H. Roßnagel, S. Mödersheim, C. Schunck (Hrsg.): Open Identity Summit 2021,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2021 205

Analyzing Requirements for Post Quantum Secure Machine Readable Travel Documents

Frank Morgner[1], Jonas von der Heyden[2]

Abstract: In a post-quantum world, the security of digital signatures and key agreements mechanisms used for Machine Readable Travel Documents (MRTDs) will be threatened by Shor's algorithm. Due to the long validity period of MRTDs, upgrading travel documents with practical mechanisms which are resilient to attacks using quantum computers is an urgent issue. In this paper, we analyze potential quantum-resistant replacements that are suitable for those protocols and the ressource-constrained environment of embedded security chips.

Keywords: MRTD; Post-quantum-cryptography

1 Introduction

Quantum computers will reduce the security of most of the cryptographic mechanisms in use today. For symmetric cryptography, Grover's algorithm [Gr96] speeds up searches for the secret key quadratically so that the key size needs to be doubled to keep the pre-quantum security level. The impact on asymmetric cryptography is much greater: Shor's algorithm effectively breaks schemes that are based on factorization or discrete logarithm [Sh99]. Especially for security chips used in identity documents, which typically have a validity period of 10 years, immediate action is required. Produced today, an ID document should still be securely usable in 2031. However, many experts are expecting a sufficiently powerful quantum computer around 2030. This temporal relation is known as "Mosca's Inequality"[Mo15]. Given the time required for standardization and transition to post-quantum secure systems, we need to worry about the impact of quantum computers for the cryptographic protocols used in identity documents.

To alleviate the threat of quantum computers towards cryptography, the US-American National Institute of Standards and Technology (NIST) has initiated a post-quantum cryptography (PQC) competition in 2017. By 2020 this competition has reached its third round with 7 finalists and 8 alternative candidates [Na20a]. In addition, two post-quantum secure hash-based signature schemes have been recommended in NIST SP 800-208 [Na20b] already. The German BSI, too, has started to include post-quantum secure algorithms into their technical guidelines [Bu21].

[1] Bundesdruckerei GmbH, Innovations, Kommandantenstraße 18, 10969 Berlin, Germany
[2] Fraunhofer AISEC, Breite Straße 12, 14199 Berlin, Germany

There are various cryptographic protocols involved in the communication between inspection systems (also called terminals) and MRTD chips (also called chips): Typically, a terminal verifies the machine readable zone of the chip via Password Authenticated Connection Establishment (PACE). This creates an end-to-end encrypted communication channel, which prevents eavesdropping and allows reading the chip's less sensitive data groups. The terminal can then use Passive Authentication to check if the Document Security Object (SOD) is unchanged and thereby verify the integrity of the data groups and of the machine readable zone. Subsequently the terminal can use either Active Authentication or Chip Authentication (version 1, CAv1) to verify the authenticity of the chip. Furthermore, Terminal Authentication (version 1, TAv1) proves the inspection system's authorization to read sensitive data such as the fingerprints [In].

Previous work on post-quantum certificates for MRTs tested how using post-quantum secure signature schemes impacted the document signing PKI [PM20]. This allows the terminal to verify the integrity of less sensitive data with Passive Authentication, but it leaves protocols involving cryptography done by the document's chip an open issue. Additionally, [KV09, GK10] devised post-quantum secure replacements for PAKE (Password authenticated key exchange), which are not suitable for replacing PACE in MRTDs due to lack of efficiency [GK10].

This paper presents intermediate results from the research project PoQuID - Post Quantum ID, which is designed as feasibility study for post-quantum secure identity documents. We analyze the cryptographic building blocks of post-quantum secure Machine Readable Travel Documents with a focus on the protocol steps that require cryptographic operations by the MRTD's chip. Our results show that some protocols can be upgraded with a post-quantum secure drop-in replacement while others need to be completely reworked due to the absence of an efficient, post-quantum secure counter part to the Diffie-Hellman key exchange.

2 Active Authentication and Chip Authentication

To prevent cloning attacks where data from one passport document is duplicated and used in a counterfeit passport, the terminal uses Active Authentication or Chip Authentication [In]. Both protocols verify that the chip is in possession of a secret key stored in secure memory. With Active Authentication, the terminal sends a nonce which gets signed by the chip. The terminal can then verify the signature using the chip's public key, which is secured by Passive Authentication of the Document Security Data.

For Chip Authentication, the chip has a static (elliptic curve) Diffie-Hellman key pair. Its public key is also signed by the document issuer (Passive Authentication). The terminal generates an ephemeral key pair within the same domain parameters as the chip and both compute a shared secret. The shared secret is then authenticated by both parties with a message authentication code (MAC). The advantage over Active Authentication is that the

chip does not need to sign a challenge, which avoids non-repudiation and therefore increases privacy.

Active Authentication can be easily migrated to a post-quantum secure signature scheme, although it is imperative to select this scheme for performance as the signature is generated by the chip. Since there are no Diffie-Hellman-like post-quantum algorithms considered in the NIST standardization process, the key exchange in Chip Authentication needs to be facilitated through a key encapsulation mechanism (KEM). Here, the terminal uses the Chip's public key to encapsulate a session key in a ciphertext, which is sent to the Chip and can be decapsulated by the chip with its private key. If desired, the security of the post-quantum algorithm could be strengthened by adding a conventional and well-tested cryptographic algorithm to the mix through the use of KEM combiners. This would establish hybrid security so that the protocol would be secure even if there is a flaw in the post-quantum algorithm (as long as there is no sufficiently powerful quantum computer).

3 Terminal Authentication

Terminal Authentication is a challenge-response protocol similar to Active Authentication. First, the terminal provides a certificate chain from the Chip's trust anchor to the terminal's certificate. Once the chip has successfully verified the signatures, it generates a challenge, which is signed by the terminal in response.

The signature scheme used in Terminal Authentication can be easily replaced with a post-quantum secure algorithm. The chip, however, needs to verify at least three signatures, one from the terminal and each individual signature from the certificates in the chain (typically with at least two certificates). Therefore the post-quantum secure signature scheme for terminal certificates and terminal signatures needs to be selected for high efficiency of verification. Also, the size of the public keys and signatures needs to be small enough to guarantee an acceptable transfer time when transmitted to the chip via NFC.

Table 1 gives an overview of the cryptographic operations performed by chip and terminal in the protocols described above.

	Chip	Terminal
Active Authentication	Signature creation	Signature validation
Terminal Authentication	Multiple signature validations	Signature creation
Chip Authentication	Key Agreement	Key Agreement, signature validation
Passive Authentication	-	Signature validation

Tab. 1: Overview of cryptographic operations performed by chip and terminal in surveyed MRTD protocols.

4 Post-Quantum Secure Algorithms for MRTD

When choosing the cryptographic schemes that fulfill the requirements given above, two complementary non-functional requirements need to be balanced: performance and robustness. In terms of performance, it has already been shown in [In17, Al18] that the newest generation of smart card chips are capable of running asymmetric post-quantum secure cryptography. For choosing post-quantum alternatives, we assume that the chip runs on a platform similar to the ARM cortex M4 with 50 MHz CPU, AVX2 support, 48 kByte SRAM and 2 Mbyte flash memory, which is a configuration very similar to those used in recent security microcontrollers [In20]. For this theoretical analysis we ignore the overhead of creating an side-channel-free implementation.

In regards to robustness, algorithms need to be secure for the whole lifetime of the document, which is typically 10 years. Therefore we are only considering the round 3 finalists in the NIST PQC competition for use in sovereign documents. More specifically, we are considering algorithms that at least achieve NIST level 1 which represents around 128 bits of classical security. Due to the immaturity of most post-quantum algorithms, the document issuer may want to improve the robustness by integrating a classical algorithm (hybrid security) or by adding an update mechanism to the chip to achieve cryptographic agility (crypto-agility). Both of these additional approaches will not be discussed here.

4.1 Post-Quantum Secure Signature Schemes

While there are three signature schemes considered as finalists for standardization and two hash-based signature schemes already standardized by NIST [Na20b], only two algorithms are considered for the use in identity documents here. This is due to the fact that one finalist (Rainbow) is too inefficient for use in MRTD chips. Moreover, the hash-based schemes are an interesting option for verifying potential cryptographic algorithm updates (crypto-agility), but since they require a state management we ruled them out as the default signature algorithm in MRTD chips. As shown in Table 2, from the two remaining schemes Dilithium and Falcon, Dilithium is preferable due to faster signature creation. This is especially relevant for Active Authentication where the chip has to compute the signatures. In addition, key generation takes much longer in Falcon. As is, the surveyed protocols use static keys, so this should not matter too much, but it is still good to have the option of fast key generation during personalization of the document.

4.2 Post-Quantum KEMs

As shown in Table 1, terminal and chip perform a key agreement in Chip Authentication. Since there is no post-quantum Diffie-Hellman-like key exchange in the NIST competition, the Chip Authentication protocol has to be adapted to use KEMs.

	Dilithium2	Falcon512
Key generation (kCycles)	1,574	171,386
Signature creation (kCycles)	3,970	38,981
Signature size	2.42 kB	657 B
Signature verification (kCycles)	1,599	475

Tab. 2: Benchmarks for post-quantum secure signature schemes (NIST security level 1) on a Cortex-M4 processor [Fr21].

Of the four KEMs that NIST designated as finalists, Classic McEliece can be eliminated right away since its keys are too large to be efficiently transmitted between chip and terminal via NFC. The remaining three contenders are compared to each other in Table 3. For forward security it is imperative to allow for ephemeral keys, especially on the chip. As seen in the table, this requirement rules out NTRU which has very slow key generation. Kyber and SABER on the other hand are very similar across all metrics. Since Kyber and Dilithium share code, we selected Kyber as the KEM for our research project.

	Kyber512	NTRU-HRSS-701	LightSABER
KeyGen (kCycles)	463	153,104	359
Encapsulation (kCycles)	567	377	491
Decapsulation (kCycles)	525	870	464
Ciphertext size	736 B	1.14 kB	736 B

Tab. 3: Benchmarks for post-quantum secure KEMs (NIST security level 1) on a Cortex-M4 processor [Fr21].

5 Conclusion

In our analysis we identified PACE, Terminal Authentication and Chip Authentication as well as the Document PKI and Terminal PKI as components that need to be adapted to make MRTDs post-quantum secure. Subsequently, we identified post-quantum secure algorithms which fulfill the requirements of resource-constrained environments. As shown in section 4, of the finalists competing the NIST PQC competition Dilithium and Kyber are most suited for deployment in MRTDs as signature scheme and KEM, respectively. Another benefit of choosing two lattice-based algorithms is that they may share code (and memory) on the chip and that they may benefit from the same coprocessor capacities. Further research will need to practically evaluate the given estimates, especially considering that there will be varying performance penalties incurred from countermeasures against side-channel attacks. Another interesting question left for further research is how protocols (in this case Chip Authentication) using Diffie-Hellman key exchange can be securely adapted for use with KEMs.

Bibliography

[Al18] Albrecht, M.; Hanser, C.; Hoeller, A.; Poeppelmann, T.; Virdia, F.; Wallner, A.: Implementing RLWE-based Schemes Using an RSA Co-Processor. In: IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019. 2018.

[Bu21] Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie 02102-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI TR-02102-1. Standard, 2021.

[Fr21] Fraunhofer AISEC: , PQDB: A comprehensive benchmark post-quantum cryptography algorithms. https://cryptoeng.github.io/pqdb/, 2021. Accessed: 2021-04-15.

[GK10] Groce, Adam; Katz, Jonathan: A New Framework for Efficient Password-Based Authenticated Key Exchange. In: Proceedings of the 17th ACM Conference on Computer and Communications Security. CCS '10, Association for Computing Machinery, New York, NY, USA, pp. 516–525, October 2010.

[Gr96] Grover, Lov K.: A Fast Quantum Mechanical Algorithm for Database Search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. STOC '96, Association for Computing Machinery, New York, NY, USA, pp. 212–219, July 1996.

[In] International Civil Aviation Organization (ICAO): Doc 9303: Machine Readable Travel Documents. Standard.

[In17] Infineon Technology AG: , Ready for tomorrow: Infineon demonstrates first post-quantum cryptography on a contactless security chip. https://www.infineon.com/cms/en/about-infineon/press/press-releases/2017/INFCCS201705-056.html, 2017. Accessed: 2021-04-15.

[In20] Infineon Technologies AG: , Infineon's Security Solutions Portfolio. https://www.infineon.com/dgdl/Infineon-Security-Solutions-Portfolio-ProductSelectionGuide-v20_02-EN.pdf, 2020. Accessed: 2021-04-15.

[KV09] Katz, Jonathan; Vaikuntanathan, Vinod: Smooth Projective Hashing and Password-Based Authenticated Key Exchange from Lattices. In (Matsui, Mitsuru, ed.): Advances in Cryptology – ASIACRYPT 2009. Lecture Notes in Computer Science. Springer, p. 636–652, 2009.

[Mo15] Mosca, M.: , Cybersecurity in a quantum world: will we be ready? https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf, 2015. Accessed: 2021-04-15.

[Na20a] National Institute of Standards and Technology (NIST): , Post-Quantum Cryptography: Round 3 Submissions. https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions, 2020. Accessed: 2021-04-15.

[Na20b] National Institute of Standards and Technology (NIST): Recommendation for Stateful Hash-Based Signature Schemes, SP 800-208. Standard, 2020.

[PM20] Pradel, Gaetan; Mitchell, Chris J: Post-Quantum Certificates for Electronic Travel Documents. In: Proceedings of DETIPS 2020 (Interdisciplinary Workshop on Trust, Identity, Privacy, and Security in the Digital Economy), September 18 2020. Lecture Notes in Computer Science. Springer, pp. 56–73, December 2020.

[Sh99] Shor, Peter W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Review, 41(2):303–332, Jan 1999.