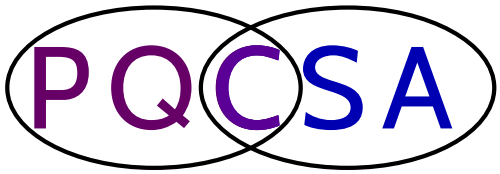

Post-Quantum Cryptography Support Action

Project number: Digital Europe 101190512

D1.1
Survey of PQC algorithms

Due date of deliverable: 30 November 2025
Actual submission date: 30. November 2025

WP contributing to the deliverable: WP1

Start date of project: 1. January 2025 Duration: 3 years

Coordinator:
Eindhoven University of Technology
https://pqcsa.eu

Revision 1.0

Project co-funded by the European Commission within Digital Europe		
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)	
SEN	Sensitive	

Survey of PQC algorithms

Tanja Lange (TUE)

Reviewer: Thibauld Feneuil (CRX) and Jan Klaußner, (BDR)

30. November 2025
Revision 1.0

The work described in this report has been funded (in part) by the European Union in the DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STANDARDPQC call in project 101190512 PQCSA. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

HISTORY OF CHANGES		
VERSION	PUBLICATION DATE	CHANGE
0.8	20 Nov 2025	Local draft version
0.9	28 Nov 2025	First circulated version
1.0	30 Nov 2025	Minor edits following internal review

Abstract

This report surveys post-quantum cryptography (PQC) algorithms that are standardized, deployed, or staged for deployment. The standardization chapter is organized by standardization body and also covers standardization that is currently in progress, to the extent that that is public information – or at least information that can be made public.

The chapter on deployed PQC systems cover the full spectrum of applications that the PQCSA consortium is aware of. Note that this report covers the cryptographic primitives that are used. For protocol development for PQC in the IETF, see D2.1.

Keywords: WP1, post-quantum cryptography, cryptographic primitives, cryptographic building blocks, deployed cryptography.

Contents

Chapter 1

Introduction

As the PQCSA project is starting, the world is at the brink of migrating to post-quantum cryptography (PQC), the biggest migration that cryptography has ever witnessed. While finally the world has recognized the need to add protection against attacks by quantum computers, the question becomes what to migrate to. Luckily there are a few contenders for providing this security. Since the term PQC was coined in 2003, researchers in cryptography have identified some core mathematical hardness assumptions that appear to hold up against quantum attacks and investigated ways to turn them into systems for key encapsulation, signatures, or even advanced cryptographic building blocks.

The competition by the US National Institute of Standards and Technology (NIST) for identifying post-quantum systems for standardization provided a boost to the area with more researchers, in particular at PhD and postdoc level, specializing in PQC. The NIST PQC competition was announced at PQCrypto 2015 in Fukuoka and drafts of the call for contributions were discussed for the next 1.5 years, leading to the final call in November 2016 and a submission deadline at the end of November 2017. The competition attracted many submissions and is described in more detail later in this report, along with a newer NIST competition for additional signature systems. By now NIST has published three of the systems as FIPS standards and is working on two more.

While the NIST competition caught a lot of the community's attention, it did not happen in a vacuum. The IRTF, the research arm of the Internet Engineering Task Force (IETF), published specifications of stateless hash-based signatures; standardization in ISO progressed on several candidates; and ETSI published some informative documents. Furthermore, some of the schemes have undergone earlier standardization on their own merit as competitive systems even without reference to protection against quantum attacks.

This report covers standardization of post-quantum systems in Chapter 2.

In some areas, in particular the regulated industries, standardization and selection in regulations have to predate deployment. However, other security products, in particular software products, often adopt systems once they have received enough study or support from the cryptographic community, or even as part of such studies to gain operational data on potential issues. Such deployment in turn facilitates standardization, as standardization bodies such as ISO and IETF often require practical deployment, or at least the expressed interest into such deployment, before even embarking on standardization.

Chapter 3 traces deployment of PQC in fielded products. We mention some feasibility studies but do not attempt to cover all dry runs of systems experimenting with PQC deploy-

ment.

This deliverable focuses on the cryptographic building blocks, in particular signatures and KEMs. Deliverable D2.1 “Survey of PQC protocols” in turn covers standardization of PQC protocols in the IETF. Deliverable D1.3 “Hot Topics and Open Problems in Post-Quantum Cryptography” complements this deliverable by pointing to gaps where suitable systems are missing.

Chapter 2

Standardization bodies covering PQC

This chapter covers the different international standardization bodies engaged in standardization of PQC, and have published standards in PQC or are in the process of issuing them (and we are not barred from publishing these efforts).

The sections are ordered in alphabetical order of the names of the standardization bodies.

2.1 ETSI

ETSI, the European Telecommunication Standardization Institute, established a working group in 2013 that covers approaches to tackle the quantum threat. The initial working group (WG), called Quantum-Safe Cryptography, covered PQC as well as Quantum Key Distribution (QKD). The WG, and later the CYBER WG, produced several instructive documents on PQC including a study of the costs of quantum attacks on symmetric cryptography. However, they have not issued any standards on cryptographic primitives.

More recently they produced two standards on PQC protocols, but they defer to NIST for the instantiations of the cryptographic primitives, so for the moment they only permit ML-KEM as specified in FIPS 203 as PQC KEM. ML-KEM is based on CRYSTALS-KYBER [37], see Section 2.5.

While PQC protocols are covered in deliverable D2.1 we nevertheless mention the two ETSI standards here as D2.1 covers only IETF/IRTF protocols. They are TS 104 015 V1.1.1 "Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies" and TS 103 744 V1.2.1 "Quantum-safe Hybrid Key Establishment".

2.2 IEEE and ANSI X.9

IEEE, the Institute of Electrical and Electronics Engineers, has one standardization project for public-key cryptography. P1363 was developed in the 1990s with the first version published in 2000 and an amendment published in 2004. The standard covers digital signatures, and public-key encryption and key agreement based on the integer factorization problem (RSA) or on discrete logarithms in elliptic curves or the multiplicative group of finite fields. In 2009, IEEE published P1363.1-2008 which supplements P1363 and covers cryptography based on

hard lattice problems. This standardizes the NTRU public-key encryption system. A draft of this standard is publicly available as [38].

NTRU [16] was first presented at the rump session of Crypto 1996 and finally published at ANTS 1998. It was proposed for offering better efficiency than ECC and RSA. While by 2008 the merits of NTRU for PQC were understood, the standardization effort focused on the performance benefits. Nevertheless, NTRU became the historically first PQC system that was standardized.

Following the IEEE standardization, NTRU was also standardized in 2010 in ANSI X9.98-2010, which has now been revised to ANSI X9.98-2010 (R2017). ANSI, the American National Standards Institute, sets internationally used standards for the financial industry in its X9 committee.

2.3 IETF and IRTF

The Internet Engineering Task Force (IETF) and its research arm, the Internet Research Task Force (IRTF), recognized early the need for standardization of post-quantum algorithms. However, they did not want to duplicate efforts. With NIST's announcement that it aimed to run a competition to identify systems for signatures and KEMs, IETF held back efforts on those. See below in Section 2.5 for the NIST efforts.

NIST's call covered only regular signatures, which have a static signing key and can be used to produce any number of messages. [1] This meant that stateful hash-based signatures were out of scope of the competition. The Crypto Forum Research Group (CFRG), part of the IRTF, followed up with RFC 8391 [17] on the stateful hash-based signature scheme XMSS [8], becoming the first effort in PQC for the IETF, and then with RFC 8554 [31] on the stateful hash-based signature scheme LMS based on [25].

While the IETF is working on several RFCs on PQC protocols that use Kyber/ML-KEM and/or Dilithium/ML-DSA, see D2.1, they refer to NIST's FIPS 203 or 204 for specifying the system. An exception is RFC 9881 [30] for ML-DSA in X.509 certificates which mostly refers to the NIST standard but includes a pre-hash version of FIPS 204, slightly modifying the External interface for FIPS 204. The RFC explicitly disallows the HashML-DSA version from the NIST standard which would also provide pre-hashing but would require a separate verification algorithm. Even in this RFC, the calls to the Internal interface rely on FIPS 204 for specificatin, which is included as normative reference.

For other PQC algorithms, so far only Internet Drafts exist. Internet Drafts (I-Ds) may be precursors to RFCs if they get adopted, but there is no guarantee that they get to that level. As the IETF datatracker always points out: "Anyone may submit an I-D to the IETF. This I-D is not endorsed by the IETF and has no formal standing in the IETF standards process." I-Ds automatically expire after 6 months unless they get renewed. NTRU Prime [6] is covered in the (currently expired) I-D [21]. NTRU [11] is covered in I-D [15], FrodoKEM [33] is covered in I-D [26], and Classic McEliece [4] is covered in I-D [22].

2.4 ISO

Similar to the IETF, ISO, the International Organization for Standardization, held off on standardization of PQC algorithms while the NIST competition was ongoing. In the mean-

[1] NIST specifically required security for up to 2^{64} signed messages.

time, ISO engaged in capacity building on the topic and eventually in 2020 issued "SC 27 committee document 208 – Post-Quantum Cryptography" which is publicly available from the ISO webpage. It covers the following topics:

1. Part I – General [12].
2. Part II – Hash-Based Signatures [32].
3. Part III – Lattice-Based Cryptography [27].
4. Part IV – Code-Based Cryptography [23].
5. Part V – Multivariate Cryptography [39].
6. Part VI - Isogeny-Based Cryptography [24].

Originally these were posted as Standing Document SD8 of SC 27 WG 2, but they were renamed as an SC 27 committee document in 2023. [2]

Following the publications of the RFCs on stateful hash-based signatures, see Section 2.3, ISO standardized XMSS and LMS in 14888-4.

ISO is currently in the process of standardizing Classic McEliece [4], FrodoKEM [33], and ML-KEM [34] in 18033-2 Encryption algorithms – Part 2: Asymmetric ciphers, Amendment 2. At the time of writing the project has passed the DIS stage.

ISO is reportedly also working on adding an Amendment to 29192-4 Lightweight cryptography – Part 4: Mechanisms using asymmetric techniques in order to standardize NTRU [11], where it has reached the DIS stage.

Finally, ISO has just announced two more projects for standardizing PQC signatures, namely 14888-5 Lattice-based mechanisms (upcoming) and 14888-6 Stateless hash-based mechanisms which is in the WD stage.

2.5 NIST

After running competitions to select the AES block cipher and the SHA-3 hash function, NIST announced in 2015 their intention to run a cryptographic competition in post-quantum cryptography. After some general discussion and an official discussion phase, NIST officially announced their Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms in December 2016 with a submission deadline on 30 November 2017. The call targeted KEMs and signatures.

NIST reported having received 82 submissions, of which it posted 69 as "complete and proper" on their Round 1 Submissions page. Researchers quickly engaged in scrutinizing the submissions and successfully broke some and weakened some others. At the same time, submission teams were still working on demonstrating the performance of their designs by providing better implementations. In January 2019, NIST announced the end of Round 1 and which submissions would be permitted to advance to Round 2, with a deadline of April 2019 for submitting updated submission packages. None of the seriously broken schemes were included and NIST also deselected some candidates it deemed less attractive in comparison. NIST's Round 2 Submissions page lists the surviving 26 schemes, covering 17 KEMs and and 9

[2] Part 3 and 6 lost the statements of authors, we include them from the original documents.

signature schemes. In July 2020 NIST announced the schemes that were permitted to advance to the next round with submission deadline in October 2020, again discarding some broken schemes and schemes which NIST deemed less interesting. NIST's Round 3 Submission page shows the remaining 15 candidates, split into 4 KEM finalists, 5 KEM alternates, 3 signature finalists, and 3 signature alternates.

In July 2022 NIST finally announced CRYSTALS-KYBER [37] as the sole winner in the KEM category, and CRYSTALS-DILITHIUM [28], FALCON [35], and SPHINCS$^+$ [18] as winners in the signature category. At the same time, NIST announced that BIKE [5], Classic McEliece [4], HQC [2], and SIKE [20] would advance to a 4th round of evaluation. SIKE was completely broken [9, 29, 36] less than a month later, while the wait for the end of Round 4 stretched till March 2025 and ended with the selection of HQC over BIKE. For Classic McEliece, NIST referred to ISO's efforts in standardizing Classic McEliece (see Section 2.4), writing "Classic McEliece is currently under consideration for standardization by the International Organization for Standardization (ISO). Concurrent standardization of Classic McEliece by NIST and ISO risks the creation of incompatible standards" and "After the ISO standardization process has been completed, NIST may consider developing a standard for Classic McEliece based on the ISO standard".

By now, NIST has issued standards for 3 of the 4 winners from 2022 and is working on the 4th and HQC. The published standards are

- FIPS 203 ML-KEM (Kyber), based on lattices,
- FIPS 204 ML-DSA (Dilithium), based on lattices, and
- FIPS 205 SLH-DSA (SPHINCS+), based on hash functions.

While already selecting 3 winners in the signature category, NIST announced in July 2022 a project for the Standardization of Additional Digital Signature Schemes. Of the initial 40 submissions posted on the Round 1 Additional Signatures page, 14 are now in the 2nd Round for the additional signatures. NIST had sought to discourage submissions of lattice-based signatures as FIPS 204 and the upcoming 206 are based on lattices and thus it is not surprising that only 1 of the remaining candidates is based on lattices. There are 3 candidates based on MQ problems, 2 on codes, 1 on isogenies, and the remaining 6 are based on the MPCitH paradigm and its developments such as VOLEitH. In the first edition of the competition in 2017, MPCitH contributed only one submission, Picnic [40]; the number of newer submissions shows a much increased interest in this topic in the community. See also D1.3 covering hot topics in PQC.

The 2nd round for the standardization of additional signatures is still ongoing at the time of writing this document.

An overview with links to all of NIST's activities in PQC standardization is available at `https://www.nist.gov/pqcrypto`.

Additionally, NIST followed IETF in standardizing stateful hash-based signatures XMSS and LMS in NIST SP 800-208.

Beyond the standardization of cryptographic primitives, NIST is also active in issuing recommendations for their use, e.g., NIST SP 800-227 covers "Recommendations for Key-Encapsulation Mechanisms", showing how to use KEMs in protocols, and NIST SP 800-133 Rev. 2 on "Recommendation for Cryptographic Key Generation", including descriptions of key combiners, relevant for combining pre- and post-quantum KEMs.

2.6 Other technical specifications

ENISA, the European Union Agency for Cybersecurity, publishes a list of ECCG Agreed Cryptographic Mechanisms which are to be used in the Common Criteria-based Cybersecurity Certification Scheme (EUCC), which in turn is based on the older Common Criteria evaluation framework SOG-IS.

Post-quantum primitives in this list include ML-DSA (FIPS 204), XMSS, LMS, SLH-DSA (FIPS 205), ML-KEM (FIPS 203), and FrodoKEM. Except for XMSS and LMS, the list includes only higher security levels of these primitives, targeting 2^{192} security (which NIST calls "category 3") and above.

Chapter 3

Deployment of PQC

While standardization has just concluded for some systems and is still ongoing for others, there are already several fielded systems that actively deploy PQC.

This chapter surveys these use-cases, focusing on which PQC systems are being used. It is promising to see that this is now a fast moving field. What began with some tests 10 years ago, to see if PQC was affordable, finally picked up speed around 2022, and even more so since NIST published FIPS 203 – 205 (see Section 2.5) and several countries and the EU announced roadmaps and timelines for the migration to PQC. This survey covers significantly more than we saw in 2023 when we wrote the grant proposal and there will likely be more material by the time this deliverable gets posted online after the review in another 8 - 10 months.

Given the scope of the deliverable we focus on what PQC algorithms are used and do not comment on the PQC protocols; see deliverable D2.1 for a survey of PQC protocols in the IETF. We close with some observations on where we notice a lack of adoption that can be traced back to a lack of suitable PQC algorithms, see also deliverable D1.3 "Report on Hot Topics and Open Problems in Post-Quantum Cryptography".

3.1 Cryptographic libraries

Cryptographic libraries per se are not applications or deployments, however, they permit developers to conveniently use the cryptosystems that they provide. Libraries influence the choices of systems in deployments, even if the libraries were used only in the development phase and later replaced by customized implementations. Because of this significance we cover PQC available in cryptographic libraries in this chapter as well and put it first as we will link back to it.

The text focuses on open-source libraries that play a significant role in bringing applications to deploying PQC. An overview of open source libraries in cryptography and investigating to which extent they cover PQC can be found in [3]. There are also an increasing number of closed-source libraries advertising PQC support; we do not cover these here. The PKI consortium has published the PQC Capabilities Matrix (PQCCM) listing several libraries, including commercial libraries and IP cores, and tabulating which of LMS, XMSS, ML-KEM/FIPS-203, ML-DSA/FIPS-204, and SLH-DSA/FIPS-205 they implement or have announced to be working on. We reproduce this table in Table 3.1.1.

Vendor	Product	Category	Updated	X.509 Hyb	LMS	XMSS	ML-KEM	ML-DSA	SLH-DSA
Ascertia	ADSS PKI Server	PKI	2025-08-12	no	no	no	yes	yes	planned
Ascertia	ADSS Signing Server	Signing software	2025-08-12	no	no	no	yes	yes	planned
Ascertia	ADSS Server SAM Service	Signing software	2025-08-12	no	no	no	yes	yes	planned
ANKATech	ANKASecure	REST API & SaaS	2025-05-30	no	yes	yes	yes	yes	yes
AppViewX	AVX ONE PKIaaS	PKI	2025-04-21	yes	planned	planned	no	yes	yes
AWS	AWS KMS	HSM	2025-09-02	N/A	no	no	no	yes	no
BERTEN	MLDS-B235	IP Core	2025-11-12	no	no	no	no	yes	no
BERTEN	MLKE-B135	IP Core	2025-11-12	no	no	no	yes	no	no
Botan	Botan	Software library	2025-02-27	no	yes	yes	yes	yes	yes
Bouncy Castle	BC	Software library	2025-02-27	yes	yes	yes	yes	yes	yes
CAST Inc	KiviPQC-KEM	IP Core	2025-11-12	no	no	no	yes	no	no
Codegic	Khatim PKI Server	PKI	2025-08-25	no	no	planned	planned	yes	planned
Codegic	Khatim Sign Server	Signing Software	2025-08-25	no	no	planned	planned	yes	planned
Cryptomathic	CrystalKey 360	KM & Signing Software	2025-08-14	N/A	yes	yes	planned	yes	no
Crypto4A	QxEDGE	HSP	2025-02-27	N/A	yes	yes	yes	yes	yes
Crypto4A	QxHSM	HSM	2025-02-27	N/A	yes	yes	yes	yes	yes
CZERTAINLY	CZERTAINLY	PKI	2025-06-22	yes	no	no	yes	yes	yes
Dell Technologies	BSAFE™ Crypto Module for C	Software library	2025-10-28	N/A	yes	no	planned	yes	no
Dell Technologies	BSAFE™ Crypto-J	Software library	2025-10-28	no	yes	no	planned	yes	no
DigiCert	Private CA	PKI	2025-06-05	no	no	no	no	yes	yes
DigiCert	Software Trust Manager	Signing software	2025-06-05	no	no	no	no	yes	yes
DigiCert	Trust Lifecycle Manager	CLM software	2025-06-05	no	no	no	no	yes	yes
DigiCert	Device Trust Manager	IoT device mgmt software	2025-06-05	no	no	no	no	yes	yes
DigiCert	TrustCore SDK	Software library	2025-06-05	no	no	no	yes	yes	yes
Entrust	nShield	HSM	2025-03-01	N/A	no	no	yes	yes	no
essendi it GmbH	essendi xc	CLM	2025-05-21	no	no	no	planned	yes	planned
EVERTRUST	STREAM/ HORIZON	PKI	2025-03-03	yes	no	no	planned	yes	planned
Eviden	IDnomic PKI	PKI	2025-03-05	no	no	no	yes	yes	no
Eviden	Trustway Proteccio™ NetHSM	HSM	2024-12-09	N/A	no	no	yes	yes	yes
ExeQuantum	ExeQuantum	REST API & SaaS	2025-04-29	no	no	no	yes	yes	yes
Fortanix	DSM	HSM	2025-02-27	N/A	yes	yes	yes	yes	yes
I4P	Trident	HSM	2025-04-16	N/A	no	no	yes	yes	yes
InfoSec Global	AgileSec Analytics	Software	2025-02-27	no	yes	yes	yes	yes	yes
IP Cores Inc	PQC1	IP Core	2025-11-10	no	no	no	yes	yes	no
Keyfactor	SignServer	Signing Software	2025-02-27	no	yes	no	no	yes	yes
Keyfactor	EJBCA	PKI	2025-05-22	yes	yes	no	yes	yes	yes
Keyfactor	Command	PKI	2025-06-23	yes	no	no	no	yes	planned
MTG	CARA	PKI	2025-05-06	no	no	no	planned	yes	yes
MTG	CLM	PKI	2025-05-06	no	no	no	planned	planned	planned
Nexus Group	Certificate Manager	PKI	2025-07-14	planned	no	no	yes	yes	yes
Open Quantum Safe	liboqs	Software library	2025-05-27	yes	yes	yes	yes	yes	no
OpenSSL	libssl	Software library	2025-04-15	no	no	no	yes	yes	yes
PQ Code Package	PQCP	Software library	2025-06-24	N/A	no	no	yes	yes	planned
PQShield	UltraPQ-Suite	IP Core and Software library	2025-11-12	no	no	no	yes	yes	no
Resquant	Customizable Cryptography Accelerator	IP Core	2025-11-12	no	no	yes	yes	yes	yes
SafeLogic	CryptoComply PQTLS	Software Library	2025-03-31	no	no	no	yes	no	no
Secure-IC	Securyzr	IP Core	2025-11-12	no	no	yes	yes	yes	no
Securosys	Primus HSM	HSM	2025-02-27	N/A	yes	yes	yes	yes	yes
Smallstep	step-ca	PKI	2025-10-02	no	no	no	yes	no	no
Thales	Luna	HSM	2025-06-30	N/A	yes	no	yes	yes	no
Utimaco	uTrust	HSM	2025-09-02	N/A	yes	no	yes	yes	no
Xiphera	xQlave	IP Core	2025-11-12	no	no	no	yes	yes	no

Table 3.1.1: Data from PQC Capabilities Matrix (PQCCM) as of 2025-11-29.

3.1.1 Early libraries supporting PQC

All submissions to the NIST PQC competition included a reference implementation and most included a somewhat faster AVX2 implementation. Candidates interested in independent benchmarking submitted their systems to eBACS. eBACS then included them in the SUPERCOP benchmarking system for distribution; SUPERCOP continues to expand its coverage of post-quantum cryptography. The PQCRYPTO project bundled all submissions resulting from the project into libpqcrypto.

For some particularly suitable systems PQCRYPTO wrote implementations for the ARM Cortex-M4 and published these as pqm4, a project that is still maintained. Hardware implementations from PQCRYPTO were bundled in pqhw.

3.1.2 strongSwan

StrongSwan is a library for IPsec and IKE. It was one of the early libraries to include PQC algorithms, e.g. already 10 years ago including the lattice-based signature scheme BLISS [14]. StrongSwan 6.0 includes ML-KEM.

3.1.3 liboqs

Researchers in Waterloo started the Open Quantum Safe project, where they gathered some implementations from the NIST submissions and re-implemented or adjusted some others. The project is by now supported by the Linux Foundation via the Post-Quantum Cryptography Alliance and liboqs is an open-source C library that can be used in projects. Their webpage warns "WE DO NOT CURRENTLY RECOMMEND RELYING ON LIBOQS OR OUR APPLICATION INTEGRATIONS IN A PRODUCTION ENVIRONMENT OR TO PROTECT ANY SENSITIVE DATA" (all-caps in original) but also provides a page listing External users of OQS. The library covers all NIST candidate KEMs from the 3rd round, except for SIKE (which is broken). It keeps an implementation of Kyber (in the 3rd round version) along with ML-KEM (in the FIPS 203 version). The other KEMs are (in alphabetical order) BIKE, Classic McEliece, FrodoKEM, HQC, NTRU, and NTRU Prime.

Among signatures, liboqs includes Dilithium as ML-DSA (in the FIPS 204 version) and has an implementation of SPHINCS+ (round 3) next to SLH-DSA (in the FIPS 205 version). It also includes the other NIST winner Falcon (still no FIPS standard) and four candidates from the ongoing competition for additional signatures, the code-based CROSS and the three MQ-based systems MAYO, SNOVA, and UOV. It also includes the stateful hash-based signature schemes LMS and XMSS.

3.1.4 Cloudflare and Google

Cloudflare and Google have been the leading players for testing usability of PQC on the Internet, starting with Google's CECPQ1 experiment in 2016 and the CECPQ2 experiment by Google and Cloudflare in 2019. The first experiment used NewHope and the second NTRU-HRSS, both times along with X25519 elliptic-curve cryptography.

Google has implemented support for PQC in its BoringSSL library. The library includes Round-3 candidates Kyber and NTRU-HRSS, as well as implementations of the FIPS standards ML-KEM, ML-DSA, and SLH-DSA.

The Cloudflare Interoperable Reusable Cryptographic Library CIRCL is a Go library that is advertised for experimenting with PQC. It includes implementations of Round-3 Kyber next to ML-KEM (FIPS 203); for both it covers all three security levels. For FrodoKEM it includes the 640-SHAKE version. It also includes an implementation of CSIDH [10]. CSIDH is a key-exchange system based on supersingular isogenies that was invented in 2018, so after the NIST competition started, and was thus not part of the competition.

On the signature side it includes Round-3 Dilithium next to ML-DSA (FIPS 204), both times covering all security levels, and all twelve parameter sets for SLH-DSA (FIPS 205).

3.1.5 Amazon

Amazon announced a year ago that the 3.0 version of their AWS-LC library has received FIPS 140-3 validation, including for their ML-KEM implementation. The library includes all three security levels of ML-KEM. FIPS validation is relevant to some regulated industries, for which this validation now permits the use of PQC.

3.1.6 Microlibraries

Some PQC algorithms have been made available as standalone libraries for easier integration into projects.

- libmceliece is an implementation of the Classic McEliece KEM. It is also available as a Debian package.
- libntruprime is an implementation of the NTRU Prime KEM. It is also available as a Debian package.
- mlkem-native is an implementation of ML-KEM.
- mldsa-native is an implementation of the ML-DSA signature system.

3.1.7 PQC support for cryptographic coprocessors

NVIDIA offers the cuPQC library for speeding up cryptography on GPUs. It covers ML-KEM and ML-DSA and for both supports all three security levels.

STMicroelectronics advertises an "X-CUBE-PQC" software library for ST microcontrollers using 32-bit ARM CPUs.

3.2 SSH and Git

SSH is used in remote server administration for logging into computers as well as the transport library of choice when connecting and authenticating to git servers. The OpenSSH library started supporting NTRU Prime as sntrup761x25519-sha512 in version 8.5, released in 2021, after preliminary integration of NTRU Prime into TinySSH. Version 9 of OpenSSH in 2022 enabled support for sntrup761x25519-sha512 by default. Today sntrup761x25519-sha512 is supported in the following SSH implementations: AbsoluteTelnet, Apache SSHD, AsyncSSH, CycloneSSH, Dropbear, HPN-SSH, JSch, OpenSSH, PKIX-SSH, Putty, SSH.NET, Tectia SSH, and TinySSH.

In 2025, OpenSSH version 9.9 added mlkem768x25519-sha256, and OpenSSH 10.0 made mlkem768x25519-sha256 the default. OpenSSH has announced that with version 10.1 it will start warning the user if connections are not secured with a PQC algorithm.

GitHub recently announced support for NTRU Prime keys for accessing repositories. This will permit users to authenticate using sntrup.

3.3 TLS

Development of PQC versions of TLS is covered in D2.1. PQC algorithms covered in the early experiments are covered in Section 3.1.4. At this point the algorithm choice has been fixed to ML-KEM, through some implementations still use Round-3 Kyber. The Cloudflare Radar now reports that about 50% of the connections reaching their servers support PQC; Cloudflare says that they are supporting PQC on most pages, so the 50% is indicative of the level of PQC support on the client side. Each of the major browsers (Chrome, Edge, Firefox, and Safari) supports PQC by default in the latest version, but not all users upgrade to the latest versions.

On the server side, measurements of the top 100000 web servers found 38931 supporting PQC (specifically X25519MLKEM768, which encrypts with ML-KEM-768 along with X25519) in September 2025, up from 27904 in March 2025.

There are many commercial and open source libraries implementing the cryptography used in TLS. Here is a representative list (in alphabetical order) of some open source SSL libraries and the PQC algorithms they support.

- Google's BoringSSL was already covered above; it supports Round-3 candidates Kyber and NTRU-HRSS, as well as implementations of the FIPS standards ML-KEM, ML-DSA, and SLH-DSA.
- Botan lists support for ML-DSA, ML-KEM, XMSS, HSS-LMS, SLH-DSA, FrodoKEM, and Classic McEliece.
- Bouncy Castle lists support for ML-KEM, ML-DSA, SLH-DSA, LMS, XMSS, BIKE, HQC, Classic McEliece, SABER, FrodoKEM, NTRU, NTRU Prime, Falcon, Picnic, Rainbow, and GeMSS.
- GnuTLS lists support for ML-KEM-768, ML-KEM-1024, ML-DSA-44, ML-DSA-65, and ML-DSA-87.
- OpenSSL lists support for ML-KEM, ML-DSA, SLH-DSA, and LMS. Other PQC algorithms are available as providers, such as oqsprovider from the OQS project.
- WolfSSL supports ML-KEM, ML-DSA, SPHINCS+, LMS, XMSS, and, via McWolf, Classic McEliece.

3.4 Messaging and email

Messaging applications are some of the frontrunners in end-to-end encryption. Unsurprisingly, they have also been the target of much academic attention for designing PQC versions of their

protocols and Signal and iMessage have in the meantime started deploying versions including PQC algorithms.

Signal's PQXDH Key Agreement Protocol uses ML-KEM 1024 along with X25519 ECC. They recently upgraded their use of PQC for better forward secrecy in SPQR.

Apple announced that iMessage will be enhanced with PQC3, using ML-KEM 1024 in combination with NIST P-256 ECC.

For email encryption, there is an ongoing discussion about PQC versions of OpenPGP, see deliverable D2.1. Vendors such as Protonmail have announced their plans to support these versions.

libgcrypt, the library at the core of GnuPG, does not advertise PQC support but the library source includes ML-KEM, sntrup761, and mceliece6688128f.

Meanwhile the email provider Tuta announced last year that they were launching TutaCrypt which would use Kyber to add PQC. Given interoperability needs such usage would be limited to exchanges between subscribers to the service with the PKI handled by Tuta.

3.5 HSMs

Several HSM vendors have been active in the PQC space during the past decade, given the long development times for hardware solutions and the long lifespan of their devices. HSM vendors were actively supporting the standardization of stateful hash-based signatures and were early adopters. Signature applications are relevant for HSMs but by now they also support KEMs. A few representative examples are as follows.

Crypto4A announced that it uses Classic McEliece in all of its HSMs.

STMicroelectronics announced that "STSAFE-TPM" supports LMS firmware updates.

Thales announced support for LMS, ML-KEM, and ML-DSA in HSMs.

Utimaco announced support for ML-KEM, ML-DSA, LMS, and XMSS, while stating that support for SLH-DSA is in progress.

For further examples (focusing on NIST standards), we refer to the HSM entries in Table 3.1.1.

3.6 VPNs

VPNs protect connections between a dedicated VPN server and clients registered with it. This leads to an ecosystem which can efficiently be upgraded on both sides. While the general discussion on how to upgrade IKE to PQC is still ongoing, some VPN projects have rolled out PQC support already.

Mullvad announced already 7 years ago that they were upgrading to using PQC. The feature is now announced as stable. Mullvad's PQC deployment makes use of the pre-shared key (PSK) in their WireGuard [13] implementation. Normally this is a static secret, shared in advance between server and client. Instead they let this field be a fresh secret, computed using Classic McEliece and Kyber. The PSK protects all messages using symmetric-key cryptography, so that WireGuard's ECC-based key exchange is not exposed to later quantum attackers.

ExpressVPN announced an upgrade to their Lightway VPN to use PQC algorithms, in particular using P256_KYBER_LEVEL1 for UDP and P521_KYBER_LEVEL5 for TCP, on top of the WolfSSL and liboqs libraries.

OpenBSD's OpenIKED has announced experimental support for sntrup761x25519.

Rosenpass is also based on WireGuard but goes further in the modifications to integrate PQC algorithms into the public-key part of the connection. It largely follows Post-Quantum WireGuard [19] but changes the ephemeral KEM to using Kyber instead of Saber; the long-term KEM continues to be Classic McEliece. Both are supplemented by pre-quantum X25519 as in WireGuard. Rosenpass credits liboqs (Section 3.1.3) with providing the PQ algorithms.

The new PQConnect [7] design borrows many elements from VPNs but aims to build tunnels end-to-end. Servers announce their support for PQConnect by adding a CNAME record. Clients automatically detect support and build a tunnel that protects all communication between client and server machine, like for VPN tunnels. The software is available at (and deployed on) `https://www.pqconnect.net/`. The PQC algorithms used are Classic McEliece for long-term keys and NTRU Prime for ephemeral keys, both in addition to X25519 ECC.

3.7 Hardware tokens

Sandbox AQ announced a PQC version of FIDO2, the protocol used in 2-factor authentication with hardware tokens. The blogpost describes an upgraded protocol using Kyber and Dilithium (the post predates the FIPS standards) and working on Nitrokey, Solokeys, and Yubico tokens. Meanwhile Authentrend has produced tokens using these PQC algorithms.

3.8 PKI and gaps in deployment

Table 3.1.1 is a copy of the state of the PQC Capabilities Matrix (PQCCM) maintained by the PKI consortium. PKIs provide public keys, typically with a certificate of authenticity. With that in mind, one would expect row of checkmarks for the signature columns, and indeed many do support some selection of ML-DSA, SLH-DSA, LMS, and XMSS, but it is remarkable that not all do. In general, the sizes of PQC signatures and public keys are seen as problematic in applications where certificate chains are needed, such as typical applications of certificates for TLS. See Deliverable D2.1 for insights into ongoing discussions regarding deployment of signatures. NIST's competition for additional signatures is meant to cater to this demand but practitioners are still not happy with the options provided. The MQ-based systems offer short signatures but at the expense of large public keys; SQISign [1] offers short signatures and keys, but has performance issues, while also being based on a very recent hardness assumption. Security concerns will hopefully be addressed through more review during the competition and speed improvements are ongoing, while there are discussions about changing how certificate chains work so that public keys for the top-level domains would not need to be included. The hope for better solutions in the future adds to common hesitation to deploy post-quantum signatures, along with the observation that signatures do not suffer from the store-now decrypt-later long-term consequences.

3.9 Privacy applications

The above demonstrates successes in deployment and a focus on adding PQC to protect encryption (more uses of KEMs than signatures), which is fully justified by the long-term

consequences. Privacy applications differ from applications that "just" aim to ensure confidentiality in that they also protect the identity or other properties of the user. This means that they often require more advanced cryptographic primitives, going beyond signatures and KEMs.

Privacy Pass is a design used in browsers to support an anonymous user-authentication mechanism, typically a proof that the user is human and not a bot. Until its introduction, users had to solve many more CAPTCHAs; now solving one creates a token which then can be used to show other sites that the user has recently solved one. The relevant feature of the design is that these proofs are not linkable. Internally, the protocol relies on blind signatures and OPRFs, areas identified as open problems in Deliverable D1.3. For now there is no deployed PQC version of Privacy Pass.

Development of the European Digital Identity wallet is still ongoing, but a privacy-friendly design would need to be based on Attribute-Based Credentials (ABCs). However, ABCs are another area identified as an open problem in Deliverable D1.3. Design considerations for the EUDI wallet at this moment do not cover protection against quantum attacks.

Bibliography

[1] Marius A. Aardal, Gora Adj, Diego F. Aranha, Andrea Basso, Isaac Andrés Canales Martínez, Jorge Chávez-Saab, Maria Corte-Real Santos, Pierrick Dartois, Luca De Feo, Max Duparc, Jonathan Komada Eriksen, Tako Boris Fouotsa, Décio Luiz Gazzoni Filho, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Luciano Maino, Michael Meyer, Kohei Nakagawa, Hiroshi Onuki, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Giacomo Pope, Krijn Reijnders, Damien Robert, Francisco Rodríguez Henríquez, Sina Schaeffler, and Benjamin Wesolowski. SQIsign. Technical report, National Institute of Standards and Technology, 2024. available at https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures.

[2] Carlos Aguilar-Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor, and Jurjen Bos. HQC. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

[3] Nadeem Ahmed, Lei Zhang, and Aryya Gangopadhyay. A survey of post-quantum cryptography support in cryptographic libraries, 2025. https://arxiv.org/abs/2508.16078.

[4] Martin R. Albrecht, Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Kenneth G. Paterson, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlinson, and Wen Wang. Classic McEliece. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

[5] Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillipe Gaborit, Shay Gueron, Tim Guneysu, Carlos Aguilar-Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Gilles Zémor, Valentin Vasseur, and Santosh Ghosh. BIKE. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

[6] Daniel J. Bernstein, Billy Bob Brumley, Ming-Shing Chen, Chitchanok Chuengsatiansup, Tanja Lange, Adrian Marotzke, Bo-Yuan Peng, Nicola Tuveri, Christine van Vredendaal, and Bo-Yin Yang. NTRU Prime. Tech-

nical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

[7] Daniel J. Bernstein, Tanja Lange, Jonathan Levin, and Bo-Yin Yang. PQConnect: Automated post-quantum end-to-end tunnels. In *ISOC Network and Distributed System Security Symposium – NDSS 2025*, San Diego, CA, USA, February 24–28, 2025. The Internet Society.

[8] Johannes A. Buchmann, Erik Dahmen, and Andreas Hülsing. XMSS - A practical forward secure signature scheme based on minimal security assumptions. In Bo-Yin Yang, editor, *Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011*, pages 117–129, Tapei, Taiwan, November 29 – December 2 2011. Springer Berlin Heidelberg, Germany.

[9] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023, Part V*, volume 14008 of *Lecture Notes in Computer Science*, pages 423–447, Lyon, France, April 23–27, 2023. Springer, Cham, Switzerland.

[10] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018, Part III*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427, Brisbane, Queensland, Australia, December 2–6, 2018. Springer, Cham, Switzerland.

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

[12] Lily Chen, Tanja Lange, and Shiho Moriai. ISO/IEC JTC1 SC27 WG2, SC 27 committee document 208, Post-Quantum Cryptography, Part I – General, 2020. Part of https://committee.iso.org/files/live/sites/jtc1sc27/files/resources/SC%2027%20committee%20document%20208%20-%20Post-Quantum%20Cryptography.zip.

[13] Jason A. Donenfeld. WireGuard: Next generation kernel network tunnel. In *ISOC Network and Distributed System Security Symposium – NDSS 2017*, San Diego, CA, USA, February 26 – March 1, 2017. The Internet Society.

[14] Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal Gaussians. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 40–56, Santa Barbara, CA, USA, August 18–22, 2013. Springer Berlin Heidelberg, Germany.

[15] Scott Fluhrer, Michael Prorock, Sofia Celi, John Gray, Xagawa Keita, and Haruhisa Kosuge. NTRU key encapsulation –draft-fluhrer-cfrg-ntru-03, 2025. https://datatracker.ietf.org/doc/draft-fluhrer-cfrg-ntru/.

[16] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In *Third Algorithmic Number Theory Symposium (ANTS)*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, June 1998.

[17] Andeas Huelsing, Denis Butin, Stefab Gazdag, Joost Rijneveld, and Aziz Mohaisen. XMSS: eXtended Merkle Signature Scheme. RFC 8391 (Informational), 2018. https://www.rfc-editor.org/rfc/rfc8391.html.

[18] 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, Jean-Philippe Aumasson, Bas Westerbaan, and Ward Beullens. SPHINCS$^+$. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

[19] Andreas Hülsing, Kai-Chun Ning, Peter Schwabe, Fiona Johanna Weber, and Philip R. Zimmermann. Post-quantum WireGuard. In *2021 IEEE Symposium on Security and Privacy*, pages 304–321, San Francisco, CA, USA, May 24–27, 2021. IEEE Computer Society Press.

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

[21] Simon Josefsson. Streamlined NTRU Prime: sntrup761 – draft-josefsson-ntruprime-streamlined-00, 2023. https://datatracker.ietf.org/doc/draft-josefsson-ntruprime-streamlined/.

[22] Simon Josefsson. Classic McEliece – draft-josefsson-mceliece-03, 2025. https://datatracker.ietf.org/doc/draft-josefsson-mceliece/.

[23] Tanja Lange. ISO/IEC JTC1 SC27 WG2, SC 27 committee document 208, Post-Quantum Cryptography Part IV – Code-Based Cryptography, 2020. Part of https://committee.iso.org/files/live/sites/jtc1sc27/files/resources/SC%2027%20committee%20document%20208%20-%20Post-Quantum%20Cryptography.zip.

[24] Tanja Lange. ISO/IEC JTC1 SC27 WG2, SC 27 committee document 208, Post-Quantum Cryptography, Part VI — Isogeny-Based Cryptography, 2020. Part of https://committee.iso.org/files/live/sites/jtc1sc27/files/resources/SC%2027%20committee%20document%20208%20-%20Post-Quantum%20Cryptography.zip.

[25] Frank T. Leighton and Silvio Micali. Large provably fast and secure digital signature schemes based on secure hash functions, 1995. https://patents.google.com/patent/US5432852A/en.

[26] Patrick Longa, Joppe W. Bos, Stephan Ehlen, and Douglas Stebila. FrodoKEM: key encapsulation from learning with errors draft-longa-cfrg-frodokem-01, 2025. https://datatracker.ietf.org/doc/draft-longa-cfrg-frodokem/.

[27] Xianhui Lu and Le Trieu Phong. ISO/IEC JTC1 SC27 WG2, SC 27 committee document 208, Post-Quantum Cryptography, Part III – Lattice-Based Cryptography, 2020. Part of https://committee.iso.org/files/live/sites/jtc1sc27/files/resources/SC%2027%20committee%20document%20208%20-%20Post-Quantum%20Cryptography.zip.

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

[29] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on SIDH. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023, Part V*, volume 14008 of *Lecture Notes in Computer Science*, pages 448–471, Lyon, France, April 23–27, 2023. Springer, Cham, Switzerland.

[30] Jake Massimo, Panos Kampanakis, Sean Turner, and Bas Westerbaan. nternet X.509 Public Key Infrastructure – Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA), 2025. https://www.rfc-editor.org/rfc/rfc9881.txt.

[31] David McGrew, Michael Curcio, and Scott Fluhrer. Leighton-Micali Hash-Based Signatures. RFC 8554 (Informational), 2019. https://www.rfc-editor.org/rfc/rfc8554.txt.

[32] Rafael Misoczki. ISO/IEC JTC1/SC27/WG2, SC 27 committee document 208, Part II – Hash-Based Signatures, 2020. Part of https://committee.iso.org/files/live/sites/jtc1sc27/files/resources/SC%2027%20committee%20document%20208%20-%20Post-Quantum%20Cryptography.zip.

[33] Michael Naehrig, Erdem Alkim, Joppe Bos, Léo Ducas, Karen Easterbrook, Brian LaMacchia, Patrick Longa, Ilya Mironov, Valeria Nikolaenko, Christopher Peikert, Ananth Raghunathan, and Douglas Stebila. FrodoKEM. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

[34] NIST. FIPS 203 – Module-Lattice-Based Key-Encapsulation Mechanism Standard, 2024. Module-Lattice-BasedKey-EncapsulationMechanismStandard.

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

[36] Damien Robert. Breaking SIDH in polynomial time. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023, Part V*, volume 14008 of *Lecture Notes in Computer Science*, pages 472–503, Lyon, France, April 23–27, 2023. Springer, Cham, Switzerland.

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

[38] William Whyte, Nick Howgrave-Graham, Jeff Hoffstein, Jill Pipher, Joseph H. Silverman, and Phil Hirschhorn. IEEE p1363.1 draft 10: Draft standard for public key cryptographic techniques based on hard problems over lattices. Cryptology ePrint Archive, Report 2008/361, 2008.

[39] Bo-Yin Yang and Ward Beullens. ISO/IEC JTC1 SC27 WG2, SC 27 committee document 208, Post-Quantum Cryptography, Part V – Multivariate Cryptography , 2020. Part of https://committee.iso.org/files/live/sites/jtc1sc27/files/resources/SC%2027%20committee%20document%20208%20-%20Post-Quantum%20Cryptography.zip.

[40] Greg Zaverucha, Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Jonathan Katz, Xiao Wang, Vladmir Kolesnikov, and Daniel Kales. Picnic. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.