ESA UNCLASSIFIED – For ESA Official Use Only

ESA ESTEC
Keplerlaan 1
2201 AZ Noordwijk
The Netherlands

TECHNICAL NOTE - POST QUANTUM CRYPTOGRAPHY FOR SPACE MISSIONS

Prepared by	Antonios Atlasis
	TEC-ESS
Document Type	TN - Technical Note
Reference	ESA-TECESS-TN-2022-003162
Issue/Revision	1 . 0
Date of Issue	10/10/2022
Status	For Information Only

APPROVAL

Title	Technical Note - Post Quantum Cryptography for Space Missions		
Issue Number	1	Revision Number	0
Author	Antonios Atlasis	Date	10/10/2022
Approved By		Date of Approval	

CHANGE LOG

Reason for change	Issue Nr	Revision Number	Date

CHANGE RECORD

Issue Number 1	Revision Number 0		
Reason for change	Date	Pages	Paragraph(s)

DISTRIBUTION

Name/Organisational Unit

Table of Contents

1. Introduction ... 4

2. Quantum Risk Assesment ... 6

3. Families of PQC Algorithms ... 7

4. The NIST PQC Competition ... 8

4.1. Evaluation Criteria ... 8

4.2. NIST Security Strengths ... 8

4.3. Results of NIST PQC Round 3 ... 9

5. The View of other Agencies on PQC Algorithms ... 11

6. Latest Research on PQC Algorithms ... 12

7. Comparison of NIST Round 3 Selected and Round 4 PQC Candidates ... 13

7.1. Public-key Encryption and Key-establishment Algorithms ... 13

7.2. Digital Signatures Algorithms ... 15

7.3. Performance Benchmarks ... 16

8. The Need for Hybrid and Agile Implementations ... 17

9. Protocol challenges and paradigms ... 18

9.1. Key Encapsulation Mechanisms ... 18

9.2. Post-Quantum Wireguard ... 18

9.3. KEMTLS and KEMTLS-PDK: TLS PQC Implementations ... 19

10. Design considerations for a PQC Space Protocol ... 21

References ... 23

1. INTRODUCTION

Public key (or asymmetric) cryptography is an indispensable component of our global communication digital infrastructure. Many of our most crucial communication protocols rely on asymmetric cryptographic primitives that offer public key encryption, digital signatures, and key exchange. Currently, these functionalities are primarily implemented using Diffie-Hellman key exchange, the RSA (RivestShamir-Adleman) cryptosystem, and elliptic curve cryptosystems. The security of these depends on the difficulty of certain number theoretic problems such as Integer Factorization or the Discrete Log Problem (NISTIR 8105, 2016).

In 1994, mathematician Peter Shor discovered a quantum computer algorithm that efficiently factors numbers and computes discrete logarithms. With it, you can break nearly all public-key cryptography deployed today, including RSA and elliptic curve cryptography (Shor, 1994). As an example (and depending on quantum implementation), according to estimations (National Academies, 2019), quantum computers using Shor's algorithm could break:

- RSA (2048 bits key) in 28.63 hours
- RSA (4096 bits key) in 229 hours
- ECC Discrete-log problem (384 bits key) in 37.67 hours
- ECC Discrete-log problem (521 bits key) in 55 hours

Two years later, Grover published a search algorithm that provides a quadratic speedup on unstructured search problems, which can be used against symmetric algorithms and hashes (Grover, 1996). However, in this case the impact on these cryptographic primitives (i.e. symmetric algorithms and hashes) can be managed by doubling their key size to compensate for the quadratic speedup achieved by Grover's algorithm. Therefore, these cryptographic functions would be less affected (NISTIR 8105, 2016).

Following the above, when quantum computers will materialise, key exchange, digital signature and authentication mechanisms employing the current asymmetric cryptographic algorithms will be in danger. There has been a lot of debate regarding the timeline of quantum computer development. According to a poll among experts published in (Mosca & Piani, 2019), quantum computers will probably (i.e. with a probability greater than 50%) be ready in 15 to 20 years (although the roadmap of some actors is far more aggressive).

While space systems are currently heavily based on symmetric cryptographic primitives and hashes, this may change in the future for the following reasons:

- CCSDS standards already foresee the usage of asymmetric primitives, for digital signature authentication, (CCSDS 352.0-B-2, 2019).
- New space and in general the use of large constellations will make the use of symmetric cryptographic mechanisms a not practical solutions due to lack of scalability (pre-shared symmetric keys approach does not scale).
- Asymmetric cryptographic mechanisms can enhance flexibility for federated operations (since exchange of pre-shared keys can be more challenging).
- Asymmetric cryptographic mechanisms can increase interoperability with terrestrial systems.

While it is anticipated that typical institutional missions will probably continue to operate with symmetric based ciphers, the flexibility and advantage of asymmetric key management should not be ignored. Future projects with large constellation can benefit from the simplicity and scalability that asymmetric based solutions offer.

Therefore, it is important to gradually evolve our space protocols to incorporate the support of asymmetric cryptography. And given the quantum threat mentioned above, such solutions must be *quantum resistant*, i.e. based on *Post Quantum Cryptography* (*PQC*).

The objective of this technical note is neither to perform a complete survey of ongoing PQC standardisation and research efforts (some good surveys can be found in (BSI, 2021) and (ENISA, 2021), nor to propose a specific solution for PQC implementation for space missions, but rather to constitute a starting point of the steps required to be taken so as to incorporate PQC cryptographic solutions in space missions. As it will be explained, such implementations do not only require the adoption of PQC cryptographic primitives, but also the adaptation (or design from scratch) of networking protocols currently used in several applications (e.g. TLS, IPSec in the Internet world, SDLS in space protocols). Due to the specificities of the PQC candidates, the required protocol adaptations are not simple and thorough design considerations and testing are needed before any of these adaptations can be implemented.

2. QUANTUM RISK ASSESMENT

While it will take a few or more years for quantum computers to materialise, this does not mean there is still time to defer the migration to asymmetric cryptographic algorithms resilient to quantum computers, due the "store now, decrypt later" class of attacks. In (Mosca & Mulholland, n.d.) and (Mosca, 2018) a formula was published to estimate the time we have until we start migration. The quantum risk assessment methodology published in (Mosca & Mulholland, n.d.) can be summarised as follows:

- Identify the threat actors and estimate their time "z" to have quantum computers available that could break currently employed cryptographic algorithms.
- Identify the lifetime of your assets "x". This lifetime includes the lifetime e.g. of your satellites, etc., AND the lifetime of the information itself (i.e. for how long information has to be protected after being generated).
- Identify the time "y" required to transform the organisations technical infrastructure to a quantum-safe implementation.
- Determine the quantum risk by calculating whether business assets will become vulnerable before the organisation can move to protect them: x+y must not be greater than z so as not to put at risk.

So, if we assume that quantum computers will become available in 15 years (z=15), and the lifetime of our assets is 10 years (x=10), we have about 5 years to migrate. However, if we consider that for a space system the development is typically quite lengthy (y > 5), we can understand that we are actually already late and we need to initiate actions literally now.

It should be noted that national security agencies of ESA Member States like the German BSI work under the hypothesis that cryptographically relevant quantum computers will be available in the early 2030s, as a benchmark for quantum risk assessment (BSI, 2022).

3. FAMILIES OF PQC ALGORITHMS

PQC algorithms are based on mathematical problems for whose solution neither efficient classical algorithms nor efficient quantum algorithms are known today (BSI, 2022). The most important families of them, are the following:

- *Code-based cryptography*: The security of code-based schemes is based on the difficulty of efficiently decoding general error-correcting codes. They typically have short ciphertext at the expense of very large key sizes.
- *Lattice-based cryptography*: The security of lattice-based schemes is based on the difficulty of solving certain computational problems in mathematical lattices. They can be used for both encryption and signatures.
- *Hash-based cryptography*: The security of hash-based signature schemes is based on the security properties of the hash function used. Their security is well understood. They are used for digital signatures. There are two families of hash-based algorithms:
    - Stateful: In this case we need to predict and keep track of the signatures we use (like XMMs and LMS, see below).
    - Stateless: No need to keep track of the signatures we used.
- *Isogeny-based cryptography*: Isogeny-based schemes base their security on the fact that it is difficult to find an isogeny between two super-singular elliptic curves, if one exists.
- *Multivariate cryptography*: The security of multivariate cryptography is based on the assumption that multivariate polynomial systems of equations over finite fields are hard to solve. Typically, they are not very efficient, since they have very large public keys and long decryption times.

4. THE NIST PQC COMPETITION

In response to the Quantum Threat to asymmetric cryptography, the U.S. National Institute of Standards and Technology (NIST) in December of 2016 initiated a public, competition-like process to select quantum-resistant public-key cryptographic algorithms (NIST, 2016a). The new public-key cryptography standards will specify algorithms for digital signatures, public-key encryption and key establishment.

In this competition experts from all over the world participate and have been invited to propose PQC asymmetric based solutions. Other countries (e.g. China, Russia) have initiated their own process to standardise such mechanisms. European security agencies abide by the NIST competition. For instance, “BSI welcomes the NIST process as a method of defining standards in a transparent international process that can then be used worldwide. It is particularly opposed to a separate process for standardising German or European algorithms” (BSI, 2022a).

4.1. Evaluation Criteria

The evaluation criteria of the NIST selection process, which involves several rounds, were published in (NIST, 2016b). Several criteria have been established (e.g. security strengths related, cost related, and other). The cost related ones, which constitute important criteria from implementation perspective, are the following:

- Public key, ciphertext, and signature size
- Computational efficiency of public and private key operations
- Computational efficiency of key generation
- Decryption failures

4.2. NIST Security Strengths

One of the important factors of the NIST evaluation criteria are the security strengths. NIST designated five security strength categories for classifying the computational complexity of attacks that violate the security definitions. These security strengths defined in (NIST, 2016b) were based on the computational resources required to perform certain brute-force attacks against the existing NIST standards for AES and SHA in a variety of different models of the cost of computation, both classical and quantum. These are:

- Security level 1 ⇒ equivalent to AES-128 key search.
- Security level 2 ⇒ equivalent to SHA-256/SHA3-256 collision search.
- Security level 3 ⇒ AES-192 key search.
- Security level 4 ⇒ SHA-384/SHA3-384 collision search.
- Security level 5 ⇒ AES-256 key search.

4.3. Results of NIST PQC Round 3

The Candidates to be Standardized and Round 4 Submissions were announced in July of 2022 (NIST, 2022a), accompanied by a status report (NIST 8413, 2022). The selected algorithms are (NIST, 2022b):

- Public-key Encryption and Key-establishment Algorithms:
    - CRYSTALS-KYBER (lattice based, https://pq-crystals.org/kyber/index.shtml)
- Digital Signature Algorithms
    - CRYSTALS-DILITHIUM (lattice based, https://pq-crystals.org/kyber/index.shtml)
    - FALCON (lattice-based, https://falcon-sign.info)
    - SPHINCS+ (stateless hash-based, https://sphincs.org)

It should be noted that while there are multiple signature algorithms selected, NIST recommends CRYSTALS–Dilithium as the primary algorithm to be implemented.

The ones that moved to Round 4 for potential future standardisation (NIST, 2022c), are the following:

- Public-key Encryption and Key-establishment Algorithms
    - BIKE (code-based, https://bikesuite.org/)
    - Classic McEliece (code-based, https://classic.mceliece.org/)
    - HQC - Hamming Quasi-Cyclic (code-based, http://pqc-hqc.org/)
    - SIKE (isopgeny-based, https://sike.org/)

In addition, in September of 2022 NIST called for additional digital signature proposals to be considered in the PQC standardization process (NIST, 2022d) with mainly focus on general-purpose signature schemes that are not based on structured lattices. For certain applications, such as certificate transparency, NIST may also be interested in signature schemes that have short signatures and fast verification.

5. THE VIEW OF OTHER AGENCIES ON PQC ALGORITHMS

Except from the NIST competition, there have been reports from other National Security Agencies on PQC. For instance, BSI currently recommends to focus on code-based, lattice-based and hash-based PQC algorithms only (BSI, 2022), since Multivariate schemes have a long history of attacks and fixes, while Isogenies should be explored further before a recommendation is considered.

Specifically, while BSI supports the ongoing NIST competition on PQC, it also recommended FrodoKEM and Classic McEliece methods for Key Establishment (BSI, 2022). The rational is that FrodoKEM can be a “conservative backup” (the reason that FrodoKEM did not advance at NIST competition does not concern the security of the scheme), while Classic McEliece has a long history (since 1978) of not being broken (however, it does require very large public keys). However, as mentioned above BSI welcomed the NSIT competition and is opposed to a separate European standardisation process. The above should be considered as mere recommendations.

BSI also recommends Merkkle (i.e. hash-based) signatures as future-proof digital signature schemes "for updateable crypto module by signature methods" (BSI, 2013),(BSI, 2022). The hash-based stateful schemes LMS (RFC 8553, 2019) and XMSS (RFC 8391, 2018) have sufficiently small signatures and keys and standardized by NIST SP 800-208 (NIST, 2020). BSI's view is that these signature schemes are most suitable for the design of long-lived root certificates and less suitable for end-user certificates due to them being stateful, a view also expressed in the aforementioned RFC. For instance, hash-based signatures can be a solution for root certificates.

6. LATEST RESEARCH ON PQC ALGORITHMS

Research on PQC algorithms is continuous, and some of the PQC families have not been researched for as many years as other. So, it is not a surprise that from time-to-time new research points out a weakness to one of the algorithms.

Lately, after NIST Round 3 announcement (NIST, 2022a), in August 2022 research presented "an efficient key recovery attack on the Supersingular Isogeny Diffie-Hellman protocol (SIDH)", where efficient means that the attack can break "the instantiation SIKEp434, which aims at security level 1 of the Post-Quantum Cryptography standardization process currently ran by NIST, in about one hour on a single core" (Castryck 2002). SIKE belongs to isogenies family, for which BSI had noted before the attack that more research is needed on this family before consideration for standardisation (BSI 2022). NIST and the SIKE teams acknowledged that SIKE and SIDH are insecure and should not be used (NIST, 2022e).

While the announcement of a broken PQC cipher which was selected as Round 4 candidate make create worries, the following should be considered.

a. Not all the PQC families have reached the same maturity. There are some PQC families which have been analysed for years (e.g. code-based), there are other (like isogenies-based) that are more recent and have suffered more from cryptanalytics attacks. Depending on the objective, there is a need to be a trade-off between how conservative a PQC cipher is (with the consulting of security agencies and experts) versus desired performance characteristics.

b. Mitigations to address concerns regarding maturity and security of PQC implementations are discussed in chapter 8.

7. COMPARISON OF NIST ROUND 3 SELECTED AND ROUND 4 PQC CANDIDATES

In this section a brief overview of the main characteristics, advantages and disadvantages of the Round 3 selected candidates and the ones moved to Round 4 are presented, based mainly on information obtained from (BSI, 2022), (ENISA, 2022) and (NISTIR 8413, 2022), unless otherwise specified. SIKE is not considered in the comparison due to the identified security issues mentioned above.

7.1. Public-key Encryption and Key-establishment Algorithms

- Crystals-Kyber (NIST Round 3 selected)
  - Comparatively small encryption keys that two parties can exchange easily; the public key sizes of Kyber are 800, 1184 and 1568 bytes for security levels 1, 3 and 5 respectively, and the ciphertext sizes are 768, 1088, 1568 bytes.
  - Fast key generation, encapsulation and decapsulation.
  - Design makes it easy to scale between the security levels and efficient to implement.
- Classic McEliece (NIST Round 4 candidate)
  - Very long history of analysis with no significant impact on the security
  - The ciphertext size is the smallest among all candidates since Round 2 and onward.
  - The disadvantage is the size of the public key, which for the highest security level takes more than 1MB.
  - It also demonstrates fairly slow key generation.
  - Despite its disadvantages, it can be used as a long-term identity key (as demonstrated by Post Quantum Wireguard), and it can also be useful also in PGP applications.
- BIKE (NIST Round 4 candidate)
  - Similarities with the Classic McEliece, but its structure allows the public key to be compressed.

- It has the most competitive performance among the non-lattice-based KEMs.

- HQC (NIST Round 4 candidate)
  - It enables small public key and ciphertext sizes; specifically, public keys are between 2249 and 7245 bytes, and ciphertexts are between 4481 and 14469 bytes, depending on the security level.
  - HQC's key generation and decapsulation only require a fraction of the kilocycles required by BIKE.

In the following table the aforementioned PQC algorithms are compared in terms of keys and ciphertext sizes (NIST 8413, 2022). For comparison reasons, in the table the corresponding sizes of RSA-2048 are included.

PQC Algorithm	Size (Bytes)								
	NIST Level I			NIST Level III			NIST Level V		
	Public Key	Private Key	Ciphertext	Public Key	Private Key	Ciphertext	Public Key	Private Key	Ciphertext
McEliece	261,120	6,492	128	524,620	13,608	188	1,044,992	13,932	240
Kyber	800	1,632	768	1,184	2,400	1,088	1,568	3,168	1,568
BIKE	1,540	280	1,572	3,082	418	3,144	5,122	580	5,154
HQC	2,249	40	4,481	4,522	40	9,026	7,245	40	14,469
RSA-2048	256	384	256						

Table 1: PQC Key Establishment algorithms (versus RSA-2048) comparison in terms of keys and ciphertext sizes (NIST 8413, 2022).

As we can see, the size of the McEliece ciphertext even for Security level 5 is smaller than the RSA-2048, but the public key size is rather extremely large, even for Security level 1. Indeed, these characteristics make McEliece ideal for long-term identity authentication, especially if the (long) public-key is pre-shared. On the other hand, Kyber, which has 3.5 times the size of the RSA-2048 public key and cipher text, outperforms BIKE and HQC regarding the size of both the public keys and the ciphertext. Based on the above characteristics, Kyber seems to be the best choice in terms of public key and ciphertext sizes, but Classic McEliece may be useful in some special cases (mentioned above).

7.2. Digital Signatures Algorithms

- CRYSTALS-Dilithium (NIST Round 3 selected);
  - A strong theoretical security basis, and an encouraging cryptanalytic history.
  - It has the benefit of not requiring floating-point arithmetic; relatively simple implementation.
- FALCON (NIST Round 3 selected);
  - A very compact and efficient post-quantum signature scheme. It has the smallest bandwidth among the third-round digital signature schemes (i.e. smallest combined size of public key and signature among all NIST candidates).
  - It is fast when verifying a signature.
  - Signing is somewhat slower than Dilithium and key generation is significantly slower. Requires complex floating point arithmetic implementation
- SPHINCS+ (NIST Round 3 selected);
  - Key generation and verification are much faster than signing. SPHINCS+ public keys are very short, but,
  - SPHINCS+ signatures are quite long. As an example, at NIST security level 1, the specification contains parameters that lead signature sizes of 7,856 bytes, while signing times are also quite large (e.g. 2,721 Mcycles for security level 1 using SHA2-256).
  - Verification speed is generally fast with (e.g. about 3 Mcycles for above parameters).

NIST recommends CRYSTALS-Dilithium as the primary algorithm, with FALCON for applications that need smaller signatures than Dilithium can provide. However, due to its very small bandwidth and fast verification signature, FALCON can also be useful for several applications. A good trade-off analysis between the two is needed depending on the application.

In the following table the three NIST Round 3 selected digital signature algorithms are compared in terms of keys and signatures sizes.

PQC Algorithm	Size (Bytes)								
	NIST Level I			NIST Level III			NIST Level V		
	Public Key	Private Key	Signature	Public Key	Private Key	Signature	Public Key	Private Key	Signature
Dilithium	1,312*	2,528*	2,420*	1,952	4,000	3,293	2,592	4,864	4,595
Falcon	897	7,553	666				1,793	13,953	1,280
SPHINCS+	32	64	7,856	48	96	16,224	64	128	29,792

* NOTE: The values (*) correspond to Security level 2.

Table 2: PQC Digital Signature algorithms comparison in terms of keys and signature sizes (NIST 8413, 2022).

7.3. Performance Benchmarks

The performance of PQC algorithms depends on a great extent to the processor (and its extensions) used for the cryptographic functions; in some cases the one may outperform the other depending on them. Hence, a comparison of them based on the available data may be misleading if someone tries to draw any conclusions for space applications.

To give an idea of an order of magnitude, on the figures below some KEM benchmarks on x86-64 processors with AVX2 extensions are given:

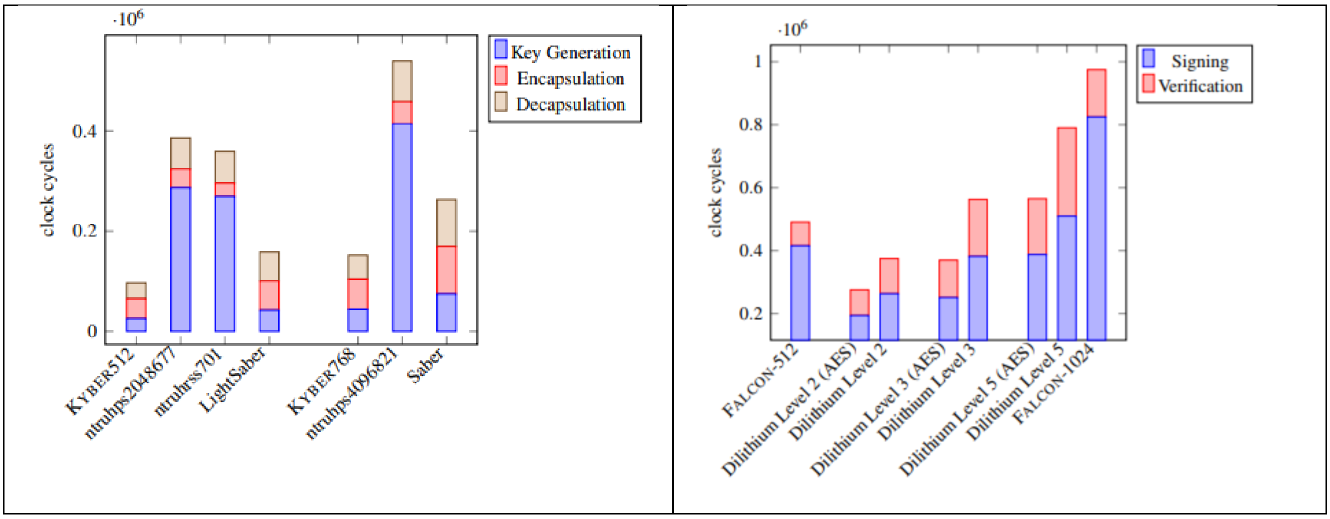

Figure 1: Examples of PQC Benchmarks on x86-64 processor with AVX2 extensions – figure from (NIST 8413, 2022).

More benchmarking graphs can be found in (NIST 8413, 2022).

8. THE NEED FOR HYBRID AND AGILE IMPLEMENTATIONS

Choosing algorithms that are quantum resistant is not the only measure we need to take to mitigate the quantum threat to cryptography. Given that, as also mentioned above, there have been attacks against some of the post quantum cryptographic families, to mitigate the risk and especially during the migration phase, a hybrid implementation is proposed, i.e. an implementation that incorporates both pre-quantum (such as RSA or (EC)DH) and post quantum algorithms (BSI 2022), (ENISA 2022). Hence, if during migration phase a new attack is published against a used PQC algorithm, the pre-quantum one will ensure the resilience against conventional computers. In the long term, the PQC one will provide the quantum resilience. Hybrid implementations can also facilitate certification and compliance needs. This approach of hybrid implementations will add a small overhead (pre-quantum algorithms have much smaller footprint than the post quantum ones).

In addition, BSI also recommends agile implementations, i.e. solutions that allow the secure and easy exchange of cryptographic parameters, procedures, or even protocols “on-the-fly”, i.e. while a cryptosystem is being used, so as to mitigate the risk of finding out later that e.g. the suitability of key lengths of security parameters cannot guarantee the required security level in long-term (BSI, 2022).

9. PROTOCOL CHALLENGES AND PARADIGMS

The replacement of pre-quantum cryptographic algorithms with post quantum ones is not a “plug-and-play” process; instead, for various reasons the various networking protocols that use asymmetric cryptography have also to be adapted, a process which is not easy at all, considering the multi-year ongoing efforts on Internet protocols like TLS and IKEv2 (there are already several efforts ongoing at IETF, and various draft RFCs are published). Such a process, i.e. design of a protocol compliant to incorporate PQC, can nevertheless and should start in parallel without having to wait for finalisation of PQC standardisation.
In this section some PQC protocol implementations are examined.

9.1. Key Encapsulation Mechanisms

One of the first major considerations regarding the protocol design is whether authentication shall be based on digital signatures, as it is typically the case in the pre-quantum era, or whether Key Encapsulation Mechanisms (KEM) should instead be used. While KEM-based implementations had already been proposed e.g. for TLS 1.3 (Schwabe, 2022), they had not been adopted so far since the benefits it offers versus digital signature based authentication is minimal, and significant updates in existing infrastructure would be required. When PQC implementations come into place, a quite different picture emerges where the KEM benefits are considerable, and existing infrastructure will have to be updated in any case. For instance, it is possible to choose PQC KEMs that offer (usually) smaller sizes and much better speed than any PQC signature scheme (Schwabe, 2022). This is why many PQC proposed implementations rely on KEM; some of them will be discussed below.
KEM-based authentication is typically demonstrated by successfully decrypting a challenge value, based on long-term public/private key pair, where the long-term public key is pre-shared by other means. This results in implicit authentication, meaning that the derived key can be computed only by the intended parties.

9.2. Post-Quantum Wireguard

The post-quantum implementation of Wireguard, or PQ-Wireguard (Hulsing, 2021), is an interesting case since it implements both post quantum forward secrecy and authentication (achieving NIST security level 3), but it also minimises the bandwidth required, by replacing the Diffie-Hellman-based handshake with a more generic approach only using interactive key-encapsulation mechanisms (KEMs). Wireguard is a “cryptographically opinionated” VPN protocol (i.e. it does not include a negotiation phase of cryptographic primitives to be used, but it rather fixes them in advance), resulting is simplicity and a small footprint. In addition, it achieves, among others, two interesting objectives:

- Finish the handshake in just one round trip;
- Fit each of the two handshake messages into just one unfragmented packet of at most 1232 bytes (i.e. what is left for the content of handshake messages in case IPv6 is used), including public key and ciphertext.

The above characteristics are interesting ones since they are also relevant for space applications (even if this is the case for different reasons).

PQ-WireGuard uses a combination of two KEMs, namely Classic McEliece and a passively secure variant of Saber. While SABER is not included in the Round 3 selected PQC algorithms, nor in the Round 4 candidates, it is worth noting how Classic McEliece is used, and the resulting benefits. Specifically, in PQ-Wireguard it is assumed that the long-term public key is pre-shared, and hence, its rather large size does not affect the length of the message. On the contrary, the reduced ciphertext size that it offers, which is 188 bytes for NIST security level 3, makes it rather ideal for such a use case.

9.3. KEMTLS and KEMTLS-PDK: TLS PQC Implementations

KEMTLS (https://kemtls.org/), an alternative for TLS handshake based on PQC KEM, was first presented in ACM CCS 2020; it focuses on server-only authentication (which is the most common case in Web browsing) and it does not rely on pre-shared long-term public-key. It does rely, inevitably, on signatures by certificate authorities to authenticate servers’ long-term KEM keys (the public key and certificate of the root CA is not transmitted during the handshake and assumed to be part of the client’s local trust store). It provides full post quantum security, i.e. including confidentiality and authentication (Schwabe, 2022).

However, KEMTLS has some drawbacks, especially in the client authentication scenario which requires a full additional roundtrip. In addition, there can be a scenario where the available bandwidth is limited, and a server certificate can be pre-shared. For such cases, KEMTLS with pre-distributed public keys can be used (Schwabe, 2021). Pre-distributed public keys may be viable in many scenarios, for example pre-installed public keys in apps, on embedded devices, cached public keys, or keys distributed out of band. Pre-installed public keys in satellites can also be such a scenario. In such cases the employed protocol can be adapted and become more efficient in terms of both bandwidth and computation. This changes also the landscape on suitability of PQC algorithms, where algorithms like Classic McEliece become suitable for long-term key identification (as we also saw in the case of PQ Wireguard).

10. DESIGN CONSIDERATIONS FOR A PQC SPACE PROTOCOL

The Space Data Link Security (SDLS) protocol operates at Layer 2 of OSI offering authentication and/or confidentiality protection to frame data (CCSDS, 2022); an asymmetric PQC protocol for CCSDS should complement SDLS by performing authentication and key exchange (negotiation) for it using an asymmetric cryptographic mechanism.

For space applications bandwidth does matter and the design of a PQC protocol for space should aim at minimising the required bandwidth, as well as the number of required exchanges (round trips). Of course, depending on the specific applications other factors also need to be considered, like available processing power, etc. In terms of protocols, one of the main questions that need to be answered is whether the design could fit everything in unfragmented frames, or whether fragmentation eventually is inevitable. This may also depend on the required security level, which, however, can vary depending on the mission.

Hybrid implementations is rather a must and so, the support of pre-quantum algorithms should also be included. Nevertheless, the overhead is expected to be minimum in comparison with PQC footprint (albeit it could prove to be critical, in case of PQC choices already approaching the limits in terms of sizes).

A critical decision that also needs to be taken is whether a CCSDS asymmetric PQC protocol should be “cryptographically opinionated”, like Wireguard; such a characteristic would contribute significantly to the simplicity and minimalistic form of the designed protocol.

“Transitional security” (i.e. focus on quantum resilient confidentiality only at the beginning) or addressing both post quantum confidentiality and post quantum authentication from the beginning is another trade-off that need to be considered. This is because the “store now decrypt later” threat does not apply to authentication.

Another question is whether there will be a single-side (i.e. “server”) authentication only (the ground segment initiating the connection and the satellite authenticating the ground segment – like is typically the case when TLS is used), or whether mutual authentication is needed (as for instance it is the case of Wireguard).

Finally, as far as the required round trips are concerned, in order to minimise them, modifications to the existing SDLS protocol will probably be needed; on the contrary, if the negotiation and authentication process is added as a separate step, SDLS modifications can be avoided, but additional exchange will be needed.

Characteristics like (perfect) forward secrecy are not discussed since it is taken for granted that need to be supported.

All the above, together with the selection of PQC algorithms that shall be used, constitute the minimum set of the design considerations for defining an asymmetric PQC protocol to complement CCSDS SDLS.

REFERENCES

BSI (2013). BSI TR-03140 (TR-SatDSiG), Technical Guideline SatDSiG - Conformity assessment according to the satellite data security act (SatDSiG), 2013.

BSI (2022a). *Quantum-safe cryptography – fundamentals, current developments and recommendations*, May 2022; available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf

BSI (2022b). BSI TR-02102-1, *Cryptographic Mechanisms: Recommendations and Key Lengths*, January 2022; available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf

Castryck W., Decru T. (2002). An Efficient Key Recovery Attack on SIDH (Preliminary Version); available at https://eprint.iacr.org/2022/975.pdf

CCSDS 355.0-B-2 (2022). *Space Data Link Security Protocol,* CCSDS Recommended Standard, BLUE BOOK, July 2022.

CCSDS 352.0-B-2 (2019). *CCSDS Cryptographic Algorithms,* CCSDS Recommended Standard, BLUE BOOK, August 2019.

ENISA (2021). *Post-Quantum Cryptography, Current state and Quantum Mitigation*, May 3 2021; available at: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

Grover, Lov K. (1996). *A fast quantum mechanical algorithm for database search*. Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing. STOC '96. Philadelphia, Pennsylvania, USA: 212–219. arXiv:quant-ph/9605043.

Hulsing A., et al (2021).. Post-quantum WireGuard, eprint, June 16, 2021; available at https://eprint.iacr.org/2020/379.pdf

RFC 8391 (2018). *XMSS: eXtended Merkle Signature Scheme,* Internet Research Task Force, May 2018. https://www.rfc-editor.org/rfc/rfc8391.html

RFC 8554 (2019). *Leighton-Micali Hash-Based Signatures*, Internet Research Task Force, April 2019. https://www.rfc-editor.org/rfc/rfc8554

Mosca, M. (2018). *Cybersecurity in an era with quantum computers: will we be ready?*, IEEE Security & Privacy (Volume: 16, Issue: 5, September/October 2018), pp.38-41.

Mosca, M., Mulholland, J., *A Methodology for Quantum Risk Assessment, Global Risk Institute*, https://globalriskinstitute.org/publications/3423-2/

Mosca, M. and Piani, M (2019), Quantum Threat Timeline Report, Global Risk Institute, 2019. https://globalriskinstitute.org/download/quantum-threat-timeline-full-report-2/

National Academies (2019). *Quantum Computing: Progress and Prospects*, The National Academy of Science, Engineering, Medicine, The National Academies Press, Washington DC, 2019, http://nap.edu/25196

NIST (2016a). *Announcing request for nominations for public-key post-quantum cryptographic algorithms*, Federal Register 81(244):92787–92788. https://federalregister.gov/a/2016-30615

NIST (2016b). *Submission requirements and evaluation criteria for the post-quantum cryptography standardization process.* Available at https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

NIST (2020). *SP 800-208, Recommendation for Stateful Hash-Based Signature Schemes*, October 2020. https://csrc.nist.gov/publications/detail/sp/800-208/final

NIST (2022a). *Post-Quantum Cryptography Standardization*, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization

NIST (2022b). *Post-Quantum Cryptography - Selected Algorithms 2022,* https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022

NIST (2022c). *Post-Quantum Cryptography – Round 4 Submissions*, 2002, https://csrc.nist.gov/projects/post-quantum-cryptography/round-4-submissions

NIST (2022d). *Post Quantum Cryptography: Digital Signatures – Call for Proposals*, NIST, https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals

NIST (2022e). *Chapter 0 – Forward and Postscript, 2022.* https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/submissions/sike-team-note-insecure.pdf

NISTIR 8105 (2016). *Report on Post-Quantum Cryptography,* NIST, April 2016; http://dx.doi.org/10.6028/NIST.IR.8105

NISTIR 8413 (2022). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, NIST, July 2022; available at: https://www.nist.gov/publications/status-report-third-round-nist-post-quantum-cryptography-standardization-process

Shor, P.W. (1994). *Algorithms for quantum computation: discrete logarithms and factoring*. Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124–134.

Schwabe, P., Stebilla, D., Wiggers, T.(2021). *More Efficient Post-quantum KEMTLS with Pre-distributed Public Keys*, European Symposium on Research in Computer Security ESORICS 2021: Computer Security – ESORICS 2021 pp 3–22; available at: https://thomwiggers.nl/publication/kemtlspdk/

Schwabe, P., Stebilla, D., Wiggers, T.(2022). *Post-Quantum TLS Without Handshake Signatures*, January 3, 2022; available at: https://cryptosith.org/papers/kemtls-20220103.pdf