H. Roßnagel, C. H. Schunck, S. Mödersheim (Hrsg.): Open Identity Summit 2021,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2021 83

How Quantum Computers threat security of PKIs and thus eIDs

Sebastian Vogt[1] and Holger Funke[2]

Abstract: Quantum computers threaten the security of asymmetric cryptography and thus the heart of a PKI - used for example to protect electronic data in passports. On the one hand, there are already promising candidates for post-quantum secure algorithms, but these also have disadvantages (stateful and / or with significantly larger public keys or signatures). On the other hand, there are some application areas for which a PKI should use post-quantum secure procedures as soon as possible. What is the situation regarding PQC in the market for secure, electronic identification (e.g. electronic travel documents)? What needs to be done to prepare electronic travel documents for a post-quantum world?

Keywords: post-quantum cryptography, PQC, quantum-safe, eID, electronic travel document, passport

1 Introduction

So-called quantum computers are subject of research for many years. These computers are not working with usual physics but are using quantum phenomena like superpositions or entanglement. Certain computational problems can be solved much more efficiently on a quantum computer than on a classical computer.

Some of these computational problems are integer factorization and calculating discrete logarithm. Both problems can be solved efficiently on a large-scale quantum computer with Shor´s algorithm, which has been invented by Peter Shor in 1994 [Sh94]. Hence, the currently widespread asymmetric algorithms RSA (security is based on hardness of integer factorization) and elliptic curve cryptography (security is based on hardness of calculating discrete logarithm) can be easily attacked if an attacker has access to a large-scale quantum computer.

Moreover, Lov Grover invented Grover-algorithm in 1996, which is able to search in an unsorted database of size N in square root N iterations [Go96]. Therefore, symmetric cryptographic algorithms can be attacked with Grover´s algorithm on a large-scale quantum computer. However, this will only halve the bit security of symmetric algorithms, so that one can avert this attack by doubling the bit security, e.g. use AES-256 instead of AES-128.

[1] secunet Security Networks AG, Division Homeland Security, Essen, sebastian.vogt@secunet.com
[2] secunet Security Networks AG, Division Homeland Security, Paderborn, holger.funke@secunet.com

Type	Algorithm	Classical bit security	Quantum bit security	Quantum attack
Asymmetric	RSA 2048	112	0	Shor´s algorithm
	RSA 3072	128		
	secp256r1	128		
	secp521r1	256		
Symmetric	AES 128	128	64	Grover´s algorithm
	AES 256	256	128	

Tab. 1: Impacts of quantum computers on bit security

Based on quantum threat timeline report 2020, more than 50% of the experts think that it is unlikely (less than 5%) that the quantum threat will occur within the next 10 years. However, more than 50% of the experts believe that it is 50% or more likely that quantum threat will occur within the next 15 years [MP21]. Hence, if data shall be protected for more than 10 or 15 years, one should already consider how to encrypt or sign them quantum-safe today.

Substantial technological progress in development of quantum computers, as well as the above-mentioned Shor algorithm, raised the need for new asymmetric cryptographic algorithms. Hence, the National Institute for Standard and Technology (NIST) started a process for the development and standardisation of quantum-safe asymmetric algorithms in 2016 [NI16]. Initially the community was asked for proposals of quantum-safe algorithms. Those algorithms have been evaluated in multiple rounds, each of them consisting of a reduced list of candidates. At the end of this process there will be new asymmetric algorithms, which are believed to be secure against attackers with access to both: quantum and classical computers.

In July 2020 NIST announced the end of round two with three remaining third-round finalists as well as three alternative candidates for digital signature algorithms. Moreover, there are four third-round finalists as well as five alternative candidates for public key encryption resp. key establishment algorithms [Al20].

As it´s getting clearer and clearer, which quantum-safe digital signature algorithms might be standardised soon, it is important to start working on the integration of these new algorithms into protocols and applications. This paper discusses how a PKI can issue quantum-safe certificates and why quantum computers threat the security of eIDs. On the one hand, for the most promising quantum-safe algorithms the applicability for PKI is analysed and on the other hand, different ways for transition to quantum-safe certificates are discussed, which includes hybrid ways to combine classical, i.e. RSA or ECC, and quantum-safe algorithms. Furthermore, a prospect of necessary steps, which have to be done before quantum-safe algorithms can be fully used in PKI, is outlined.

2 Post-Quantum Signature algorithms

Several proposals for quantum-safe signature algorithms have been invented. They rely on completely different mathematical principles and they have different characteristics, e.g. statefulness, large signatures or large public keys.

First of all, some stateful hash-based signature algorithms are believed to be quantum-safe. The security of these algorithms relies on the security of the underlying hash function. Two of these algorithms are eXtended Merkle Signature Scheme (XMSS) [Hu18] and Leighton-Micali Hash-Based Signatures (LMS) [MC19]. They have already been standardised in RFC 8301 resp. RFC 8554. Both algorithms are stateful and thus, for each state only one signature is allowed to be calculated. This also implies that the total amount of signatures for one key pair is limited (based on the chosen parameter set this might be around one thousand or one million signatures).

Both XMSS and LMS can in general be used for a PKI. However, for each use case it needs to be precisely evaluated if a hash-based signature scheme is suitable. The Certification Authority (CA) itself is a system in a controlled environment and thus, it should be possible to maintain the state of a hash-based signature scheme appropriately, although the limited amount of signature might be a challenge for certain PKIs if a CA has to issue a lot of certificates. In such a case one should evaluate whether one of the other candidates for quantum-safe signature algorithms might be a better choice.

Besides these two signature algorithms, which are already standardised, several other proposals for quantum-safe signature algorithms have been submitted to NIST process. These candidates rely on different mathematical principles, like lattices or multivariate polynomials. In the following, the three third-round finalists of NIST process will be described and evaluated for their suitability to be used in a PKI.

CRYSTALS-DILITHIUM is a lattice-based signature scheme [Du18]. Its security relies on the hardness of Module Learning With Errors (MLWE) and Module Short Integer Solution (MSIS) problem. Both public keys and signatures are roughly 1-2 KB large and hence relatively balanced, however, a little bit larger than for RSA scheme. Key generation, signing and verification of signatures are very efficient. Based on NIST report on second round, this scheme is slightly favoured compared to the other lattice-based finalist FALCON, since implementation of signing in FALOCON algorithms is complex and might lead to security issues, i.e. revealing of private key [Al20].

FALCON is a lattice-based signature scheme as well [Fo18]. Security of this scheme relies on the hardness of Short Integer Solution (SIS) problem over NTRU rings. Public keys and signature sizes are slightly smaller than for DILITHIUM and overall FALCON has the smallest sum of public key and signature size of all quantum-safe signature schemes in NIST process. Key generation is slower than for DILITHIUM, however, signing and signature verification are very efficient. NIST stated that one of these two lattice-based signature schemes will be most likely selected as the primary post-quantum

signature scheme [Al20].

Both DILITHIUM as well as FALCON generally are good candidates to be used in a PKI. Since both have larger public keys and signatures than currently used RSA and ECC algorithms, certificates will get larger as well. Thus, for each use case it needs to be evaluated if these larger certificates are still suitable.

Another third-round finalist of NIST process is Rainbow, which is a multivariate signature scheme [DS05]. Signature size is very small and both signing and verification of signatures is very fast. However, public keys are very large (approximately 150 KB). Hence, this scheme might not be used in a PKI, since certificates would be too large. Nevertheless, Rainbow is one of the third-round finalists of NIST process, since NIST wants to offer a quantum-safe signature scheme for applications that does not need to send keys often but could benefit from small and fast signatures [Al20].

We can already expect that the lattice-based signature algorithm, which will be selected after round three of NIST process, i.e. DILITHIUM or FALCON, will most likely be the primary signature scheme for quantum-safe PKIs in the future. Besides this lattice-based scheme, we can expect that XMSS or LMS will be used for certain use cases in a PKI, especially in the near future, before NIST process is finished.

Algorithm	Public key size (in bytes)	Signature size (in bytes)
DILITHIUM	1472	2701
FALCON	897	652
Rainbow	157800	66
XMSS	64	2500
LMS	56	2512
RSA-2048	256	256
Secp256r1	32	64

Tab. 2: Overview of public key and signature sizes of some quantum-safe signature algorithms compared to RSA and ECC

3 Integration of Post-Quantum signature algorithms in PKI

Experts are discussing several variants how post-quantum signature algorithms could be integrated into a PKI. Of course, the simplest variant is to just replace the current RSA or ECC algorithm with a post-quantum signature scheme. Besides, there are different variants for hybrid use of pre- and post-quantum algorithms. This chapter describes different variants how a PKI could integrate post-quantum algorithms.

3.1 Quantum-safe Certificates

This variant simply uses a quantum-safe signature algorithm instead of the currently

used RSA or ECC algorithms. This ensures that these certificates are safe against an attacker who has access to a classical as well as a quantum computer.

A disadvantage of this approach is that every application, which needs to verify these certificates, has to migrate to post-quantum algorithms until a specific deadline. Hence, this does not ensure a smooth transition. Moreover, it might turn out in a few years, that the chosen post-quantum scheme can be attacked by either an attacker with access to a classical or quantum computer. In that case the whole PKI would need to be replaced. Another threat could be that even if the algorithm itself is secure, it is a difficult task to develop secure implementations of an algorithm. Either the implementation itself could be attacked or in terms of side channel attacks.

However, there are advantages of this approach as well. First of all, current standards would not need to be changed, only the list of allowed signature algorithms for a specific use case, e.g. like in ICAO Doc 9303 [IA15], would need to be updated. Moreover, size of certificates would increase, but it would not additionally increase, because there are two signatures and two public keys contained.

3.2 Hybrid Certificates

This variant combines both a pre- and post-quantum algorithm. On the one hand, there are two signatures in the certificate, one which is created by a classical signature algorithm and one which is created by a post-quantum signature algorithm. On the other hand, there are also two public keys in the certificate. To be able to store the additional signature and public key in the certificate, the international standard ISO/IEC 9594-8 proposed three X.509 extensions: Alt signature algorithm, Alt signature value and Subject Alt public key [IS20b]. However, ISO/IEC 9495-8 does not define to verify both signatures, but only one of them. Hence, this does not strictly fulfil requirements of a hybrid approach. This approach is illustrated on the left-hand side of Fig. 1.

It is best to create these new X.509 extensions as uncritical. This ensures that applications which are not yet able to process them, can still process the hybrid certificates based on the pre-quantum algorithm. This provides an elegant way for a smooth transition to post-quantum cryptography.

There is at least one additional variant for a hybrid approach to combine a pre- and a post-quantum algorithm. This variant does not use additional X.509 extensions, but just concatenates the second signature after the first signature in the same signature blob. The same will be done for both public keys respectively [OP21]. This approach is actually described for even more than two signatures and public keys, however, since size of certificates increases with each new signature and public key, the combination of one pre- and one post-quantum algorithm is the only practical choice. This is illustrated on the right-hand side of Fig. 1.

This variant implies that all applications, which would like to use these certificates, are

already able to process the used post-quantum algorithm and moreover, they need to be able to parse the signature and public key blob into the corresponding two signatures, respectively two public keys. Hence, this variant does not allow a smooth but rather abrupt transition to post-quantum cryptography.

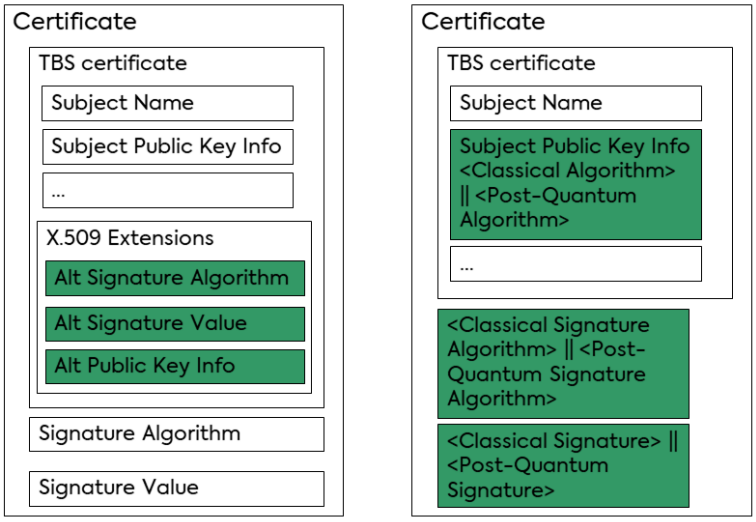

Fig. 1: Hybrid certificates variant 1 (on the left-hand side) and variant 2 (on the right-hand side)

Both variants ensure that these certificates are safe against an attacker who has access to a classical as well as a quantum computer.

A drawback of both variants is that they contain two signatures and two public keys in the same certificate, which enlarges the certificates significantly compared to the currently used ones.

3.3 Parallel Hierarchies

Another variant to combine pre- and post-quantum algorithms for certificates is the use of parallel hierarchies. One PKI hierarchy uses a classical algorithm, e.g. RSA or ECC, while the other PKI hierarchy uses a post-quantum algorithm. Each entity, i.e. each CA and each End-Entity, gets two certificates, one of each hierarchy. This approach is illustrated in Fig. 2.

As long as the classical algorithms can still be assessed as secure, certificates from that classical hierarchy will be used. Optionally, certificates from post-quantum hierarchy can already be validated additionally. As soon as the quantum threat becomes real, only certificates from post-quantum hierarchy will be used. From that time on, each entity will only get new certificates from post-quantum hierarchy.

One advantage of this approach is, that classical algorithms can still be used, as long as the quantum threat is not yet real. However, each entity is already equipped with a quantum-safe certificate, which enables them for the transition to post-quantum cryptography. Hence, this approach does not need an abrupt migration but ensures a smooth transition. Another advantage of this approach is, that each certificate only stores one signature and one public key, so that these certificates are not as large as the hybrid certificates.

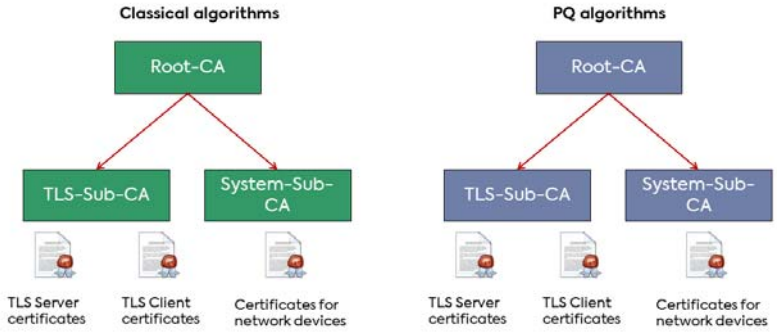

Fig. 2: Parallel PKI hierarchies

3.4 Comparison of different approaches

In the previous subsections different approaches to integrate post-quantum algorithms into certificates have been described. If both signatures are validated in the hybrid approach of subsection 3.2, it is the most secure approach, while just replacing the current algorithms with post-quantum ones as described in subsection 3.1 requires the fewest changes of existing standards. The approach of parallel hierarchies is the most balanced one. The different pros and cons are shown in Tab. 3.

Approach	Advantages	Disadvantages
Quantum-safe certificates	- Only few changes of standards and applications/devices - Only moderate increase of certificate size	- Abrupt migration for all applications at the same time - No fall back in case security or implementation issues are discovered for quantum-safe algorithms in the future
Hybrid certificates (variant 1)	- Smooth transition to quantum-safe certificates - Combines security of pre- and post-quantum algorithms	- Needs changes of standards (e.g. RFC 5280 [Co08]) to store and verify two signatures and two public keys in a certificate - Size of certificates increases

		the most
Hybrid certificates (variant 2)	- Combines security of pre- and post-quantum algorithms	- Abrupt migration for all applications at the same time - Needs changes of standards (e.g. RFC 5280 [Co08]) for two signatures and two public keys in a certificate - Size of certificates increases the most
Parallel hierarchies	- Only few changes of standards and applications/devices - Smooth transition to quantum-safe certificates - Only moderate increase of certificate size	- PKI software needs to be changed to manage parallel hierarchies

Tab. 3: Comparison of different approaches for quantum-safe certificates

4 Impacts on eIDs

Once available, quantum computers will be able to solve certain calculations much faster than today's computers, threatening security algorithms such as RSA and ECC. Various popular protocols like Transport Layer Security (TLS), S/MIME or PGP use cryptography based on RSA or ECC to protect data communication between computers. In this context smart cards play an important role. Smart cards have limited resources and cannot solve large key sizes. A typical smart card, that is used in an eID, has available memory around 80 Kbyte which makes the usage of large PQC resistant key sizes impossible. Another challenge – especially for eID – is the long lifetime of these documents: a usual ePassport has a lifetime of ten years. During these ten years a fundamental change of cryptographic protocols in the field is impossible.

In the field of eID the International Civil Aviation Organization (ICAO) and the German Federal Office for Information Security (BSI) have specified several cryptographic protocols that are used in eID and similar documents. ICAO has specified these protocols in Doc 9303 [IA15] and BSI in the technical guideline TR-03110 [Fe15]. A typical use case of these protocols is to sign the stored data to assure the integrity and authentication. An ePassport includes electronic information (e.g. holder information like name and birthday but also a facial image and fingerprints). This information is signed by a document signer key which is certified by the country signing certification authority (CSCA). CSCAs are root CAs whose self-signed certificates are uploaded into the ICAO public key directory (ICAO PKD) that is similar to an PKI for international exchange of these certificates. The corresponding signer keys are short-term usage keys to sign the electronic information but need to remain secure for the entire lifetime of the

ePassport. This procedure – called Passive Authentication (PA) – uses protocols for signature generation and verification of certificates based on protocols that are affected by quantum computers. ICAO Doc 9303 requires in part 12 the usage of RFC 4055 [Sc05] which specifies two signature mechanisms, RSASSA-PSS and RSASSA-PKCS1_v15. A compromise of this digital signature scheme would mean fake passports and identities could be easily created. That would certainly be a nightmare for States and their border controls.

To assure that only authorized States are able to read sensitive information like fingerprints another protocol is used in context of ePassports called Extended Access Control (EAC). One key role of EAC is Terminal Authentication (TA), where the reading terminal must authenticate itself against the ePassport. And again, TA is based on certificate chains that must be verified by the chip in the ePassport. In [Fe15] you can find the algorithms and key sizes that are currently used in the field and again you can see vulnerable algorithms based on RSA like RSA-v1-5-SHA-256 and RSA-PSS-SHA-256 or ECC-based like secp256r1 or BrainpoolP512r1.

Besides signing data, the encryption and decryption of the communication between the reader and the ePassport is affected by quantum cryptography. The popular protocol Password Authenticated Connection Establishment (PACE) currently uses AES with a key size of 128 bit. As you can see in table 1, this key length is also not quantum-safe.

The trend from smart card based eID documents to mobile and virtual eIDs based on smartphones or wearables might turn out as a solution for the limitations described [Fu20]. But these mobile devices also use a kind of smart card (e.g. Secure Elements (SE) or eUICCs) as a secure hardware token to assure higher eIDAS levels of assurance.

Additionally, these problems are not limited to the area of eID. Smart cards are used in various domains like banking, health, access control etc. Most of these smart card applications are based on the international standard ISO/IEC 7816 [IS20a]. The working group behind this standard (ISO/IEC JTC1/SC17 WG4 “Generic interfaces and protocols for security devices”) recognized this risk and established in 2020 an ad-hoc working group to focus this challenge. The issue of this working group is to identify the concerned algorithms and key size and replace them by PQC-safe algorithms. With this new working group, a first step is done to migrate the eID-ecosystem to a PQC-safe era. But there might be new challenges during this migration, like new side channel attacks of new algorithms or more expensive smart cards.

5 Outlook

Even though the quantum threat is not yet real the transition to post-quantum cryptography should already start today. Most of the data should be secure for 10 or 15 years. Moreover, there are use cases like IoT, in which devices usually have a lifetime of more than 15 years and do not have any possibility to change the cryptographic

mechanism, once the devices are in place. Since most experts estimate a probability of 50% or higher that large-scale quantum computers will be available in 15 years, we should already start the transition to quantum-safe algorithms now.

However, before a PKI can issue quantum-safe certificates, there is still a long way in terms of standardisation and migration. First of all, before further standardisation can take place, the NIST process needs to be finished, except for use cases for which the use of stateful hash-based algorithms is suitable. Afterwards the selected algorithms will be standardised and other standards, which defines cryptographic algorithms for specific use cases (like ICAO Doc 9303 [IA15] or BSI TR-03110 [Fe15]), might adopt them. Moreover, standardised object identifiers (OIDs) need to be defined for those algorithms as well as for stateful hash-based algorithms. Transitions of other cryptographic algorithms, e.g. from DES to AES or from MD5 and SHA-1 to SHA-2, have shown that standardisation of new algorithms and migration of applications usually takes several years or even a decade.

Meanwhile, for some use cases, which are a closed system, transition to post-quantum cryptography can already be started or at least tested. One of these use cases is authentication of firmware updates. German BSI already recommends using stateful hash-based signature schemes for this use case [Fe20]. Since some vendors of Hardware Security Modules (HSM) are already offering these signature algorithms, hardly anything is left to be done before this use case can be implemented quantum-safe.

In our opinion, there is also a strong need to evaluate whether stateful hash-based signature algorithms are suitable for CSCA and Document Signer certificates. Michele Mosca introduced a very picturesque way to evaluate if there is an urgent need for transition to post-quantum cryptography for a specific use case [Mo18]. One needs to take the following three questions into account:

1. How long should your data remain confidential? This is denoted as X.

2. How long will it take to deploy post-quantum cryptography? This is denoted as Y.

3. How long will it take to build a cryptographic relevant quantum computer? This is denoted as Z.

If the sum of X and Y is shorter than Z there is time left to start the transition to post-quantum cryptography. If the sum of X and Y is larger than Z there is a serious security problem. This approach is illustrated in Fig. 3.

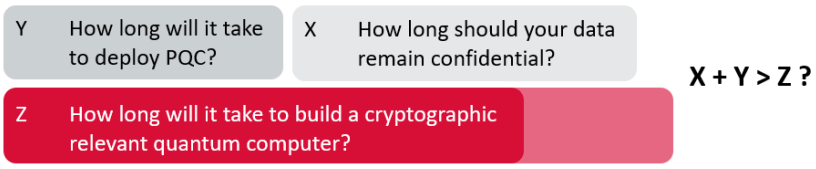

Fig. 3: Do we have to act now?

For the use case of CSCA PKI we know that X is 13 years. As we discussed in Chapter 1 we can assume Z to be 15 years and this is already a rather optimistic interpretation of quantum threat timeline report 2020 [MP21]. This shows that Y should not be larger than two years. Even if ICAO Doc 9303 [IA15] were changed today to use quantum-safe signature algorithms for CSCA and Document Signer certificates from now on, migration of CSCA systems and renewal of corresponding certificates would take more than two years. However, the longer it takes until CSCAs are quantum-safe, the more likely it becomes that passports may not be secure for their whole lifetime of ten years.

Are stateful hash-based signature algorithms suitable for CSCA and Document Signer certificates? Firstly, CSCA and Document Signers are used in a controlled environment so that it should be possible to maintain the state and do not use one state for more than one signature. Secondly, at least the parameter set for about one million signatures should provide enough signatures for that use case. Since these algorithms are believed to be quantum-safe, it is possible to use the approach of quantum-safe certificates as described in Section 3.1 for CSCA PKI hierarchy.

We conclude that there is a strong need for a fast transition to a quantum-safe CSCA PKI hierarchy and that the CSCA PKI hierarchy is suitable for the use of stateful hash-based signature algorithms.

A similar evaluation of the usage of stateful hash-based signature algorithms for PKI hierarchies of other eIDs should be done. However, as discussed in Chapter 2 there are limitations for the usage of stateful hash-based signature algorithms, i.e. number of signatures and statefulness. Hence, migration of PKI hierarchies for other eIDs to post-quantum cryptography might only be possible after NIST process is finished.

Bibliography

[Al20] Alagic, G. et al.: Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NISTIR 8309, US National Institute of Standards and Technology, 2020, DOI: https://doi.org/10.6028/NIST.IR.8309.

[Co08] Cooper, D. et al.: Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile. IETF RFC 5280, 2008

[DS05] Ding, J.; Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme, International Conference on Applied Cryptography and Network Security. Springer, Berlin, Heidelberg, 2005.

[Du18] Ducas, L. et al.: Crystals-dilithium: A lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems: 238-268, 2018.

[Fe15] Federal Office for Information Security (BSI): Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, 2015

[Fe20] Website: Federal Office for Information Security (BSI): Migration zu Post-Quanten-

Kryptografie, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf, accessed: 13/02/2021.

[Fo18] Fouque, P. et al.: Falcon: Fast-Fourier lattice-based compact signatures over NTRU, Submission to the NIST's post-quantum cryptography standardization process 36, 2018

[Fu20] Holger Funke: Digital and mobile Identities. In (H. Roßnagel, C. Schunck, S. Mödersheim, D. Hühnlein, ed.): Open Identity Summit 2020, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020

[Go96] Grover, Lov: A fast quantum mechanical algorithm for database search, Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996

[Hu18] Huelsing A et al.: XMSS: eXtended Merkle Signature Scheme. IETF RFC 8391, 2018

[IA15] ICAO: Doc 9303 Machine Readable Travel Documents, 7th edition, 2015

[IS20a] ISO: ISO/IEC 7816 Identification cards — Integrated circuit cards, 2020

[IS20b] ISO: ISO/IEC 9594:8 Information technology — Open systems interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks, 2020

[MC19] McGrew, D.; Curcio, M.; Fluhrer, S.: Leighton-Micali Hash-Based Signatures, IETF RFC 8554, 2019

[Mo18] Mosca, M.: Cybersecurity in an era with quantum computers: will we be ready?, IEEE Security & Privacy 16.5: 38-41, 2018

[MP21] Website: Global Risk Institute, https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/, accessed: 13/02/2021.

[NI16] Website: National Institute for Standard and Technology: https://www.federalregister.gov/documents/2016/12/20/2016-30615/announcing-request-for-nominations-for-public-key-post-quantum-cryptographic-algorithms, access: 13/02/2021.

[OP21] Ounsworth, M.; Pala, M.: Composite Keys and Signatures For Use In Internet PKI draft-ounsworth-pq-composite-sigs-04. IETF Internet-Draft https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-sigs/, 2021.

[Sc05] J. Schaad, B. Kaliski, R. Housley, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF RFC 4055, 2005.

[Sh94] Shor, P.: Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th annual symposium on foundations of computer science, IEEE, 1994.