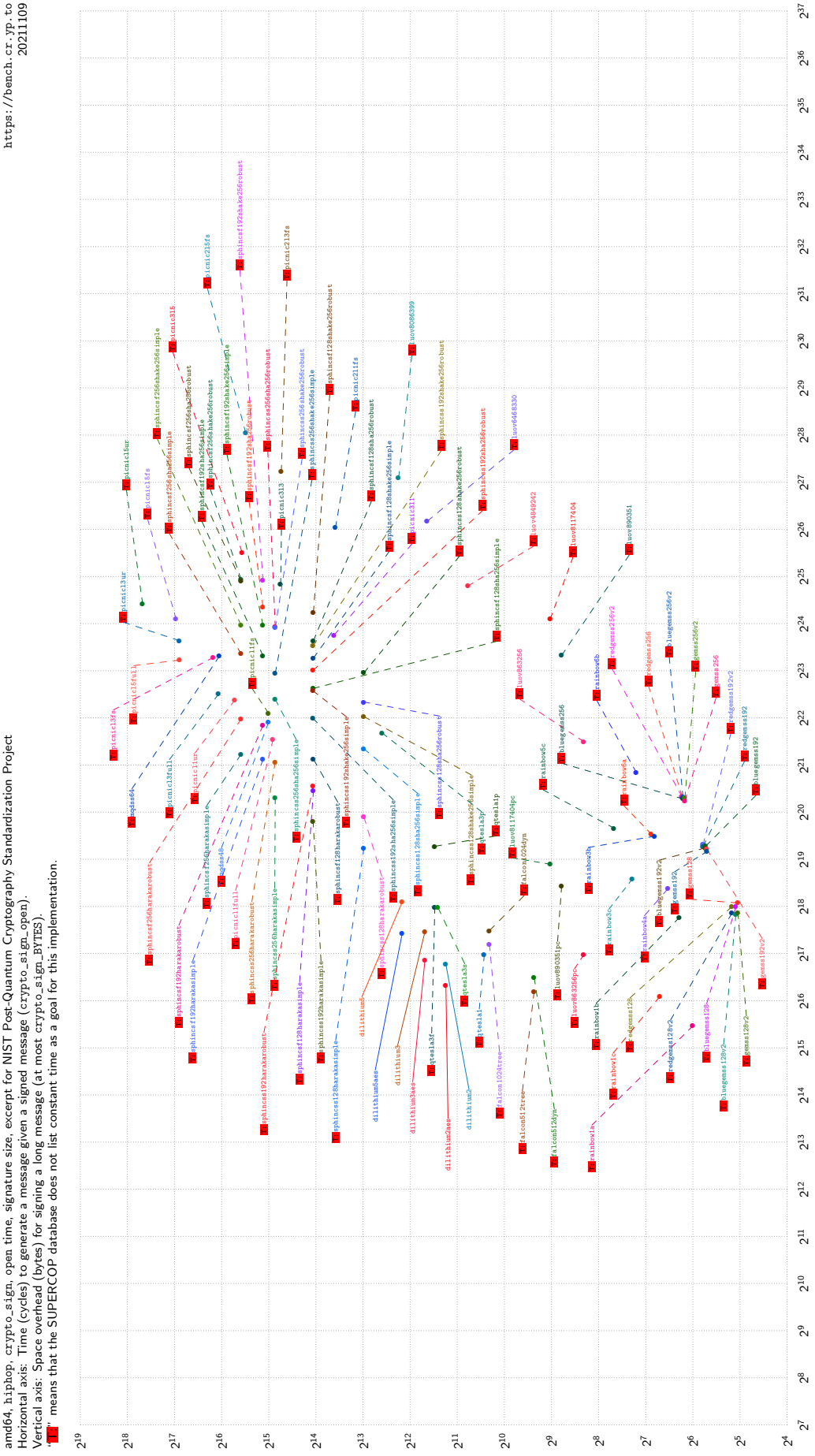


Figure 2.5: Horizontal axis: time generate a message given a signed message. Vertical axis: space overhead in bytes for signing a long message. Figure taken from https//bench.cr.yp.to/graph/amd64-hiphop-sign-mcycles,sbytes-nistpqc.pdf.

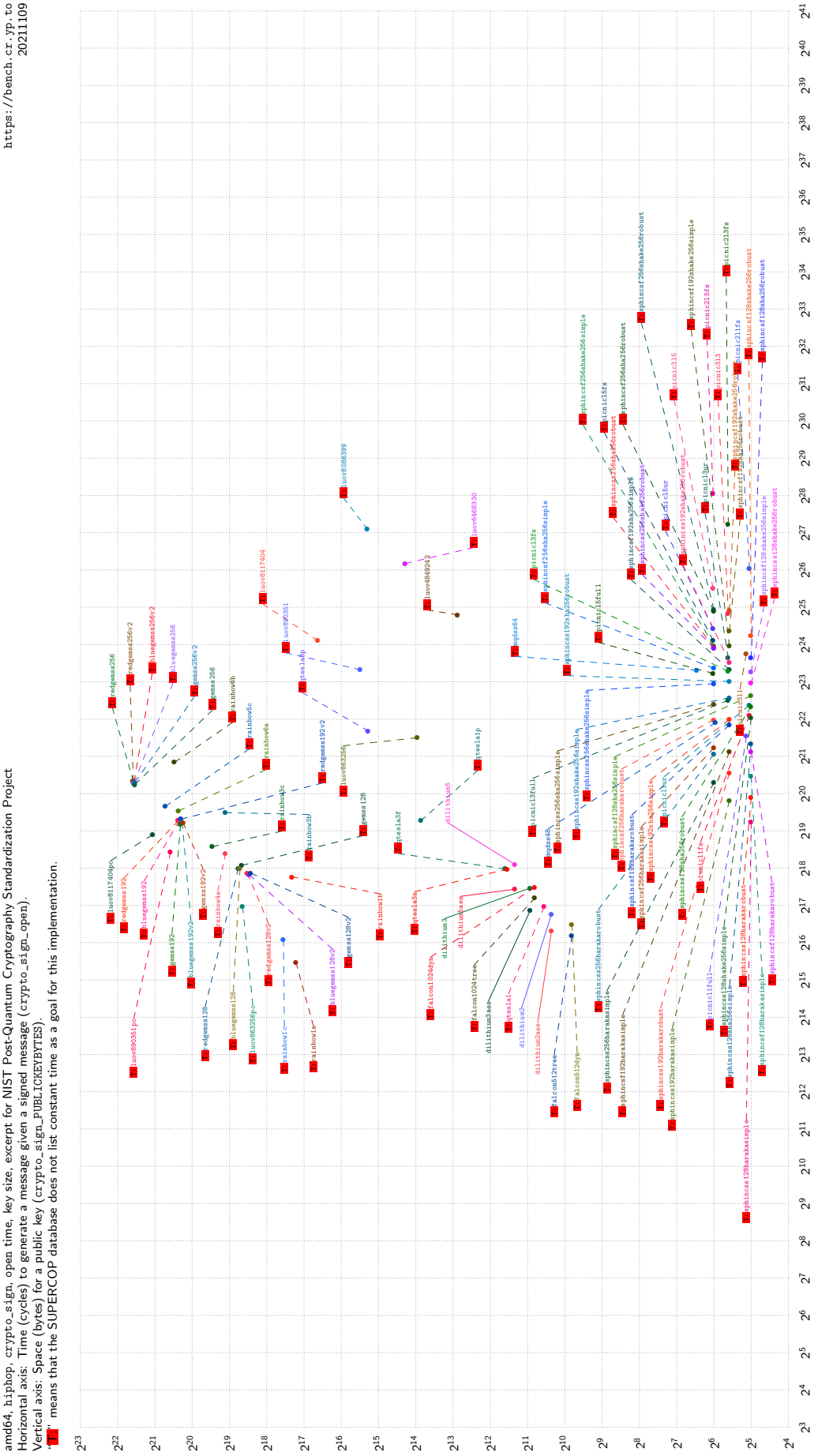


Figure 2.6: Horizontal axis: time generate a message given a signed message. Vertical axis: space in bytes for a public key. Figure taken from https://bench.cr.yp.to/graph/amd64-hiphop-sign-mcycles, pkbytes-nistpqc.pdf.

mentation'; see generally [20].

Many protocols, including HTTP and HTTPS, are built on top of TCP, which hides the packet-size limits by internally splitting the server's stream of data into sufficiently small packets to send to the client. The client reassembles the packets into the original stream of data. The client's stream of data to the server is similarly split into packets. TCP is capable of sending huge amounts of data such as long videos, much larger than the keys, ciphertexts and signatures in any of the post-quantum proposals under consideration.

However, some protocols are built directly on top of IP or on top of UDP, which is like IP in delivering only limited-size packets, and these protocols are not necessarily prepared for post-quantum sizes. Even for protocols built on top of TCP, sizes can still be a problem, because of limits in the protocols or in the software implementing the protocols. For example, Langley [50] found that the TLS software on various major web sites rejected 'ClientHello messages larger than 3970 bytes'. These ClientHello messages are the simplest place to put post-quantum keys in TLS 1.3. Given this limitation, Google and Cloudflare discarded code-based systems and systems based on unstructured lattices from consideration for their joint post-quantum experiment CECPQ2 [48]. Cloudflare experimented with SIKE and NTRU-HRSS while Google also rejected SIKE, reportedly out of concerns over performance and denial-of-service attack potential; see, e.g. [47].

2.3 PROTOCOLS ADAPTED TO POST-QUANTUM CRYPTOGRAPHY AND PERFORMANCE STUDIES

The works considered in this section fall roughly into three categories:

1. Complete designs of protocols that offer security against quantum attacks and where the designers have made one choice of algorithm, which is motivated in the scientific paper.
2. Comparison studies analysing the suitability of different post-quantum systems for a protocol. These papers typically implement and analyse all potentially suitable systems and show the impact those choices have. They might give recommendations but typically include tables of results highlighting good choices for certain use cases.
3. Large Internet companies supporting post-quantum cryptography in prototype and deployments.

We will cover a selection of all categories.

2.3.1 Post-quantum WireGuard

WireGuard [30] is a relatively new VPN protocol that breaks with the tradition of designing these protocols based on IPsec and instead builds them with modern systems and single choices, avoiding negotiation between participating nodes. While WireGuard in principle is designed to work between nodes that are equal, a typical deployment uses clients and servers and in general the protocol is asymmetric in that one party, the server, is known by a long-term key while the client can be registered with the server using a long-term key. These long-term keys are exchanged during a registration phase and are never sent during a protocol run. Instead, each party makes an ephemeral key for each connection and uses a combination of the resulting shared keys (ephemeral and long-term) for computing the session key which is then used to encrypt the content of the communication.

The post-quantum WireGuard design [42] uses the Classic McEliece system for the long-term keys and Saber for ephemeral keys. Their design benefits from the short ciphertexts provided by Classic McEliece and the fast key-generation speeds and compact key and ciphertext size of Saber, without encountering the cost for sending the large Classic McEliece keys. This allows the protocol to keep UDP packet sizes within the 1280-byte limit.

The publication shows a full implementation as well as a security proof for the new protocol.

2.3.2 Web browsing secured with NTRU Prime

OpenSSLNTRU [10] is similar to CECPQ2 in that it integrates post-quantum key exchange into TLS 1.3 using a new one-time KEM key for each TLS session. The post-quantum details are different, achieving higher security with higher performance. Specifically, with

the latest software, CECPQ2's `ntruhrss701` takes 359076 cycles on an Intel Haswell core for key generation plus encapsulation plus decapsulation, the total work of the client and the server; the key and ciphertext together use 2276 bytes. With the software from [10], OpenSSLNTRU's `sntrup761` takes 259472 cycles on an Intel Haswell core for key generation plus encapsulation plus decapsulation; the key and ciphertext together use 2197 bytes.

Furthermore, OpenSSH has supported Streamlined NTRU Prime since version 8.0 in 2019 and has it enabled on servers by default since version 9.0[2] that appeared in 2022. This means that clients will be free to select it without any action by the server administrator.

2.3.3 Use of post-quantum cryptography for VPNs

In 2018, ETSI published [59] an analysis and comparison of the use of post-quantum systems in VPNs.

The document gives detailed descriptions of the Internet Key Exchange (IKE) protocol, the typical basis for VPNs built on IPsec, Transport Layer Security (TLS), used for transportation, the Media Access Control Security (MACsec) protocol, sometimes used for securing communications for the last mile between router and client, and finally the Secure Shell (SSH) protocol. For each of these protocols, requirements for drop-in replacements as well as for combined (hybrid) systems are analysed and recommendations are given. At 35 pages that study is too detailed to summarise here and the reader is invited to consult that source directly which is freely available.

2.3.4 Studies analysing post-quantum systems for TLS

Several publications have tackled the TLS protocol. The Open Quantum Safe library (liboqs) [66] has made prototyping very easy by providing systems fitted into a fork of OpenSSL. The benchmarking of different systems for TLS is covered in [57] while combinations of different systems (hybrids) for key exchange is covered in [26] (see also Chapter 4). The latest TLS version is 1.3; [63] investigates post-quantum systems for authentication. Cloudflare very recently released a study [71] on the impact of signature and certificate sizes of post-quantum systems on TLS. This study also addressed problems regarding authentication.

2.3.5 Signature verification on very small devices

Some processors are so small that they cannot hold the full public key or signature for some of the post-quantum systems. Signature verification in feature activation[3] in cars is such a scenario and is the topic of [35]. The paper analyses the impact on performance when the RAM size is restricted to 8kB, meaning that signatures and/or keys need to be streamed into the device. Should the public key need to be streamed in, the device needs to have a hash of the public key in secure memory in order to compare the streamed-in key against this hash. For the large-key systems Rainbow and GeMSS this caused a serious impact on performance due to the extra hashing. SPHINCS+ naturally has a very small public key and the implementation ran with only a few adjustments on the ARM Cortex-M3 development board. For Dilithium the fastest implementation required too much code size, while key size and signature size posed no problems.

2.3.6 Signature verification and generation in a high-load scenario

Car-to-car communication needs to be authenticated to prevent rogue stations from creating accidents by causing cars break suddenly to avoid colliding with non-existing obstacles. On a busy street, cars receive many signatures per second and need to check the validity and react on the contents without losing time. Cars also continuously send messages for which they need to generate signatures.

A recent study [17], presented at NIST's round 3 workshop, showed that the differences

[2] https://www.openssh.com/txt/release-9.0, (accessed October 17, 2022).
[3] Feature activation is the remote activation of features that are already implemented in the software and hardware of the car. For example, an additional – pre-installed but deactivated – infotainment package. A short activation code can be protected with a signature to prevent unauthorised activation of the feature.

between Dilithium and Falcon, which seem rather small in the benchmarks presented in Section 2.1, have a significant impact in aggregation and that the latency of signature transmission, i.e. the size overhead, makes a significant difference in car-to-car communication.

2.3.7 Large companies supporting post-quantum Internet solutions

CISCO has issued guidance on how to configure MACsec for post-quantum[4] for their routers. See also [45] for the corresponding scientific paper.

Amazon Web services advertises support for post-quantum TLS for key-management services [38]. Similarly, Microsoft now supports post-quantum cryptography for VPN connections [31].

2.4 SUMMARY

Post-quantum systems have different trade-offs in size and speed than their pre-quantum counterparts. Protocol designers need to understand the space of options presented in Section 2.1 to make optimal choices for each use case. This chapter presents the impact on performance of these choices. Chapter 5 covers the implications for security proofs.

Six example studies are presented to show the options for adding post-quantum protection to existing protocols. Making these choices, in particular if bandwidth is an issue, is still a topic of academic papers and some expertise is needed. The graphs and summaries in Section 2.1 can provide guidance.

[4] https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/configuring-post-quantum-macsec-in-cisco-switches.pdf, (accessed October 17, 2022).

3 NEW PROTOCOLS DESIGNED AROUND POST-QUANTUM SYSTEMS

A different approach to dealing with the difference in interfaces is to design new protocols which are developed around post-quantum systems, taking their specifications into account. This is likely the option that leads to the most efficient protocols but it requires a lot of work. The number of published proposals is still somewhat limited and more work in this direction is required.

3.1 USING KEMS IN PLACE OF SIGNATURES

Already in a pre-quantum world, Diffie-Hellman and KEMs are more efficient than signatures, making it attractive to design protocols using these primitives for authenticity and secrecy rather than using them only for secrecy and using signatures for authenticity. In the Diffie-Hellman context this can be traced back to at least 2006 when Bernstein presented very efficient DH speeds and proposed[1] to use DH in place of signatures.

In the post-quantum context, and in particular for lattices, signatures are both larger and less efficient to compute than KEMs, which prompted [28] to investigate the security of combining two KEMs, one with ephemeral keys for forward secrecy and one with long-term keys for authentication. The paper lays out the combinations and gives a proof in the random oracle model. This approach is also taken in PQWireGuard described above.

For TLS applications, where typically one side is authenticated, [62] describes a combination of two post-quantum KEMs and reports implementation results.

3.2 NEW DESIGNS TO DEAL WITH KEY SIZE

The public keys in the code-based system Classic McEliece are 1 MB and larger for the 5th category. This had led to recommendations to use the system only for long-term keys, as using them ephemerally would cause a high level of fragmentation. The McTiny protocol [12] deals with the scenario in which a client transmits an ephemeral key to the server while the server has a long-term Classic McEliece key used for authentication and to protect the integrity and secrecy of the key shares and partial encryptions. The protocol uses the intrinsic properties of code-based systems to handle encryptions using parts of the key. The paper considers the denial-of-service attack surface posed to servers accepting large keys and presents a design in which servers do not allocate any per-client memory beyond the size of an incoming internet packet and fully avoid memory-flooding DoS. The protocol is fully implemented and tested for latency and deploys congestion control.

3.3 NEW DESIGNS ADDRESSING DIFFERENT LAYERS

Besides interface and speed issues, a concern with replacing pre-quantum systems with post-quantum systems is that it is a slow process which requires years of discussions in the standardisation bodies that control the systems. Even if NIST's choices will be adopted without changes and those bodies start working even before the full specifications of the new standards are announced, several more years of data will be protected purely with pre-quantum systems.

An avenue pursued in parallel is to leverage the layer structure of the Internet to add post-quantum protection for all connections between nodes that offer support. PQConnect [8, 51] builds secure tunnels between a user's browser and supporting websites.

[1] Daniel J. Bernstein, "Elliptic vs. hyperelliptic, part 1", pages 4-6, https://cr.yp.to/talks.html#2006.09.20, (accessed October 17, 2022).

Each connection is secured with two long-term identity keys, one using the code-based Classic McEliece system, the other using pre-quantum elliptic-curve cryptography, and two ephemeral keys, combining elliptic curves with structured lattices. The combination is done in such a way that the (potentially) weaker systems are wrapped inside the stronger ones, forcing attackers to break the stronger systems to gain access to those ciphertexts and keys. The existing prototype uses a SOCKS proxy but the finished project should operate in kernel space the same way that a VPN does and protect the full communication from DNS lookups to data transfer.

3.4 SUMMARY

To tackle the challenge of transitioning to post-quantum cryptography some new protocols have chosen to break out from replacing (or augmenting; see Chapter 4) pre-quantum systems with post-quantum systems of the same type. These protocols are instead designed around post-quantum systems. Examples covered are replacing signatures with KEMs, putting key-sizes as guiding factors, and offering post-quantum protection at a different layer of the Internet. The latter has the additional benefit of promoting a fast rollout, not hampered by slow standardisation bodies.

So far only a few studies have departed from the standard approach of replacing pre-quantum with post-quantum or strapping on post-quantum systems, but existing works are promising and more research and deployment work is needed in this area.

4 DOUBLE ENCRYPTION AND DOUBLE SIGNATURES

Almost all of the post-quantum cryptosystems submitted to NIST have lower security against the best attacks known today than against the best attacks that were known in 2017. In many cases the loss of security was severe enough that the submissions are categorised as broken. There is no guarantee that the surviving post-quantum cryptosystems are secure. Cryptanalysts could have missed an important attack, perhaps even an attack that runs quickly on today's computers. Furthermore, many serious bugs have already been discovered in the complicated new ecosystem of post-quantum cryptographic software and there is a clear risk of further bugs. State-of-the-art tools can guarantee that cryptographic software does not have buffer overflows, but formal verification of full functional correctness remains challenging.

Consequently, there is a risk that switching from pre-quantum elliptic-curve cryptography to a post-quantum cryptosystem will damage security, not just failing to protect against quantum computers but also losing protection against today's computers.

To address this risk, you should deploy post-quantum cryptography today as an *extra* layer together with pre-quantum cryptography, rather than deploying it as a *replacement* for pre-quantum cryptography. Sign with a pre-quantum cryptosystem and with a post-quantum cryptosystem, making sure that the verifier checks both signatures. Encrypt as usual with pre-quantum cryptography, and then encrypt the result with post-quantum cryptography, so that decryption requires both secret keys.

For example, Google's 'CECPQ1 (combined elliptic curve + post-quantum)' key-exchange mechanism [21] combines a well-known pre-quantum elliptic-curve cryptosystem, X25519, with a post-quantum lattice-based cryptosystem, NewHope-1024:

> The post-quantum algorithm might turn out to be breakable even with today's computers, in which case the elliptic-curve algorithm will still provide the best security that today's technology can offer.

CECPQ2a combines X25519 with another post-quantum lattice-based cryptosystem, NTRU-HRSS-701. CECPQ2b combines X25519 with a post-quantum isogeny-based cryptosystem, SIKE-p434. In each case, even if the post-quantum cryptosystem completely fails, the user's data is protected by X25519. Large quantum computers will eventually break X25519, but this failure is farther in the future than the immediate disaster that would occur if X25519 were omitted.

4.1 REVIEWING DOUBLE CRYPTOSYSTEMS

Double encryption and double signing sound straightforward, but one must be careful with the details. For example, it is dangerous to reuse keys across multiple systems. It is dangerous to reuse any randomness used for encryption, signing, etc. It is dangerous to assume that the presence of one component will compensate for weaknesses in another component: 1993 Maurer–Massey [53, Section 1] gave an example where inserting one weak encryption layer exposes a sample application to the weaknesses of a second encryption layer, where the second encryption layer by itself would not have been exploitable for the same application. Each component should be designed to be secure by itself.

A well-designed double cryptosystem makes it easy for security auditors to see that the cryptosystem is strong if *at least* one of the component cryptosystems is strong. This means, in particular, that adding post-quantum cryptography does not damage the pre-quantum security provided today by elliptic-curve cryptography. This also provides a

straightforward way to integrate post-quantum cryptography while remaining in compliance with existing regulations and policies that require elliptic-curve cryptography. Double cryptosystems thus help fast deployment of post-quantum cryptography.

Names in the literature for the same concept include 'double encryption' (and, more generally, 'multiple encryption'), 'combiners', and 'hybrid cryptosystems'. Be aware that the name 'hybrid cryptosystem' is also used for various constructions requiring *all* of the component cryptosystems to be strong: the standard example is encrypting data using a cipher key that was exchanged with a public-key cryptosystem.

Security analysis of the `CECPQ1_RSA_WITH_AES_256_GCM_SHA384` TLS cipher suite starts from the assumption that CECPQ1 encryption *and* RSA signatures *and* the AES-256-GCM authenticated cipher *and* SHA-384 are secure; security analysis specifically of CECPQ1 starts from the assumption that X25519 *or* NewHope is secure.

ETSI [60] has specified mechanisms to combine pre-quantum encryption with post-quantum encryption. Another specification [65] is under development within IETF. NIST's key-derivation standard [6, Section 2, second paragraph] permits a standard shared secret (which for NIST currently means a pre-quantum shared secret) to be concatenated with an 'auxiliary shared secret' (which NIST has not specified how to obtain, but would presumably be a post-quantum shared secret), with the concatenation hashed in specified ways to obtain a key.

4.2 DETAILS OF DOUBLE ENCRYPTION

Recall that user data is normally encrypted and authenticated with an authenticated cipher such as AES-256-GCM or ChaCha20-Poly1305, after an elliptic-curve key-exchange mechanism is used to establish the 256-bit session key used by this authenticated cipher.

These authenticated ciphers are not threatened by quantum computers. Shor's algorithm does not apply to them, and the key sizes are large enough to leave a comfortable security margin even considering Grover's algorithm. See, e.g. [4]. The possibility of double encryption using, e.g. AES-256-GCM together with ChaCha20-Poly1305 is outside the scope of this document.

What *is* threatened by quantum computers is the elliptic-curve key-exchange mechanism. For example, consider the ECDH KEM: there is a standard elliptic-curve point G; Alice generates a secret key a and sends a public key $A = aG$; Bob generates a secret b and sends a ciphertext $B = bG$; Alice and Bob now compute the same point $a(bG) = b(aG)$, and hash this point to obtain a session key k. Assume that all of the objects A, B, k are encoded as fixed-length strings.

Now consider a post-quantum KEM where Alice generates a fixed-length public key A'; Bob generates a fixed-length ciphertext B'; Alice and Bob compute a fixed-length session key k'. You should build a double KEM as follows, with keys and other random objects generated independently for the ECDH KEM and the post-quantum KEM:

- Alice's public key in the double KEM is the concatenation (A, A');
- Bob's ciphertext in the double KEM is the concatenation (B, B');
- The session key encapsulated under public key (B, B') is a standard hash of the concatenation (k, k', B, B').

These concatenations are unambiguous since A, B, k, k' have fixed length.

This description implicitly assumed that the two input KEMs (the ECDH KEM and the post-quantum KEM) are 'quiet', always returning session keys, never rejecting ciphertexts. To allow non-quiet KEMs, define the double KEM to reject (B, B') if the first input KEM rejects B or the second input KEM rejects B'.

The above construction is an example of the 'first proposal' in [34, Section 1.1]. See [34] and [14] for further constructions; these papers identify the necessary security properties achieved by the hashing of (k, k', B, B'), and use this to replace the hashing with something faster. See also [40] for an even faster construction that merges this hashing with the two hashing layers inside the two KEMs, although this no longer treats the KEMs as black boxes. Finally, see [65] for a variant that omits this hashing in the context of TLS (which has a subsequent hashing layer) and for an analysis of options for negotiating key-

exchange choices.

4.3 DETAILS OF DOUBLE SIGNING

There are two common interfaces for signature systems:

- A 'detached signature' is separate from the message. Verification takes a message and a detached signature, and returns acceptance or rejection.
- A 'signed message' (also called a 'signature with message recovery') includes the message. Verification takes a signed message and returns a message or rejection.

The signed-message interface avoids the risk of forgetting to verify a signature. Sometimes signed messages are designed to take less space than a message plus a separate signature. One can generically convert a signed-message interface into a detached-signature interface by signing a hash of the message, although this loses the benefits of a signed-message interface.

With a detached-signature interface, combining a pre-quantum signature system P with a post-quantum signature system Q is a simple matter of concatenating the two signatures, assuming the signatures have fixed length. The double-signature verifier accepts the double signature exactly when the P verifier accepts the P signature and the Q verifier accepts the Q signature.

Beware that some proposed post-quantum signature systems have variable-length signatures. Concatenation is still safe as long as the first system has fixed-length signatures. An alternative is to use an unambiguous encoding of variable-length strings, as in the 'composite' signatures in [56]. Beware that [56] points to patent applications regarding multiple signatures; for prior art see, e.g. [16].

With a signed-message interface, combining a pre-quantum signature system P with a post-quantum signature system Q is a simple matter of signing first with P and then signing the result with Q. The double-signature verifier applies the Q verifier followed by the P verifier.

An alternative is to sign first with Q and then with P. Signing first with P has the advantage that the auditor can entirely ignore Q in checking that any message produced as output was verified by P. If Q is first, then the P auditor also has to check a minimal correctness property of Q, namely that if a message is signed by Q and then given to the Q verifier without modification then the output of verification cannot be any other message.

There are more complicated double-signing proposals that modify how signatures are used in applications: for example, modifying TLS to check a certificate using a P signature and to check a separate certificate using a Q signature. It is simpler to build an application-independent double-signature system and upgrade applications to use that system.

4.4 PERFORMANCE

As explained earlier in this document, post-quantum cryptosystems send more data than elliptic-curve cryptosystems. For example, a NewHope-1024 ciphertext is 2208 bytes, an NTRU-HRSS-701 ciphertext is 1138 bytes, a compressed SIKE-p434 ciphertext is 236 bytes, and an X25519 ciphertext is just 32 bytes. Applications that can afford the data sent by post-quantum cryptography are likely to be able to afford an extra 32 bytes for double encryption with elliptic-curve cryptography and post-quantum cryptography. Similar comments apply to double signing.

However, hybrids can be a larger performance problem in other cost metrics. For example, there has been some investigation of compact implementations of post-quantum cryptography for small devices (see, for example, [72]), and there are various ideas on how to save space by merging implementations of post-quantum cryptography with implementations of elliptic-curve cryptography (see, for example, [5]). The details and costs require further investigation.

4.5 LONG-TERM PERSPECTIVE

One hopes that security analysis of post-quantum cryptosystems will eventually stabilise, preferably without many more broken cryptosystems. Furthermore, the fact that elliptic-

curve cryptography has security value today does not mean that it will have security value forever. The first public use of a quantum computer to compute a 256-bit elliptic-curve discrete logarithm will naturally raise questions regarding the continued value of deploying elliptic-curve cryptography, even if the break is very expensive. Assuming that there is public consensus someday that elliptic-curve cryptography is obsolete, it will then be reasonable to consider removing it from protocols such as TLS, with the goal of eventually allowing simpler TLS implementations.

4.6 SUMMARY

Start with a system that encrypts and/or signs using elliptic-curve cryptography. Add an *extra* layer that *also* encrypts and/or signs using post-quantum cryptography. This is 'double encryption' and/or 'double signing'. If this is done properly, then any attack will require breaking the elliptic-curve system *and* breaking the post-quantum system, so upgrading to post-quantum cryptography will not damage the [cryptographic] security of the existing system, even if there are vulnerabilities in the post-quantum cryptosystem or post-quantum software[1]. State-of-the-art tools can guarantee that cryptographic software does not have buffer overflows, but formal verification of full functional correctness remains challenging. In all cases, the details must be handled carefully for security. Usually there is no real performance reason to remove elliptic-curve cryptography.

[1] This is not to say that double encryption/signature is a catch-all solution to badly written or malicious software. If, for example, due to a supply-chain attack, the new system uses a compromised software library with malicious code enabling remote code execution security overall will be compromised, despite the soundness of the cryptography in use.

5 SECURITY PROOFS IN THE PRESENCE OF QUANTUM ATTACKERS

The common expectation is that quantum computers only threaten the security of public key cryptography (PKC), more specifically of the basic PKC schemes, such as encryption, KEM, and signature schemes. However, this is mostly based on the already existing knowledge of attacks that threaten these schemes while attacks against other schemes and protocols are not known for now. A common approach in modern cryptography is to reduce the attack surface against the mathematical security of a protocol or system to break the security of its basic building blocks via security proofs. Building blocks in this case can either be mathematical problems such as the RSA problem or the LWE problem, or these can be higher level building blocks like KEMs, signature schemes, or hash functions for which we already established security by another proof or cryptanalysis[1].

Clearly, if new protocols are constructed these require new proofs. But even existing proofs for well-known protocols have to be revisited. The reason is that when we aim for post-quantum security, i.e. security against adversaries making use of a quantum computer, we have to model our adversaries also as quantum algorithms. This requires changing models and deciding about the specific abilities of quantum adversaries. Afterwards, proofs have to be vetted again in the new setting. This process has been started and is progressing well for basic building blocks, especially those considered in the NIST competition. However, in many other areas, especially in the analysis of protocols, the process has not even begun. In this section we discuss known results and afterwards summarise open questions for all dimensions of this problem. For a more detailed overview of recent topics in this area, see the talks of the Quiques workshop[2], co-organised by one of the authors, professor Hülsing and professor Majenz.

5.1 QUANTUM ACCESS

Security games often model the attacker as having access to oracles. For example, in the standard definition of security for signatures, the adversary is given a public key and access to a signing oracle that allows it to learn signatures on messages of its choice under the corresponding secret key.

The first question when revisiting existing security models is whether an adversary should be given quantum access to the oracles provided and, if so, to which ones. In this context, quantum access to an oracle for a function f refers to the ability to make a query with a superposition of inputs for f and receive the corresponding superposition of outputs of f. More formally, a quantum superposition oracle for a function $f : X \to Y$ is defined as the unitary transform

$$U_f : \sum_{x \in X, y \in Y} \alpha_{x,y} |x, y\rangle \to \sum_{x \in X, y \in Y} \alpha_{x,y} |x, y \oplus f(x)\rangle ,$$

where $\oplus$ refers to bitwise xor. It should be noted that given a classical description of f this quantum oracle can be implemented using standard techniques.

[1] It should be noted that we commonly aim for security against computationally bounded adversaries. That is, we require that it is hard to solve a problem or break a cryptographic system in reasonable time. In this setting, eventually the security of some basic building block has to be established by cryptanalysis. Security proofs can help by focusing the cryptanalytic efforts on a few selected problems.

[2] Videos and slides are available at https://quiques.huelsing.net/, (accessed October 17, 2022).

Standard model vs idealised models. In this context, an important distinction has to be made. This is between the standard model and idealised models such as the random oracle or the ideal cipher model. In the standard model, the adversary is only given oracle access to functionalities that it cannot compute itself, usually because they use a secret key that is not available to the adversary as in the case of the signing oracle. In idealised models, some cryptographic building blocks are replaced with ideal versions, e.g. hash functions with random functions (random oracle model) or block ciphers with a collection of random permutations (ideal cipher model). These ideal building blocks do not allow for efficient descriptions. Hence they are introduced into the model as oracles to which all parties have access.

Three different classes of models. For decisions on which oracles should be quantum-accessible, the following classification, introduced in [32] (with prefix 'QS') and now widely used (with prefix 'Q'), distinguishes the most relevant models:

- In Q0 models, access to all oracles is classical.
- In Q1 models, quantum access is given to oracles that simulate functions from an ideal model that are not secretly keyed. Oracles implementing secretly keyed functions only allow for classical access.
- In Q2 models, quantum access is given to all oracles, including those that implement secretly keyed functions.

The Q0 models cover the setting of a world where no quantum computers exist.

When we want to consider the setting in which an adversary has access to a quantum computer we have to consider Q1 models. The reason is that in idealised models, we are modelling functions that are publicly known as oracles. In the real world, these functions could be implemented as quantum algorithms by an adversary and then run on a quantum computer. Therefore, these functions are computable in superposition by the adversary in the real world. Q1 models reflect this by providing quantum access to ideal functionalities that are not secretly keyed. While it was questioned if this makes a relevant difference, this question has been recently settled in the affirmative by [73] giving a separation between the classical random oracle model (ROM) and the quantum-accessible random oracle model (QROM).

Q2 models go beyond this. In general, Q2 models would apply in a world where honest users work on quantum computers, connected via a quantum network with other users and the adversary. In this setting, it might happen that an adversary gets quantum access to secretly-keyed functionalities. Another case where one would have to apply the Q2 model is the exceptional case where an adversary is actually given quantum access to such secretly keyed functionalities although honest users still use classical computers. This is, for example, the case in a setup where the adversary is given an obfuscated circuit of a secretly-keyed block cipher. In this case, the adversary could translate the circuit into a quantum circuit and obtain quantum access.

In summary, when one aims for protecting the current infrastructure against an adversary that may have access to a quantum computer, Q1 models are generally the right choice. However, Q2 models can be relevant in the far future or for analyses of some advanced protocols.

5.2 NEW MODELS

After deciding which oracles have to allow for quantum access the quantum counterpart of the old (classical) security model can be defined by changing the following two of its aspects: Firstly, the adversary is assumed to be a quantum algorithm. Secondly, the adversary is given quantum access to the selected oracles. This gives a valid model. However, it does not guarantee that the model is useful, as security in this model may be unachievable. This problem occurred often in Q2 models, necessitating the development of new security models (e.g. see [19, 33, 1]).

In this report, we are concerned primarily with Q1 models. For Q1 models, the standard model only changed by allowing the adversary to be a quantum algorithm. In this setting, post-quantum security is achievable for most tasks if we assume that mathematical problems that are hard for quantum computers to solve do exist. However, even in this case it turns out that models have to be carefully analysed. Some models may not reflect the

intended behaviour anymore. For an example, see [68].

When it comes to idealised models, the most widely used model, the random oracle model (ROM), was already analysed in 2011 and the quantum-accessible random oracle model (QROM) was introduced as its Q1 counterpart [18]. So far, most security notions seem to be also achievable in the QROM. Its sibling, the quantum ideal cipher model, was only introduced in 2018 [39]. Known examples also pose achievable security notions.

The random oracle and ideal cipher model are the most basic idealised models. When it comes to the analysis of more advanced constructions or protocols, two common models are the indifferentiability framework [54] and the universal composability (UC) framework [22]. The general possibility of proofs of post-quantum security in the indifferentiability framework was recently demonstrated [74]. The general possibility of proofs in stronger variants of this framework is the subject of ongoing investigation. The achievability of proofs of post-quantum security in the UC model is still an open question. It is known that the UC model can be extended even to the Q2 setting when considering information-theoretic security; but there is an important distinction between information-theoretic results and complexity-theoretic results. The UC framework is commonly used in the analysis of cryptographic protocols, and complexity-theoretic results are necessary for establishing the security of protocols that use public key cryptography.

5.3 REVISITING PROOFS

When the models are fixed, a last challenge is to vet the existing proofs or to write new ones where necessary. Due to the focus of this report, we restrict ourselves in the following to results for the Q1 models. Proofs in the standard model do still apply when considering quantum adversaries as long as they avoid certain problematic techniques, most notably rewinding. A formal analysis that describes the precise conditions under which a classical proof directly translates to the corresponding Q1 model appeared in [64]. Unfortunately, these seem to be the only proofs that remain intact. Proofs that make use of the mentioned techniques have to be rewritten. While the question of rewinding proofs in a quantum setting has been the subject of a long line of research, many open questions remain (cf. [67] or the lecture by Unruh at Quiques [70]).

Proofs in idealised models generally have to be revisited as the oracles change. When the oracles become quantum-accessible a lot of commonly used proof techniques become inapplicable. Notable exceptions are so-called history-free reductions. For these it was shown in [18] that they also apply in the QROM.

The two main reasons for ROM proofs to fail in the QROM are as follows. Firstly, we have to measure a quantum register to learn its state. However, a measurement can and in most cases does change the state of the register. As a consequence, a reduction cannot learn the queries an adversary makes to its oracles anymore, which was a crucial step in many proofs. Secondly, an adversary may query an oracle at all possible inputs with a single query. This causes the failure of proofs that reason about an adversary not querying an oracle on a certain position, another technique that is frequently used in proofs. Both issues have been solved in recent works [74, 3, 36].

Generally, most of the results in the ROM have been recovered in the QROM though with less tight bounds. Most importantly, new security proofs in the QROM are known for the different constructions of KEM and signature schemes used for the NIST proposals (see Chapter 3 of the recent ENISA study Post-Quantum Cryptography: Current state and quantum mitigation[3]). For KEMs that are constructed from a deterministic PKE scheme, the QROM proofs are almost as tight as the proofs in the ROM [15, 46]. However, these form a notable exception as most other proofs are significantly less tight than the corresponding proofs in the ROM. The problem with less tight bounds is that with such bounds parameter selection is not supported by the proofs as the relation between the security of a scheme and the underlying mathematical problems is too loose. This is especially dangerous as we are lacking experience when it comes to the impact of quantum attacks on schemes and protocols. Even if they do not fully break them, they can significantly decrease the security level (see for example the case of MQDSS, a second round NIST

[3] https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation, (accessed October 17, 2022).

candidate [44]). Hence, more research is necessary on new techniques that allow tighter proofs in the QROM.

The two main open questions when it comes to giving proofs of post-quantum security refer to the handling of random permutations and again the UC framework. So far, several attempts have been made to extend the solution that allows to observe adversarial queries in the QROM [74] to permutations [27, 69] but so far all of them have turned out to be flawed. This problem is relevant to the analysis of SHA-3. As mentioned above, so far the UC model is unexplored territory in the post-quantum setting. The UC model is necessary whenever different instances of a protocol or scheme may be composed in some way to build a bigger scheme. Hence, many protocols, including password-authenticated key exchange, and multi-party computation protocols, are commonly proven to be secure in the UC framework. Therefore, it is a necessity to explore this space in order to also recover security proofs for these protocols.

5.4 SUMMARY

When considering adversaries equipped with quantum computers, not only the mathematical assumptions have to change but also the models and security proofs in use. In the foreseeable future, the relevant security models are Q1 models, meaning that adversaries get quantum access to oracles implementing public functions and classical access to oracles implementing secretly keyed functions (like a signing or a decryption oracle). The most prominent Q1 model is the quantum-accessible random oracle model (QROM). Proofs for basic building blocks, such as KEMs and signatures, have been recovered in the QROM. However, the bounds are worse. Thus, they often cannot support the claimed security for proposed parameters – except for a few notable exceptions as discussed above.

Beyond basic primitives, new models and proofs are still sparse. More research on new models and proof techniques for these models is required. This will enable us to justify parameter choices for post-quantum cryptography by security proofs.

6 STANDARDISATION EFFORTS FOR PROTOCOLS

Besides NIST, other standardisation bodies have also been busy with preparing for post-quantum cryptography.

ETSI, the European Telecommunications Standards Institute, has established a working group on Quantum-Safe Cryptography (QSC)[1]. The working group has published several documents including one on protocols and standards adapted to post-quantum cryptography[2].

The IETF (Internet Engineering Task Force) defines protocols for Internet communication. Different protocols are handled by different working groups. The CFRG ()Crypto-Forum Research Group) which handles cryptosystems for different applications, has deferred standardising any KEMs and signature schemes until after the end of the NIST process. However, other working groups have investigated how the protocols under their guard can be adapted. For example the IKE (Internet key exchange) working group has formulated how to use pre-shared keys in IKE in Mixing Preshared Keys in IKEv2 for Post-quantum Security[3]. The IKE protocol is used in IPsec for VPNs. There are also proposals to the TLS working group regarding mechanisms to use various NIST candidates in TLS, and a proposal Quantum Safe Cryptography Key Information[4] regarding key serialisation. The LAMPS working group is discussing an Internet draft for supporting PQ in certificates [76]. Further working groups started similar discussions but do not have Internet drafts yet.

ISO's working group on cryptography, SC 27/JTC 1 WG 2, has conducted a two-year study period on post-quantum cryptography during which the experts were briefed by researchers in the field on the functioning of and main avenues for the families of post-quantum cryptography. While discussions about choosing candidates have been delayed till after NIST's decision, the working group has published a standing document [25] describing all families of systems.

Following a workshop on 'Considerations in Migrating to Post-Quantum Cryptographic Algorithms', NIST's National Cybersecurity Center of Excellence (NCCoE) wrote a summary report [7], covering five application scenarios which currently deploy pre-quantum cryptography and outlining the high-level architecture and referencing relevant standards.

While we recognise NIST's leading role in standardising cryptographic systems we recommend that all stakeholders – governments, industry, and data-protection officers as well as other standardisation bodies – acquire sufficient understanding of post-quantum cryptography to make informed decisions.

Most recently, after the draft for this report was finalised, the French cybersecurity agency ANSSI published its views on the transition to post-quantum cryptography [55]. Beyond giving common advice to use double encryption, but without going into the details, the report also cautions about the immaturity of post-quantum algorithms, saying that they are still in the research phase. The report does not make any recommendations regarding which systems to choose but states explicitly that systems which are not chosen by NIST but are demonstrably stronger also qualify for security evaluation and certification. Even more recently, a report by the German BSI appeared [75] discussing their view on post-quantum security and giving recommendations for the next steps. Similar to ANSSI, the

[1] https://www.etsi.org/technologies/quantum-safe-cryptography, (accessed October 17, 2022).
[2] https://www.etsi.org/newsroom/press-releases/1805-2020-08-etsi-releases-migration-strategies-and-recommendations-for-quantum-safe-sch (accessed October 17, 2022).
[3] https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-qr-ikev2, (accessed October 17, 2022).
[4] https://datatracker.ietf.org/doc/draft-uni-qsckeys/, (accessed October 17, 2022).

BSI recommends the use of double encryption and signatures, and highlights the need for further research on post-quantum cryptography. Moreover, the BSI report provides background and makes recommendations for short-term protective measures.

The above-mentioned works show progress towards securing infrastructure against quantum attacks. At the same time it should be noted that standardisation bodies continue to standardise protocols built using pre-quantum systems that will not withstand quantum attacks. For example, the CFRG is currently in the process of selecting a new standard for password-authenticated key exchange (PAKE). It seems advisable to also apply the concepts of double encryption, double KEM, double signatures, etc. – see Chapter 4 – to such advanced protocols. However, this is not on the current roadmap. Worse, the existence of a recent standard can make it a lot harder to motivate an organisation or the community to develop a new standard. Therefore, we recommend that post-quantum integration should already be considered when developing new standards.

6.1 SUMMARY

Several standardisation bodies have agendas for standardising post-quantum systems and protocols. However, not all new initiatives for standards consider security under quantum attacks and more attention to future-proofing is necessary. Furthermore, we recommend that all relevant parties acquire knowledge in post-quantum cryptography and not rely solely on external standards.

7 CONCLUSIONS

We had already discussed in ENISA's 2021 'Post-Quantum Cryptography: Current state and quantum mitigation' study[1] that Quantum Technology and in particular Quantum Computing are set to be a major disruptor. We have known for more than two decades that the development of a sufficiently large and practical quantum computing machine will render most cryptographic systems insecure, radically transforming the existing threat model and endangering our infrastructure. Current public key cryptosystems, used in e-commerce, digital signatures, electronic identities etc., will be the most impacted by such a development.

While such a system does not yet exist, there are several ongoing large scale investments from both industry players and nation states. However, not all development in the area is public and it is not unthinkable that the first fully functional large quantum computer will not be publicly announced. In addition, rolling out new cryptographic systems takes a lot of time and effort; it might even be infeasible for systems with restricted accessibility, such as satellites. Thus, policy makers and system owners should make preparations.

Deciding on a new quantum-resistant cryptoalgorithm, like the ones selected by NIST, is only one part of the solution. Any PQC proposal will need to either integrate with existing systems and protocols or will require the design and deployment of new systems and protocols. Neither is a trivial task. The differences between existing cryptoalgorithms and PQC, in terms of key and ciphertext size, and computation times, even when small in absolute numbers, might in aggregate introduced unexpected problems for specialized use cases; such as in car2car communications. Which means that we might end up with multiple options, each catering for different use cases and causing further overhead on standardizing and implementing these migrations.

Furthermore, as with any new proposal in cryptography, there will be some uncertainty with the actual security levels offered by proposed PQC systems, at least in the early stages. A scenario where a new cryptanalytical attack is discovered after we have migrated away to PQC, from current cryptography, such as modern Elliptic Curve Cryptography (ECC) systems, is not inconceivable. In an even worse scenario, such an attack might not require quantum computations at all, making our communications and infrastructure weaker here and now.

Therefore early adopters will need to make a trade-off between quantum-resistance (i.e. migrating to a PQC system), current security-levels attested by years of research (i.e. keep using a current proven cryptosystem, such as ECC) and financial, time or computational resources (i.e. deploy and use a double encryption or signature scheme), at least till PQC systems mature and the advent of new security models, new proof techniques, and supporting tools allow us to identify [cryptographic] constructions that cannot be proven secure and replace them.

This study provides an overview of the state-of-the-art with regard to the challenges awaiting us, beyond the design and selection of a PQC system.

In the world of post-quantum cryptography, protocol designers need to be aware of the possibility of different trade-offs and choose systems matching their application scenario, taking into account (1) how frequently public keys are sent, relative to ciphertexts or signed messages using them, and (2) how important computation speed is relative to bandwidth. Developing guidelines for major use cases will ease the process.

Existing protocols might need tweaks and updates to ensure proper integration with PQC. It makes sense to withhold major changes till we decide on one or more PQC systems

[1] https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation, (accessed October 17, 2022).

through standardization, such as the ongoing NIST PQC process[2]. As an indication, from the 82 initial proposals in 2017, only four candidate algorithms have been selected in July 2022 for standardization and four[3] additional algorithms will continue into the fourth round. So any investment in integrating the withdrawn or rejected candidates would have had diminishing returns. Any changes will need to be tested to ensure they do not unknowingly introduce undesirable changes; for example security weaknesses, both at the design level and for each implementation.

A different approach to dealing with the difference in interfaces is to design new protocols, developed around post-quantum systems and taking their specifications into account. This option will probably lead to the most efficient protocols, but with a greater cost. Examples covered are: replacing signatures with KEMs, putting key-sizes as guiding factors, and offering post-quantum protection at a different layer of the Internet. The latter has the added benefit of promoting a fast rollout, not hampered by slow standardisation processes. The number of published proposals for new protocols built specifically around PQC systems is still somewhat limited and more work in this direction is required.

We already mentioned the uncertainty of migrating to a new cryptosystem. To address this risk one can use a hybrid system; i.e. deploy post-quantum cryptography today as an extra layer together with pre-quantum cryptography, rather than deploying it as a replacement for pre-quantum cryptography. Sign with a pre-quantum cryptosystem and with a post-quantum cryptosystem, making sure that the verifier checks both signatures. Encrypt as usual with pre-quantum cryptography, and then encrypt the result with post-quantum cryptography, so that decryption requires both secret keys.

Applications that can afford the data sent by post-quantum cryptography are likely to be able to afford an extra 32 bytes for double encryption with elliptic-curve cryptography and post-quantum cryptography. Similar comments apply to double signing.

However, hybrid systems can be a greater performance problem in other cost metrics. There has been some investigation of compact implementations of post-quantum cryptography for small devices, and there are various ideas on how to save space by merging implementations of post-quantum cryptography with implementations of elliptic-curve cryptography. This is another area where more work is required.

At some point the security analysis of post-quantum cryptosystems will eventually stabilize and provided quantum cryptanalysis shows some practical results (i.e. computing elliptic-curve discrete logarithms of considerable length) we will need to revisit the continued value of deploying elliptic-curve cryptography. Assuming that there is public consensus someday that elliptic-curve cryptography is obsolete, it will then be reasonable to consider removing it from protocols such as TLS, with the goal of eventually allowing simpler TLS implementations, and from any hybrid implementations.

Based on existing knowledge of quantum attacks, the consensus is that only public key cryptography is threatened, while attacks against other schemes and protocols are not known for now (with symmetric systems a duplication of the key size would defeat current best quantum cryptanalysis). A common approach in modern cryptography is to reduce the attack surface against the mathematical security of a protocol or system to breaking the security of its basic building blocks via security proofs. Building blocks in this case can either be mathematical problems, such as the RSA problem, or higher level building blocks; such as key encapsulation mechanisms (KEM), signature schemes, or hash functions for which we have already established security by another proof or cryptanalysis.

Clearly, if new protocols are constructed these require new proofs. But even existing proofs for well-known protocols have to be revisited. The reason is that when we aim for security against adversaries making use of a quantum computer, we have to model our adversaries also as quantum algorithms. This requires changing models and deciding about the specific abilities of quantum adversaries. Existing proofs will have to be vetted again in this new setting. Beyond basic primitives, new models and proofs are still sparse; especially in the analysis of protocols. More research on new models and proof

[2] e.g. NIST's https://csrc.nist.gov/Projects/post-quantum-cryptography, (accessed October 17, 2022).
[3] One of fourth round selections, SIKE, was cryptanalysed later that month https://eprint.iacr.org/2022/975. A second attack was published soon after https://eprint.iacr.org/2022/1026, (accessed October 17, 2022).

techniques for these models is required. This will enable us to justify parameter choices for post-quantum cryptography by security proofs.

Finally, it should be noted that standardisation bodies continue to standardise protocols built using pre-quantum systems that will not withstand quantum attacks. It is advisable to apply the concepts of hybrid systems (double encryption, double KEM, double signatures, etc.) to such advanced protocols. However, this is not on the current roadmap. Worse, the existence of a recent standard can make it a lot harder to motivate an organization or the community to develop a new standard. Therefore, it is recommend that post-quantum integration should be considered whenever developing new standards or updating existing ones.

BIBLIOGRAPHY

[1] Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. Unforgeable quantum encryption. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018, Part III*, volume 10822 of *Lecture Notes in Computer Science*, pages 489–519. Springer, Heidelberg, April / May 2018.

[2] Martin R. Albrecht, Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Kenneth G. Paterson, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlinson, and Wen Wang. Classic McEliece. Round 3 submission to NIST post-quantum call for proposals, 2020. https://classic.mceliece.org/.

[3] Andris Ambainis, Mike Hamburg, and Dominique Unruh. Quantum security proofs using semi-classical oracles. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 269–295. Springer, Heidelberg, August 2019.

[4] Daniel Augot, Lejla Batina, Daniel J. Bernstein, Joppe Bos, Johannes Buchmann, Wouter Castryck, Orr Dunkelman, Tim Güeysu, Shay Gueron, Andreas Hülsing, Tanja Lange, Mohamed Saied Emam Mohamed, Christian Rechberger, Peter Schwabe, Nicolas Sendrier, Frederik Vercauteren, and Bo-Yin Yang. Initial recommendations of long-term secure post-quantum systems, 2015. https://pqcrypto.eu.org/docs/initial-recommendations.pdf.

[5] Reza Azarderakhsh, Rami Elkhatib, Brian Koziel, and Brandon Langenberg. Hardware deployment of hybrid PQC: SIKE+ECDH. In Joaquín García-Alfaro, Shujun Li, Radha Poovendran, Hervé Debar, and Moti Yung, editors, *Security and Privacy in Communication Networks - 17th EAI International Conference, SecureComm 2021, Virtual Event, September 6-9, 2021, Proceedings, Part II*, volume 399 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 475–491. Springer, 2021.

[6] Elaine Barker, Lily Chen, and Richard Davis. NIST special publication 800-56C revision 2: Recommendation for key-derivation methods in key-establishment schemes, 2020. https://csrc.nist.gov/publications/detail/sp/800-56c/rev-2/final.

[7] William Barker and Murugiah Souppaya. NIST's National Cybersecurity Center of Excellence work on Migration to Post-Quantum Cryptography, 2021. https://www.nccoe.nist.gov/sites/default/fileslibrary/project-descriptions/pqc-migration-project-description-final.pdf.

[8] Daniel J. Bernstein. D2.5 Internet: Integration. PQCRYPTO project Deliverable D2.5 https://pqcrypto.eu.org/deliverables/d2.5.pdf, 2018.

[9] Daniel J. Bernstein, Billy Bob Brumley, Ming-Shing Chen, Chitchanok Chuengsatiansup, Tanja Lange, Adrian Marotzke, Bo-Yuan Peng, Nicola Tuveri, Christine van Vredendaal, and Bo-Yin Yang. NTRU Prime. Round 3 submission to NIST post-quantum call for proposals, 2020. https://ntruprime.cr.yp.to/nist.html.

[10] Daniel J. Bernstein, Billy Bob Brumley, Ming-Shing Chen, and Nicola Tuveri. OpenSSLNTRU: Faster post-quantum TLS key exchange. In *USENIX Security 22: 31st USENIX Security Symposium*, Boston, MA, August 2022. USENIX Association. https://www.usenix.org/conference/usenixsecurity22/presentation/bernstein.

[11] Daniel J. Bernstein and Tanja Lange (editors). ebacs: Ecrypt benchmarking of cryptographic systems. https://bench.cr.yp.to, accessed 15 Nov 2021.

[12] Daniel J. Bernstein and Tanja Lange. McTiny: Fast high-confidence post-quantum key erasure for tiny network servers. In Srdjan Capkun and Franziska Roesner, editors, *USENIX Security 2020: 29th USENIX Security Symposium*, pages 1731–1748. USENIX Association, August 2020.

[13] Ward Beullens, Jan-Pieter D'Anvers, Andreas Hülsing, Tanja Lange, Lorenz Panny, Cyprien de Saint Guilhem, Nigel P. Smart, Evangelos Rekleitis, Angeliki Aktypi, and Athanasios-Vasileios Grammatopoulos. Post-quantum cryptography: Current state and quantum mitigation, 2021. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation/@@download/fullReport.

[14] Nina Bindel, Jacqueline Brendel, Marc Fischlin, Brian Goncalves, and Douglas Stebila. Hybrid key encapsulation mechanisms and authenticated key exchange. In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019*, pages 206–226. Springer, Heidelberg, 2019.

[15] Nina Bindel, Mike Hamburg, Kathrin Hövelmanns, Andreas Hülsing, and Edoardo Persichetti. Tighter proofs of CCA security in the quantum random oracle model. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019: 17th Theory of Cryptography Conference, Part II*, volume 11892 of *Lecture Notes in Computer Science*, pages 61–90. Springer, Heidelberg, December 2019.

[16] Nina Bindel, Udyani Herath, Matthew McKague, and Douglas Stebila. Transitioning to a quantum-resistant public key infrastructure. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017*, pages 384–405. Springer, Heidelberg, 2017.

[17] Nina Bindel, Sarah McCarthy, Hanif Rahbari, and Geoff Twardokus. Suitability of 3rd round signature candidates for vehicle-to-vehicle communication, 2021. https://csrc.nist.gov/CSRC/media/Presentations/suitability-of-3rd-round-signature-candidates-for/images-media/session-5-bindel-suitability-vehicle.pdf.

[18] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology – ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, Heidelberg, December 2011.

[19] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013, Part II*, volume 8043 of *Lecture Notes in Computer Science*, pages 361–379. Springer, Heidelberg, August 2013.

[20] Ron Bonica, Fred Baker, Geoff Huston, Robert M. Hinden, Ole Troan, and Fernando Gont. IP fragmentation considered fragile, 2020. https://datatracker.ietf.org/doc/html/rfc8900.

[21] Matt Braithwaite. Experimenting with post-quantum cryptography, 2016. https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html.

[22] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *42nd Annual Symposium on Foundations of Computer Science*, pages 136–145. IEEE Computer Society Press, October 2001.

[23] A. Casanova, J.-C. Faugère, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem. GeMSS. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.

[24] Cong Chen, Oussama Danba, Jeffrey Hoffstein, Andreas Hulsing, Joost Rijneveld, John M. Schanck, Peter Schwabe, William Whyte, Zhenfei Zhang, Tsunekazu Saito, Takashi Yamakawa, and Keita Xagawa. NTRU. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.

[25] Lily Chen, Tanja Lange, Shiho Moriai, Rafael Misoczki, Xianhui Lu, Le Trieu Phong, Bo-Yin Yang, and Ward Beullens. SD8 (post-quantum cryptography). Technical Report N 2271–2276, ISO/IEC JTC 1/SC 27/WG 2, 2020. https://www.din.de/resource/blob/721042/4f1941ac1de9685115cf53bc1a14ac61/sc27wg2-sd8-data.zip.

[26] Eric Crockett, Christian Paquin, and Douglas Stebila. Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH. Cryptology ePrint Archive, Report 2019/858, 2019. https://eprint.iacr.org/2019/858.

[27] Jan Czajkowski. Quantum indifferentiability of SHA-3. Cryptology ePrint Archive, Report 2021/192, 2021. https://ia.cr/2021/192.

[28] Cyprien Delpech de Saint Guilhem, Nigel P. Smart, and Bogdan Warinschi. Generic forward-secure key agreement without signatures. In Phong Q. Nguyen and Jianying Zhou, editors, *ISC 2017: 20th International Conference on Information Security*, volume 10599 of *Lecture Notes in Computer Science*, pages 114–133. Springer, Heidelberg, November 2017.

[29] Jintai Ding, Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang, Matthias Kannwischer, and Jacques Patarin. Rainbow. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.

[30] Jason A. Donenfeld. WireGuard: Next generation kernel network tunnel. In *ISOC Network and Distributed System Security Symposium – NDSS 2017*. The Internet Society, February / March 2017.

[31] Karen Easterbrook, Kevin Kane, Brian LaMacchia, Dan Shumow, Greg Zaverucha, and Christian Paquin. Post-quantum cryptography VPN – pqcrypto-vpn 1.3. https://www.microsoft.com/en-us/research/project/post-quantum-crypto-vpn and https://github.com/microsoft/PQCrypto-VPN.

[32] Tommaso Gagliardoni. *Quantum Security of Cryptographic Primitives*. PhD thesis, Darmstadt University of Technology, Germany, 2017.

[33] Tommaso Gagliardoni, Andreas Hülsing, and Christian Schaffner. Semantic security and indistinguishability in the quantum world. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016, Part III*, volume 9816 of *Lecture Notes in Computer Science*, pages 60–89. Springer, Heidelberg, August 2016.

[34] Federico Giacon, Felix Heuer, and Bertram Poettering. KEM combiners. In Michel Abdalla and Ricardo Dahab, editors, *PKC 2018: 21st International Conference on Theory and Practice of Public Key Cryptography, Part I*, volume 10769 of *Lecture Notes in Computer Science*, pages 190–218. Springer, Heidelberg, March 2018.

[35] Ruben Gonzalez, Andreas Hülsing, Matthias J. Kannwischer, Juliane Krämer, Tanja Lange, Marc Stöttinger, Elisabeth Waitz, Thom Wiggers, and Bo-Yin Yang. Verifying post-quantum signatures in 8 kb of RAM. In *PQCrypto*, volume 12841 of *Lecture Notes in Computer Science*, pages 215–233. Springer, 2021.

[36] Alex B. Grilo, Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz. Tight adaptive reprogramming in the QROM. Cryptology ePrint Archive, Report 2020/1361, 2020. https://eprint.iacr.org/2020/1361.

[37] Mike Hamburg. Three Bears. Technical report, National Institute of Standards and Technology, 2019. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

[38] Andrew Hopkins. Post-quantum TLS now supported in AWS KMS. AWS Security Blog, 2019. https://aws.amazon.com/blogs/security/post-quantum-tls-now-supported-in-aws-kms/.

[39] Akinori Hosoyamada and Kan Yasuda. Building quantum-one-way functions from block ciphers: Davies-Meyer and Merkle-Damgård constructions. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 275–304. Springer, Heidelberg, De-

cember 2018.

[40] Loïs Huguenin-Dumittan and Serge Vaudenay. FO-like combiners and hybrid post-quantum cryptography, 2021. https://eprint.iacr.org/2021/1288.

[41] Andreas Hulsing, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kolbl, Tanja Lange, Martin M Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, Jean-Philippe Aumasson, Bas Westerbaan, and Ward Beullens. SPHINCS+. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.

[42] Andreas Hülsing, Kai-Chun Ning, Peter Schwabe, Florian Weber, and Philip R. Zimmermann. Post-quantum WireGuard. Cryptology ePrint Archive, Report 2020/379, 2020. https://eprint.iacr.org/2020/379.

[43] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, David Urbanik, Geovandro Pereira, Koray Karabina, and Aaron Hutchinson. SIKE. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.

[44] Daniel Kales and Greg Zaverucha. An attack on some signature schemes constructed from five-pass identification schemes. In Stephan Krenn, Haya Shulman, and Serge Vaudenay, editors, *CANS 20: 19th International Conference on Cryptology and Network Security*, volume 12579 of *Lecture Notes in Computer Science*, pages 3–22. Springer, Heidelberg, December 2020.

[45] Panos Kampanakis. Configuring post-quantum MACsec in Cisco switches, 2020. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/configuring-post-quantum-macsec-in-cisco-switches.pdf.

[46] Veronika Kuchta, Amin Sakzad, Damien Stehlé, Ron Steinfeld, and Shifeng Sun. Measure-rewind-measure: Tighter quantum random oracle model proofs for one-way to hiding and CCA security. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020, Part III*, volume 12107 of *Lecture Notes in Computer Science*, pages 703–728. Springer, Heidelberg, May 2020.

[47] Kris Kwiatkowski. Towards post-quantum cryptography in tls. Presentation at ECC 2019. https://eccworkshop.org/2019/slides/kwiatkowski.pdf.

[48] Kris Kwiatkowski and Luke Valenta. The TLS post-quantum experiment, 2018. https://blog.cloudflare.com/the-tls-post-quantum-experiment/.

[49] Tanja Lange. Post-quantum cryptography, part of selected areas in cryptology. Course in Mastermath, all materials online, 2021. https://hyperelliptic.org/tanja/teaching/pqcrypto21/.

[50] Adam Langley. Post-quantum confidentiality for TLS, 2018. https://www.imperialviolet.org/2018/04/11/pqconftls.html.

[51] Jonathan D. Levin. PQConnect: An Automated Boring Protocol for Quantum-Secure Tunnels. Master's thesis, Eindhoven University of Technology, 2021.

[52] Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehlé, and Shi Bai. CRYSTALS-DILITHIUM. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.

[53] Ueli M. Maurer and James L. Massey. Cascade ciphers: The importance of being first. *Journal of Cryptology*, 6(1):55–61, March 1993.

[54] Ueli M. Maurer, Renato Renner, and Clemens Holenstein. Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In Moni Naor, editor, *TCC 2004: 1st Theory of Cryptography Conference*, volume 2951 of

Lecture Notes in Computer Science, pages 21–39. Springer, Heidelberg, February 2004.

[55] Agence nationale de la sécurité des systèmes d'information. ANSSI views on the Post-Quantum Cryptography transition, 2022. https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/.

[56] Mike Ounsworth and Massimiliano Pala. Composite signatures for use in Internet PKI, 2021. https://datatracker.ietf.org/doc/html/draft-ounsworth-pq-composite-sigs/.

[57] Christian Paquin, Douglas Stebila, and Goutam Tamvada. Benchmarking post-quantum cryptography in TLS. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020*, pages 72–91. Springer, Heidelberg, 2020.

[58] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. FALCON. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.

[59] ETSI Technical Report. Quantum-safe virtual private networks. ETSI TR 103 617, 2018. https://www.etsi.org/deliver/etsi_tr/103600_103699/103617/01.01.01_60/tr_103617v010101p.pdf.

[60] ETSI Technical Report. Quantum-safe hybrid key exchanges. ETSI TS 103 744, 2020. https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.01.01_60/ts_103744v010101p.pdf.

[61] Peter Schwabe, Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, and Damien Stehlé. CRYSTALS-KYBER. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.

[62] Peter Schwabe, Douglas Stebila, and Thom Wiggers. Post-quantum TLS without handshake signatures. In Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna, editors, *ACM CCS 2020: 27th Conference on Computer and Communications Security*, pages 1461–1480. ACM Press, November 2020.

[63] Dimitrios Sikeridis, Panos Kampanakis, and Michael Devetsikiotis. Post-quantum authentication in TLS 1.3: A performance study. In *ISOC Network and Distributed System Security Symposium – NDSS 2020*. The Internet Society, February 2020.

[64] Fang Song. A note on quantum security for post-quantum cryptography. In Michele Mosca, editor, *Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014*, pages 246–265. Springer, Heidelberg, October 2014.

[65] Douglas Stebila, Scott Fluhrer, and Shay Gueron. Hybrid key exchange in TLS 1.3, 2021. https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design.

[66] Douglas Stebila and Michele Mosca. Post-quantum key exchange for the internet and the open quantum safe project. In Roberto Avanzi and Howard M. Heys, editors, *SAC 2016: 23rd Annual International Workshop on Selected Areas in Cryptography*, volume 10532 of *Lecture Notes in Computer Science*, pages 14–37. Springer, Heidelberg, August 2016. https://openquantumsafe.org/.

[67] Dominique Unruh. Quantum proofs of knowledge. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 135–152. Springer, Heidelberg, April 2012.

[68] Dominique Unruh. Computationally binding quantum commitments. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 497–527. Springer, Heidelberg, May 2016.

[69] Dominique Unruh. Compressed permutation oracles (and the collision-resistance of sponge/SHA3). Cryptology ePrint Archive, Report 2021/062, 2021. https://ia.cr/2021/

062.

[70] Dominique Unruh. Quantum rewinding. Lecture at Quiques 2021, 2021.

[71] Bas Westerban. Sizing up post-quantum signatures, 2201. https://blog.cloudflare.com/sizing-up-post-quantum-signatures/.

[72] Yufei Xing and Shuguo Li. A compact hardware implementation of CCA-secure key exchange mechanism CRYSTALS-KYBER on FPGA. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(2):328–356, 2021. https://tches.iacr.org/index.php/TCHES/article/view/8797.

[73] Takashi Yamakawa and Mark Zhandry. Classical vs quantum random oracles. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021, Part II*, volume 12697 of *Lecture Notes in Computer Science*, pages 568–597. Springer, Heidelberg, October 2021.

[74] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 239–268. Springer, Heidelberg, August 2019.

[75] Stephan Ehlen, Heike Hagemeier, Tobias Hemmert, Stavros Kousidis, Manfred Lochter, Stephanie Reinhardt and Thomas Wunderer. Quantum-safe cryptography - fundamentals, current developments and recommendations. Federal Office for Information Security (BSI), 2022, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=4.

[76] Sean Turner, Panos Kampanakis, Jake Massimo, and Bas Westerbaan. Algorithm Identifiers for NIST's PQC Algorithms for Use in the Internet X.509 Public Key Infrastructure, March 2022. https://datatracker.ietf.org/doc/draft-turner-lamps-nist-pqc-kem-certificates/01/. (work in progress).

TP-03-22-080-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-590-6
doi: 10.2824/151162