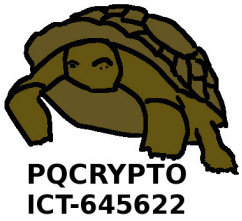

PQCRYPTO

Post-Quantum Cryptography for Long-Term Security

Project number: Horizon 2020 ICT-645622

D5.2

Standardization: Final report

Due date of deliverable: 28. February 2018
Actual submission date: 09. April 2018

WP contributing to the deliverable: WP5

Start date of project: 1. March 2015 Duration: 3 years

Coordinator:
Technische Universiteit Eindhoven
Email: coordinator@pqcrypto.eu.org
www.pqcrypto.eu.org

Revision 1.6

Project co-funded by the European Commission within Horizon 2020		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission services)	

Standardization: Final report

Walter Fumy, Frank Morgner, Andreas Hülsing

09. April 2018
Revision 1.6

The work described in this report has in part been supported by the Commission of the European Communities through the Horizon 2020 program under project number 645622 PQCRYPTO. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Abstract

This report discusses ongoing standardization activities in the area of post-quantum cryptography and achievements towards the objectives of Work Package 5 of PQCRYPTO in the entire project period.

Keywords: Standardization, ANSI, ETSI, IEEE, IETF, IRTF, FIPS, ISO, NIST

Contents

1 Introduction

During and after completion of PQCRYPTO, the project team envisions substantial efforts being undertaken in building a portfolio of standardized post-quantum algorithms and protocols, in upgrading security standards (such as SSL, IPsec, the EMV standard, eID cards, ...) and their recommended implementations, in incorporating post-quantum cryptography into training materials for new cryptographers, and in general in bringing post-quantum cryptography to the same level of maturity as RSA, DSA, and elliptic-curve cryptography. Work Package 5 of PQCRYPTO is to support this transformation and has the following main objectives:

- Make PQCRYPTO visible towards the scientific community as well as other stakeholders, such as policy makers and industry. This is done by elaborating and providing dissemination material by which the project's results are submitted for consideration by international standardization bodies such as ISO, ETSI or IEEE.
- Organize the project's standardization activities which are relevant both for communicating the project's outcomes and getting valuable feedback from standardization expert groups.

The activities of this work package are organized in 2 tasks that together cover the whole duration of the project.

Task 5.1 (M0–M24): Selection of algorithms.

- The purpose of this task is to select a portfolio of cryptographic algorithms and protocols to be considered later for submission to standardization groups. Given the diversity of potential candidates, the task will define a list of categories as well as technical requirements that the candidate mechanisms shall fulfill, such as security and performance with respect to their best known hardware and software implementations.

Task 5.2 (M0–M36): Operational standardization activities.

- This task coordinates actions undertaken in standardization groups. It is meant to identify promising standardization bodies (ISO/IEC SC27, IEEE P1363, ETSI, etc.), mandate liaison officers to connect the project to relevant working groups in these bodies, coordinate their actions through a roadmap of actionable objectives, and organize follow-up meetings and internal reporting to partners.

This report focuses on activities within task 5.2 and discusses ongoing standardization activities in the area of post-quantum cryptography and achievements towards the objectives of Work Package 5 of PQCRYPTO.

2 Selected Activities towards Standardization of Post-Quantum Cryptography

2.1 Introduction

In the past years, a large community has emerged to address the issue of information security in a quantum computing future. In the academic world, "Post-Quantum Cryptography"

has established itself as an active area of research with its own conference series. These efforts have led to advances in fundamental research, paving the way for the consideration of post-quantum cryptosystems in industry and standards development organizations (SDOs). Several SDOs have started their own activities in this field. The following sections provide an overview over SDOs with particular activities in the area of post-quantum cryptography.

It is worth noting that recently, post quantum cryptography has also gained increased attention from industry. For example, Google has integrated a post quantum secure key exchange mechanism into both, the development version of their web browser (Chrome Canary) and into some of their web servers (e.g. `https://play.google.com/store`) [10]. The algorithm identified as "CECPQ1" combines "New Hope" [1], a post-quantum key exchange developed by members of PQCRYPTO and others, with X25519, an elliptic curve based Diffie-Hellman key agreement scheme. This hybrid approach guarantees backward compatibility and is fully integrated into the Internet's transport layer security protocol TLS. Also, Microsoft has published SIDH, a software library implementing a suite of Supersingular Isogeny Diffie-Hellman key exchange algorithms [16]. Though these initiatives are promising and show the feasibility of integration into existing standards, these projects are marked as research experiment with a limited lifetime. Furthermore, these initiatives underline the need for standardization to achieve interoperability, hence we focus on SDO activities rather than on research or industry activities.

2.2 ETSI

ETSI, the European Telecommunications Standards Institute, produces standards for Information and Communications Technologies (ICT). Examples include standards for GSM, DECT, Smart Cards and electronic signatures. ETSI is a not-for-profit organization with more than 800 member organizations worldwide and officially recognized by the European Union as a European Standards Organization.

ETSI produces a variety of standards, specifications and reports to suit different purposes. Types of deliverables include European Standard (EN), ETSI Standard (ES), ETSI Guide (EG), ETSI Technical Specification (TS), and ETSI Technical Report (TR). ETSI standards are available free of charge (`www.etsi.org`), access to draft deliverables is restricted.

In the area of post-quantum cryptography, the following ETSI activities are noted:

- ETSI, in partnership with the Institute for Quantum Computing (IQC), has held five "Quantum-Safe Cryptography" Workshops since 2013. These Workshops took place in Sophia Antipolis, France, 26 to 27 September 2013, in Ottawa, Canada, 6 to 7 October 2014, in Seoul, Korea, 5 to 7 October 2015, in Toronto, Canada, 19 to 21 September 2016, and in London, UK, 13 to 15 September 2017.

  The PQCRYPTO project had a strong footprint in these workshops, giving presentations introducing the project at all workshops since its start and presenting several results. Workshop proceedings are available online.

- In October 2014, ETSI has published a White Paper "Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges" [14] summarizing security considerations in view of quantum computing and discussing challenges of a transition from today's cryptographic infrastructure to a quantum-safe or post-quantum infrastructure. Note that the term quantum-safe includes quantum cryptography, in particular quantum key distribution (QKD). In particular, the ETSI White

Paper discusses security and performance aspects of the following families of quantum-safe cryptosystems:

  - Quantum key distribution (QKD)
  - Code-based cryptosystems
  - Lattice-based cryptosystems
  - Hash-based cryptosystems
  - Multivariate cryptosystems

- In March 2015, ETSI has launched a Quantum-Safe Cryptography (QSC) Industry Specification Group (ISG) (http://www.etsi.org/qsc). QSC projects include
  - DSG/QSC-001: Quantum-safe algorithmic framework

    This document gives an overview of the current understanding and best practices in academia and industry about quantum-safe cryptography (QSC). It focuses on identifying and assessing quantum-safe cryptographic primitives that have been proposed for efficient key establishment and authentication applications, and which may be suitable for standardization by ETSI and subsequent use by industry. It also describes an assessment framework and provides a preliminary discussion of key sizes.
    The assessment framework states that ETSI ISG-QSC will assess candidate cryptographic primitives for suitability against a number of criteria, grouped under the headings of security, efficiency and deployment considerations.
  - DSG/QSC-002: Cryptographic primitive characterization

    In this document, a range of proposed quantum-safe cryptographic algorithms across all classes of quantum-safe cryptographic algorithms are studied in-depth, with particular attention paid to ease of use and security aspects.
  - DSG/QSC-003: Cryptographic primitive suitability assessment
  - DSG/QSC-004: Quantum-safe threat assessment

    This document presents a quantitative threat assessment for a number of use cases. It makes a number of assumptions regarding the timescale for the deployment of viable quantum computers, and discusses the impact of quantum computing on various scenarios.
  - DSG/QSC-006: Fundamental limits of quantum computing applied to cryptography
  - DSG/QSC-007: Quantum safe key exchanges QSC-KEX

    This document provides a comparison of quantum-resistant key establishment schemes and discusses security, efficiency, parametrization and implementation aspects.
  - DSG/QSC-008: Quantum safe signatures

    This document provides a comparison of quantum-resistant signature schemes and discusses security, efficiency, parametrization and implementation aspects.

– DSG/QSC-009: Quantum Safe Virtual Private Networks (QSC-VPN)

  This document discusses the impacts of integrating quantum safe algorithms into VPN technologies. This includes a discussion of the use of hybrid schemes to allow efficient and practical use of traditional cryptography with quantum safe cryptography. Recommendations will include protocol changes, algorithm formats, efficiency and implementation considerations.

– DSG/QSC-013: Migration strategies and recommendations to Quantum-Safe schemes

  This document presents recommendations and guidelines for users seeking to adopt a QSC model and who will need to migrate from an existing non-QSC environment. The guidance will discuss both the high level strategic and lower level practical issues to be considered for migration from non-QSC to QSC algorithms and key management.

As of March 2018, several of the DSG-QSC projects have resulted in a publication. ETSI Group Reports were published on projects DSG/QSC-001 [4], DSG/QSC-003 [5], DSG/QSC-004 [6] and DSG/QSC-006 [7], while project DSG/QSC-007 resulted in ETSI Technical Report 103 570 [8].

Furthermore, ETSI TC Cyber has published an ETSI Guide [3] addressing aspects of business continuity arising from the concern that Quantum Computing is likely to invalidate the problems that lie at the heart of both RSA and ECC asymmetric cryptography. In particular this guide discusses the transition to the post-quantum era, how to re-assert CAs in a PKI infrastructure, the distribution of new algorithms, and the distribution of new keying material.

2.3 NIST

NIST, the U.S. National Institute of Standards and Technology, is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's *Computer Security Resource Center* (CSRC) provides a well-established resource for information security standards and guidelines (`http://www.csrc.nist.gov`) with international recognition. Types of deliverables include *Federal Information Processing Standards* (FIPS) and *Special Publications* (SP). NIST publications are available free of charge; draft deliverables are published for review and comment.

In the area of post-quantum cryptography, the following NIST activities are noted:

- In April 2015, NIST has held a Workshop on *Cybersecurity in a Post-Quantum World*. The workshop discussed issues related to post-quantum cryptography and its potential future standardization. The PQCRYPTO project had a strong footprint in this workshop and presented several papers. Workshop proceedings are available online.

- In April 2016, NIST has published NIST Interagency Report[1] (NISTIR1) 8105: Report on Post-Quantum Cryptography [22]. In this report, NIST shares its view about the status of quantum computing and post-quantum cryptography. Based on the perceived impact of large scale quantum computers on common crypto algorithms (see Figure 2.1), the report identifies the challenge of moving to new cryptographic infrastructures and stresses the need for industry and governments to manage crypto agility. In addition,

[1] NIST Internal or Interagency Reports (NISTIRs) describe research of a technical nature of interest to a specialized audience.

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Figure 2.1: Impact of quantum computers on common crypto algorithms (source: [22])

the report outlines NIST's action plan for initiating standardization efforts in the field of post-quantum cryptography (some of this changed based on discussions in 2017):

- As a first step, NIST specified preliminary evaluation criteria for quantum-resistant public key cryptography standards. NIST is looking for a long term solution to attacks from quantum computing excluding "hybrid modes"[2] from the competition as well as algorithms that contain major components that are not quantum secure. All patents and the conditions of their use have to be made explicit by their authors. Restrictions for using a patent must be free of unfair discrimination and may or may not include a compensation to the patent holders. The draft criteria were released for public comment in August 2016 [23]. The PQCRYPTO project actively participated in the discussion of these criteria and made several official comments as documented on the official NIST pqc-forum mailinglist.

  1. Security is evaluated in terms of how the algorithms can be used as alternatives within existing standards, their security model and in terms of target security strength. NIST doesn't require submitters to give security proof of their algorithms. For public key cryptography, NIST is primarily concerned with attacks that use classical (rather than quantum) queries to oracles and names indistinguishability under adaptive chosen ciphertext attacks ("IND-CCA2") for encryption and existential unforgeability under adaptive chosen message attacks ("EUF-CMA") for signatures that the algorithms should provide. NIST defines five target security strengths ranging from 128 bits classical security and 64 bits quantum security to 256 bits classical security and 128 bits

[2] "Hybrid Mode" algorithms are created from both, a post-quantum algorithm and an established pre-quantum algorithm. For example, a digital signature consists of two signatures, which both must be verified. This approach guarantees security as long as at least one scheme is secure. That way, the introduction of new schemes does not harm security.

quantum security. NIST defines the computational complexity based on brute force attacks against block ciphers and hash functions and later plans to define units for measuring computational complexity, memory requirements etc., taken the best quantum attack (Grover's algorithm) into account. Additional security properties such as perfect forward secrecy, resistance to side channel attacks and resistance to multi-key attacks and even resistance to misuse are also desirable features.

2. NIST will continually seek public input regarding performance metrics in terms of costs of a public-key cryptosystem. Currently, sizes of public keys, ciphertexts and signatures are in scope as well as computational cost in hardware and software.
3. Flexibility to achieve additional functionality and design simplicity is also desired.

– As a second step, NIST intends to select at least one candidate algorithm providing the functionality of quantum-resistant public key encryption, of quantum-resistant digital signatures, and of quantum-resistant key establishment for standardization. NIST set the submission deadline to November 2017 for algorithms to be considered, and expects the proposals to be subject to 3 to 5 years of public scrutiny before they are standardized[3].

- In December 2016, NIST formally announced its Call for Proposals ("Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms"[4]) and set November 30, 2017 as deadline for submission.

  – With this call, NIST is soliciting proposals for post-quantum digital signature as well as public key encryption / key encapsulation mechanisms and it will solicit comments from the public as part of its evaluation process. NIST expects to perform multiple rounds of evaluation, over a period of three to five years. The goal of this process is to select a number of acceptable candidate cryptosystems for standardization.

  – NIST anticipates that the evaluation process for these post-quantum cryptosystems will be significantly more complex than for previous competitions, e.g. in the area of hash functions or symmetric encryption algorithms. As a result of these complexities, NIST believes that its post-quantum standards development process should not be treated as a competition. NIST will perform a thorough analysis of the submitted algorithms in a manner that is open and transparent to the public, as well as encourage the cryptographic community to also conduct analyses and evaluation. This combined analysis will inform NIST's decision on the subsequent development of post-quantum standards.

- In response to the call, NIST has received a total of 82 submissions from 25 coun-

[3] While NIST's process for standardizing quantum-resistant public key cryptography has commonalities with the processes that led to the standardization of AES [19] and SHA3 [21], this is not a competition. Rather it is similar to the ongoing block cipher modes development process [20] and NIST sees its role as managing a process of achieving consensus in the crypto-community in a transparent manner.

[4] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization/Call-for-Proposals

tries, among them 23 signature schemes and 59 encryption/key establishment mechanisms [17]. Table 2.3 shows a breakdown of the initial schemes received.

	Signatures	KEM / Encryption	Total
Lattice-based	4	24	28
Code-based	5	19	24
Multi-variate	7	6	13
Hash-based	4	0	4
Other	3	10	13
Total	23	59	82

Table 2.1: Initial NIST submissions (source: [17])

  - Thirteen of the submissions received failed to meet the formal criteria specified by NIST and thus were not included in NIST's initial posting of round 1 algorithms.
  - As of March 28, 2018 four of the remaining 69 submissions have been withdrawn.

- April 11-13, 2018, NIST organizes a First PQC Standardization Conference.

2.4 ANSI

ANSI, the American National Standards Institute is the main voice of the U.S. standards and conformity assessment system and as such represents the U.S: within ISO. The Accredited Standards Committee X9 (ASC X9, `http://www.x9.org`) is the ANSI accredited standards developing organization responsible for the development of financial services standards. ASC X9 is composed of four Subcommittees, with X9F responsible for Data & Information Security.

In 2010, the ASC X9F Working Group X9F1 has specified NTRU, a lattice-based key establishment algorithm for the financial services industry in [2]. NTRU-based schemes use a specific class of lattices that have an extra symmetry, resulting in performance and key size advantages over other lattice-based schemes.

2.5 IEEE

The Institute of Electrical and Electronics Engineers (IEEE, `http://www.ieee.org`) is a large organization of technical professionals with more than 420.000 members in over 160 countries. IEEE publishes a substantial fraction of the world's technical literature in electrical engineering, computer science, and electronics and is a leading developer of international standards. The current portfolio consists of nearly 1,300 standards and projects under development.

IEEE P1363 is an IEEE standardization project (`http://grouper.ieee.org/groups/1363/`) for public-key cryptography which resulted in specifications for traditional public-key cryptography (IEEE Std 1363-2000 and 1363a-2004), lattice-based public-key cryptography (IEEE Std 1363.1-2008), password-based public-key cryptography (IEEE Std 1363.2-2008), and identity-based public-key cryptography using pairings (IEEE Std P1363.3-2013).

In 2008, IEEE standardization project P1363 has specified NTRU in [24][5]. IEEE Std 1363.1-2008 provides specifications of several public key cryptographic techniques based on

[5]Note that the chair of the IEEE P1363 working group is William Whyte of NTRU Cryptosystems, Inc. (now part of OnBoard security), who has been serving as chairman since August 2001. Former P1363 working group chairs were Ari Singer, also of NTRU (1999-2001), and Burt Kaliski of RSA Security (1994-1999).

hard problems over lattices, including primitives for key establishment, public-key encryption, authentication and digital signatures, as well as cryptographic schemes based on those primitives. Specifications of related cryptographic parameters, including public and private keys are also provided.

2.6 IETF and IRTF

The *Internet Engineering Task Force* (IETF, http://www.ietf.org) is an international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture. In contrast to other SDOs, the IETF is open to any interested individual.

The technical work of the IETF is done in Working Groups, which are organized by topic into several areas, security being one of the areas. The IETF Standards Process is described in several RFCs [13]. While the IETF focuses on shorter term issues of engineering and standardization, the parallel organization Internet Research Task Force (IRTF, http://www.irtf.org) focuses on longer term research topics related to the Internet. The IRTF is a composed of a number of long-term Research Groups. Participation is by individual contributors, rather than by representatives of organizations. Currently there are ten research groups, including CFRG, the *Crypto Forum Research Group*.

The CFRG aims to bridge between theory and practice by bringing new cryptographic techniques to the Internet community and promoting an understanding of the use and applicability of these mechanisms via Informational RFCs. Topics of discussion include post-quantum cryptography.

As of August 2016, several Internet-Drafts[6] specifying post-quantum mechanisms or providing guidance for quantum-safety exist, so far none of the projects has resulted in an RFC, however, some have been adopted by a working group. Current activities include

- **Hash-based signatures (1)**
  An Internet-Draft co-authored by members of PQCRYPTO in the domain of hash-based signatures describes the eXtended Merkle Signature Scheme (XMSS) [12]. The Internet-Draft was adopted by CFRG and, at the time of writing, is in the RFC-editor queue. This is the last step in the process of becoming an RFC and is a pure editorial step. The document specifies the WOTS+ one-time signature scheme and two variants of XMSS, a single-tree (XMSS) and a multi-tree variant (XMSS^{MT}). Both variants use WOTS+ as a main building block. XMSS provides digital signatures only relying on the properties of cryptographic hash functions. The schemes provide strong security guarantees even when the collision resistance of the underlying hash function is broken. The schemes are claimed to be suitable for compact implementations, are relatively simple to implement, and naturally resist side-channel attacks. The schemes are considered to resist quantum attacks as generic attacks against hash functions at most achieve a square-root speed-up.

- **Hash-based signatures (2)**
  A second Internet-Draft in the domain of hash-based signatures [15] describes the Leigthon-Micali signature scheme (LMS). The Internet-Draft was adopted by CFRG.

[6] Note that Internet-Drafts have no formal status, and are subject to change or removal at any time (http://ietf.org/iesg/statement/removal-of-an-internet-draft.html); therefore they should not be cited or quoted in formal documents. Anyone can submit Internet Drafts and the drafts do not necessarily have any standing in the IETF unless, adopted by a working group or approved as a RFC.

The document specifies both a one-time signature scheme and a general signature scheme. As for [12], the schemes are claimed to be suitable for compact implementations, are relatively simple to implement, and naturally resist side-channel attacks. The schemes are considered to resist quantum-attacks for the same reasons as [12].

- **Quantum-safe hybrid TLS cipher-suite**
  A current Internet-Draft describes a quantum-safe hybrid cipher suite for the Transport Layer Security (TLS) protocol version 1.3 [27]. This cipher suite specifies the use of the NTRUEncrypt encryption scheme in combination with RSA/DH for key establishment in the TLS handshake. The mechanism uses a hybrid approach that combines the classical handshake mechanism with key encapsulation instantiated with quantum-safe encryption schemes.

- **Selection criteria for quantum-safe hybrid cryptography**
  The *quantum-safe hybrid* concept is a modular approach, allowing any authenticated key establishment mechanism to be protected against "harvest-then-decrypt" attacks by exchanging additional secret material protected with an ephemeral key for a quantum-safe public key cryptographic algorithm and including that secret material in the Key Derivation Function (KDF) run at the end of the key establishment protocol. Such an approach has been proposed for TLS in [27]. A current Internet-Draft provides a guideline to criteria for selecting public key encryption algorithms approved for experimental use in the quantum safe hybrid setting [26].

- **Key establishment**
  This Internet-Draft describes an extension of the Internet key exchange protocol IKEv2 to allow it to be post quantum [9]. The scheme is based on pre-shared keys.

- **Terminology of quantum computing and its effect on classical cryptography**
  This Internet-Draft [11] aims at describing quantum computing in general and how it might be used to attack classical cryptographic algorithms. Specifically, properties of quantum computers are described as well as Shor's and Grover's algorithm.

2.7 ISO and ISO/IEC JTC 1/SC 27

ISO, the *International Organization for Standardization* (`http://www.iso.org`) is the largest international SDO with a membership of more than 160 national standards bodies, one per country. ISO has published beyond 21.000 International Standards and related documents, covering almost every sector. More than 3.300 technical bodies take care of standards development and maintenance. These technical bodies are hierarchically organized in Technical Committees (TCs), Subcommittees (SCs), and Working Groups (WGs). In the area of information technology, ISO and the *International Electrotechnical Commission* (IEC) have created a Joint Technical Committee, ISO/IEC JTC 1 *Information Technology*.

ISO/IEC JTC 1/SC 27 *IT Security Techniques* was established in 1990 and over the years has become an internationally recognized center for information and IT security standardization. Membership of SC 27 consists of more than 50 voting countries and about 20 observing countries. SC 27 also collaborates with over 70 liaison organizations world-wide. Since its establishment, SC 27 has published more than 150 security and privacy standards, including a range of bestselling standards, e.g., those belonging to the ISMS family of ISO/IEC

27000 standards, standards for the security evaluation of products and systems (ISO/IEC 15408), and various standards covering cryptographic techniques such as ISO/IEC 10118 on hash-functions, ISO/IEC 18033 on encryption algorithms, ISO/IEC 9796 and ISO/IEC 14888 on digital signatures, ISO/IEC 11770 on key management, ISO/IEC 19772 on authenticated encryption, and ISO/IEC 29192 on lightweight cryptography.

In October 2015, SC 27 Working Group 2 *Cryptography and other security mechanisms* created a Study Period to investigate the area of post-quantum cryptography and to prepare standardization activities of SC 27 in the field (see also Section 3.4). During the study period several rounds of contributions were initiated and analyzed. At the November 2017 meeting in Berlin it was agreed to terminate the study period and to initiate a Standing Document (WG 2/SD 8) on quantum resistant cryptography. Different chapters will cover different families of algorithms. Members of PQCRYPTO are part of the editor team.

2.8 German Federal Office for Information Security (BSI)

The BSI's Technical Guideline SatDSiG specifies conformity assessment according to the German Satellite Data Security Act. Highly capable space-based earth remote sensing satellites are constructed in Germany with the intention of the worldwide commercial marketing of the acquired images and data. SatDSiG gives guidance for conformity evaluation facilities to perform assessments of IT-security measures of high grade Earth Observations Systems (EOS). Among others, the Technical Guidelines make evaluation of the crypto concept obligatory. For the cryptographic security mechanisms only algorithms endorsed by BSI shall be used. The long operational life-time of a high grade EOS from the design-phase until the end of mission ($\approx$ 15 years) has to be taken into account for selection of the algorithms as well as the target life time of the encrypted data. BSI specifically mentions Merkle-signature as example for securing update-able crypto modules. The Technical Guideline TR-02102 recommends algorithms and key-lengths. It directly references definitions and parameters of XMSS [12].

3 PQCRYPTO Outreach to SDOs

From the beginning, the PQCRYPTO project was actively involved in a number of standardization activities in the area of post-quantum cryptography. In many cases, project members contributed to workshops organized by SDOs, or submitted PQCRYPTO recommendations to relevant SDO activities, such as study periods.

This section provides an overview over PQCRYPTO outreach activities to relevant SDOs for the period covered (M0–M36).

3.1 ETSI

As mentioned in Section 2.2, the PQCRYPTO project had a strong footprint in ETSI's "Quantum-Safe Cryptography" Workshops and presented several papers.

At ETSI's "3rd Quantum-Safe Cryptography Workshop" which took place 5 to 7 October 2015 in Seoul, South Korea, Andreas Hülsing gave two talks. In the first talk he introduced PQCRYPTO and presented the initial algorithm recommendations of PQCRYPTO. In the second talk, he presented on the ongoing standardization of hash-based signatures within IRTF's crypto forum research group (CFRG) in which he signs responsible for one Internet draft on behalf of PQCRYPTO.

Fumy and Morgner have successfully submitted a paper "Is PQ-Crypto ready for Standardization" to ETSI's "4th Quantum-Safe Cryptography Workshop" which took place 19 to 21 September 2016 in Toronto, Canada and Andreas Hülsing gave an invited presentation on the PQCRYPTO results and positions.

At the "5th Quantum-Safe Cryptography Workshop" which took place in London, UK, 13 to 15 September 2017, Andreas Hülsing gave another invited presentation on recent PQCRYPTO results and updated positions.

3.2 NIST

As mentioned in Section 2.3, the PQCRYPTO project had a strong footprint in NIST's Workshop on "Cybersecurity in a Post-Quantum World", presented several papers and participated in panel discussions as panelists. PQCRYPTO also used this workshop to announce the existence of the project with a presentation and a press release. Workshop proceedings are available online.

Furthermore, the PQCRYPTO project was involved in a substantial number of submissions in response to NIST's Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms. Members of the project contributed to the following submissions (in alphabetical order):

Encryption:

- BIG QUAKE (BInary Goppa Quasi–cyclic Key Encpasulation)
  by Alain Couvreur, Magali Bardet, Elise Barelli, Olivier Blazy, Rodolfo Canto-Torres, Philippe Gaborit, Ayoub Otmani, Nicolas Sendrier, Jean-Pierre Tillich.

- BIKE: Bit Flipping Key Encapsulation
  by Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillipe Gaborit, Shay Gueron, Tim Güneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Gilles Zemor.

- Classic McEliece
  by Daniel J. Bernstein, Tung Chou, Tanja Lange, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Wen Wang.

- CRYSTALS-Kyber
  by Peter Schwabe, Roberto Avanzi, Joppe Bos, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, Damien Stehle.

- DAGS: Key Encapsulation using Dyadic GS Codes
  by Gustavo Banegas, Paolo S. L. M. Barreto, Brice Odilon Boidje, Pierre-Louis Cayrel, Gilbert Ndollane Dione, Kris Gaj, Cheikh Thiecoumba Gueye, Richard Haeussler, Jean Belo Klamti, Ousmane N'diaye, Duc Tri Nguyen, Edoardo Persichetti, Jefferson E. Ricardini.

- FrodoKEM - Learning with Errors Key Encapsulation
  by Michael Naehrig, Erdem Alkim, Joppe Bos, Leo Ducas, Karen Easterbrook, Brian

LaMacchia, Patrick Longa, Ilya Mironov, Valeria Nikolaenko, Christopher Peikert, Ananth Raghunathan, Douglas Stebila.

- KINDI
  by Rachid El Bansarkhani.
- NewHope
  by Thomas Pöppelmann, Erdem Alkim, Roberto Avanzi, Joppe Bos, Leo Ducas, Antonio de la Piedra, Peter Schwabe, Douglas Stebila.
- NTRU-HRSS-KEM
  by John M. Schanck, Andreas Hülsing, Joost Rijneveld, Peter Schwabe.
- NTRU Prime
  by Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, Christine van Vredendaal.
- Post-quantum RSA-Encryption
  by Daniel J. Bernstein, Josh Fried, Nadia Heninger, Paul Lou, Luke Valenta.
- Ramstake
  by Alan Szepieniec.
- SABER
  Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, Frederik Vercauteren.

Signatures:

- CRYSTALS-Dilithium
  by Vadim Lyubashevsky, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehle.
- GUI
  by Jintai Ding, Ming-Shen Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang.
- LUOV
  by Ward Beullens, Bart Preneel, Alan Szepieniec, Frederik Vercauteren.
- MQDSS
  Simona Samardjiska, Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Peter Schwabe.
- Picnic
  by Greg Zaverucha, Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig.
- Post-quantum RSA-Signature
  by Daniel J. Bernstein, Josh Fried, Nadia Heninger, Paul Lou, Luke Valenta.
- qTESLA
  by Nina Bindel, Sedat Akleylek, Erdem Alkim, Paulo S. L. M. Barreto, Johannes Buchmann, Edward Eaton, Gus Gutoski, Juliane Krämer, Patrick Longa, Harun Polat, Jefferson E. Ricardini, Gustavo Zanon.

- Rainbow
  by Jintai Ding, Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang.
- SPHINCS+
  by Andreas Hülsing, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe.

All submissions are available on the homepage of the NIST post-quantum cryptography project. The PQCRYPTO project also already contributed significantly to the evaluation of submitted algorithms, which started with the publication of the algorithms on 21 December 2017. PQCRYPTO members presented the following attacks (sorted alphabetically) on 11 algorithms from the initial set of published algorithms:

- DME, reduced security.
  Attack by Ward Beullens.
- Edon-K, full break, withdrawn.
  Attacks by Matthieu Lequesne, Nicolas Sendrier, Jean-Pierre Tillich.
- Giophantus, attack on ring choice.
  Attack by Wouter Castryck and Frederic Vercauteren.
- Guess Again, full break.
  Attack by Lorenz Panny.
- HILA5, IND-CCA broken.
  Attack by Daniel J. Bernstein, Leon Groot Bruinderink, Tanja Lange, Lorenz Panny.
- HK17, full break, withdrawn.
  Attack by Daniel J. Bernstein, Tanja Lange.
- RaCoSS, full break.
  Attack by Daniel J. Bernstein, Andreas Hülsing, Tanja Lange, Lorenz Panny.
- RankSign, full break, withdrawn.
  Attack by Thomas Debris-Alazard and Jean-Pierre Tillich.
- RVB, full break, withdrawn.
  Attack by Lorenz Panny.
- SRTP1, full break, withdrawn.
  Attack by Daniel J. Bernstein, Tanja Lange, Bo-Yin Yang.
- Walnut DSA, full break for all submitted parameters.
  Attack by Ward Beullens, Simon R. Blackburn.

These attacks are all documented on the official NIST pqc-forum mailinglist.

3.3 IETF

The PQCRYPTO project has stimulated the discussion of post-quantum cryptography in IRTF's CFRG and has submitted an Internet-Draft on hash-based signatures (see also Section 2.6). Moreover, members of the PQCRYPTO project developed a boilerplate for post-quantum cryptography standardized within IETF/IRTF which has to be used for all future RFCs on post-quantum cryptography in the foreseeable future.

3.4 ISO/IEC JTC 1/SC 27

Noting the post-quantum cryptography initiative of SC 27 Working Group 2, PQCRYPTO resolved to establish formal relationship via the ISO liaison mechanism with this SDO and to provide WG 2 with the project's "Initial recommendations of long-term secure post-quantum systems" [25]. In a second step, representatives of PQCRYPTO attended the April 2016 and the October 2016 meetings of the Working Group and in particular the sessions of the WG 2 Study Period on Post-quantum cryptography.

- **Establishment of liaison**
  - In September 2015, the PQCRYPTO project formally requested to establish a Category C Liaison between PQCRYPTO and ISO/IEC JTC 1/SC 27/WG 2.
  - The request was supported by WG 2 at their April 2016 meeting and approved by the SC 27 Plenary meeting, April 19, 2016 (Resolution 20).
  - After a default letter ballot at JTC 1 level, the Category C Liaison between PQCRYPTO and ISO/IEC JTC 1/SC 27/WG 2 was formally established in July 2016.
  - Tanja Lange serves as Liaison officer from PQCRYPTO to SC 27/WG 2 and Frank Morgner has been nominated to serve as Liaison officer from SC 27/WG 2 to PQCRYPTO.
- **Contributions to WG 2 Study Period on Post-quantum cryptography**
  - PQCRYPTO Initial recommendations [25] fed into SC 27 / WG 2 in response to a first Call for contributions to WG 2 Study Period on Quantum computing resistant cryptography.
  - In response to a second questionnaire sent out by the WG 2 Study Period on Post-quantum cryptography, Bundesdruckerei GmbH in September 2016 has organized a detailed response from PQCRYPTO to SC 27/WG 2 [18].
  - At the November 2017 meeting in Berlin Tanja Lange in her role as Liaison officer from PQCRYPTO to SC 27/WG 2 introduced to WG 2 the results published on the project home page `https://pqcrypto.eu.org` under the section "Preprints and Reprints", where extensive tutorial material (videos, slides, exercises, etc.) is available. As a further resource Tanja Lange recommended `https://pqcrypto.org` for its good link collection and for the proceedings of the PQCrypto conference series and also the summer schools held in coordination with them. This contribution was very welcome and Tanja Lange was invited to join the editor team for the new SC 27/WG 2 Standing Document (WG 2/SD 8) on post-quantum cryptography.

3.5 ISO/TC 68 SC2

Lange was invited to an ISO/TC 68 SC2 (Financial Services, security) in April 2017 to give a presentation on post-quantum cryptography and the effects of quantum computers on the security on currently deployed cryptography. The discussions were productive and PQCRYPTO was invited to apply for liaison status with this working group and obtained this status in August 2017. PQCRYPTO participated in the phone conference on 29 November 2017.

4 Conclusion

While we are able to report an increasing and meanwhile impressive number of "Post-Quantum Cryptography" activities within standards development organizations (SDOs) and furthermore can claim a substantial impact of the PQCRYPTO project in driving and shaping such activities (see, e.g., the engagement of PQCRYPTO with the NIST call, the IETF Internet-Draft, the active presence of PQCRYTO at ETSI's "Quantum-Safe Cryptography" Workshops, or the successful Cat C Liaison with SC 27 / WG 2), it is very clear, that the road to standardization of post-quantum cryptography is a long one. Therefore, project partners interested in standardization of post-quantum cryptography need to continue their efforts beyond the formal termination of PQCRYPTO.

References

[1] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. Post-quantum key exchange - A new hope. In *USENIX Security Symposium*, pages 327–343. USENIX Association, 2016.

[2] ANSI. X9.98-2010: Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry, 2010.

[3] ETSI. EG 203 310: Quantum Computing Impact on security of ICT Systems - Recommendations on Business Continuity and Algorithms, June 2016.

[4] ETSI. GR QSC 001: Quantum-Safe Cryptography (QSC) - Quantum-safe algorithmic framework, July 2016.

[5] ETSI. GR QSC 003: Quantum-Safe Cryptography - Case Studies and Deployment Scenarios, February 2017.

[6] ETSI. GR QSC 004: Quantum-Safe Cryptography - Quantum-Safe threat assessment, March 2017.

[7] ETSI. GR QSC 006: Quantum-Safe Cryptography (QSC) - Limits to Quantum Computing applied to symmetric key sizes, February 2017.

[8] ETSI. TR 103 570: Quantum-Safe Key Exchanges, October 2017.

[9] S. Fluhrer, D.A. McGrew, and P. Kampanakis. Postquantum Preshared Keys for IKEv2. Internet-Draft 27 Feb 2018 https://datatracker.ietf.org/doc/draft-ietf-ipsecme-qr-ikev2/.

[10] Google. Experimenting with Post-Quantum Cryptography, 2016. https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html?m=1.

[11] Paul Hoffman. The transition from classical to post-quantum cryptography. Internet-Draft 2018-02-12, expires 2018-08-16.

[12] A. Hülsing, D. Butin, S. Gazdag, and A. Mohaisen. XMSS: Extended Hash-Based Signatures. Internet-Draft 2018-03-29, https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/.

[13] IETF. The IETF Process: an Informal Guide, 2015. https://www.ietf.org/about/process-docs.html.

[14] European Telecommunications Standards Institute. White Paper No. 8, Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges, 2014.

[15] D.A. McGrew and M. Curcio. Hash-Based Signatures. Internet-Draft 2016-03-21, expires 2016-09-22.

[16] Microsoft. SIDH Library, 2016. https://www.microsoft.com/en-us/download/details.aspx?id=52438&751be11f-ede8-5a0c-058c-2ee190a24fa6=True.

[17] Dustin Moody. The ship has sailed - the nist post-quantum crypto competition. NIST. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf, December 2017.

[18] ISO/IEC SC 27/WG 2 N1310. Summary of contributions received to WG 2 N1265 Call for contributions to WG 2 Study Period on Quantum computing resistant cryptography, 2016.

[19] NIST. AES Competition. http://csrc.nist.gov/archive/aes/.

[20] NIST. Modes Development. http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html.

[21] NIST. SHA-3 Competition. http://csrc.nist.gov/groups/ST/hash/sha-3/.

[22] NIST. NIST Interagency Report (NISTIR) 8105: Report on Post-Quantum Cryptography, 2016.

[23] NIST. Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process, 2016.

[24] IEEE P1363.1. Public-Key Cryptographic Techniques Based on Hard Problems over Lattices, 2008.

[25] PQCRYPTO. Initial recommendations of long-term secure post-quantum systems, 2015. http://pqcrypto.eu.org/docs/initial-recommendations.pdf.

[26] J.M. Schanck, W. Whyte, and Z. Zhang. Criteria for selection of public-key cryptographic algorithms for quantum-safe hybrid cryptography. Internet-Draft 2016-04-08, https://datatracker.ietf.org/doc/draft-whyte-select-pkc-qsh/.

[27] J.M. Schanck, W. Whyte, and Z. Zhang. Quantum-Safe Hybrid (QSH) Cipher-suite for Transport Layer Security (TLS) version 1.3,. Internet-Draft 2016-04-04, expires 2016-10-04.