PQCSA

Post-Quantum Cryptography Support Action

Project number: Digital Europe 101190512

D1.3

Hot Topics and Open Problems in Post-Quantum Cryptography

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	

Hot Topics and Open Problems in Post-Quantum Cryptography

Nicolas Bon, Thibauld Feneuil, Jan Klaußner, Tanja Lange, Jonathan Levin, Matthieu Rivain, Mélissa Rossi, and Monika Trimoska

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
0.9	27 November 2025	First circulated version
1.0	30 November 2025	Minor edits after internal review by KUL and TCD

Abstract

This report provides an overview of current hot topics and open problems in post-quantum cryptography. It first presents the results of a community survey conducted among researchers and practitioners in post-quantum cryptography to gather their insights. Based on the survey responses and internal discussions within the PQCSA consortium, it then elaborates on a selection of topics identified as currently hot in the field and/or for which important open problems remain.

At a high level, our study highlights that continued progress in post-quantum cryptography requires strengthening the security foundations of existing schemes through cryptanalysis, advancing the efficiency and functionality of basic cryptographic primitives (KEMs and signatures), developing post-quantum counterparts of advanced primitives that are essential for modern privacy-preserving applications, and addressing the complex, multidisciplinary challenges posed by the global transition to PQC.

Keywords: WP1, post-quantum cryptography, hot topics, open problems

Contents

Chapter 1

Introduction

This report aims to present a comprehensive overview of the current hot topics and open problems in the field of post-quantum cryptography (PQC). PQC is a rapidly evolving area of research, driven by the imminent threat that quantum computers pose to traditional cryptographic schemes and by the need to anticipate this threat through a migration of our cryptographic infrastructure to quantum-resistant alternatives. As the field matures, identifying and addressing the most pressing challenges becomes essential to ensuring the security and efficiency of cryptographic systems in a post-quantum world.

The content of this report is partly based on a community survey conducted among researchers and practitioners in post-quantum cryptography. The survey aimed to gather insights on the most relevant and urgent topics, as well as the key open problems that must be addressed to advance the state of the art in PQC. The survey is presented in Chapter 2, which summarizes the methodology and main findings.

The report further elaborates on a selection of hot topics and open problems identified through the survey and internal discussions within the PQCSA consortium. These topics are presented in Chapter 3, organized into thematic sections covering families of post-quantum cryptographic schemes, security aspects, advanced primitives and protocols, and real-world aspects and use cases. Each section presents the progress achieved and the challenges that remain.

The report concludes with a summary of the key findings and recommendations for future research directions in post-quantum cryptography.

Chapter 2

Community survey

2.1 Survey description

In the preparation of this document, a community survey was conducted to gather insights on hot topics and open problems in post-quantum cryptography from the community. The results of this survey are summarized in this chapter.

The survey included three main sections with the following questions:

1. **Hot topics:** *From your perspective, which topics are currently attracting the most attention in post-quantum cryptography research, and which directions appear most promising?*

2. **Open problems:** *What do you see as the most critical open problems in post-quantum cryptography? Are there any areas where you feel progress is urgently needed?*

3. **Topics needing more attention:** *In your opinion, which topic(s) or open problem(s) in post-quantum cryptography should receive more attention than they currently do, either today or in the near future?*

Other optional sections of the survey collected background information on the respondents as well as additional thoughts, concerns, or predictions they would like to share.

A total of 54 responses were received from a diverse group of researchers and practitioners in the field of post-quantum cryptography. The respondents included primarily academic researchers (approximately 65%), many of whom are internationally recognized experts and long-standing contributors to PQC theory, cryptanalysis, and design. A significant fraction came from industry (about 35%), spanning semiconductor companies, large technology firms, secure hardware vendors, and telecommunications providers, often working on implementation, deployment, or product integration of PQC as well as standardization.

2.2 Survey results

Table 2.2.1 summarizes the responses to the three main questions of the survey. For each topic, the table indicates the number of times it was mentioned as a hot topic, an open problem, or a topic needing more attention. We only report numbers of occurrences ≥ 3. We stress that the questionnaire was made of open-ended questions with free-text responses so that there is a part of interpretation in the classification of the answers. We also acknowledge that the sample may be somewhat biased, as we contacted experts in all areas of post-quantum but without a systematic selection process balancing the numbers between different areas. The counts should therefore be taken with a grain of salt and not over-interpreted quantitatively. Nevertheless, we believe they are indicative of current trends. We provide more detailed analysis and discussion of the survey results hereafter.

2.2.1 Families of cryptosystems

The MPC-in-the-Head family was frequently mentioned as a hot topic, arguably due to the number of schemes based on this paradigm in the ongoing NIST process, as well as the recent surge of related research. It was, however, less often cited as a critical or urgent open problem, or as a topic needing more attention. This may reflect a perception that the area is already well studied and currently receives substantial attention from the community.

Isogeny-based cryptography was also often cited as a hot topic and identified as particularly promising for achieving signatures with small public keys and signature sizes, albeit with performance that remains slow compared to other families. Improving the efficiency of isogeny-based schemes was therefore highlighted as a key open problem.

Lattice-based cryptography was mentioned repeatedly as the predominant family in today's PQC landscape, featuring the first standards, and as the most promising foundation for cryptographic primitives with advanced functionalities.

The importance of maintaining diversity across cryptographic families was raised in all three categories. This was most commonly meant as a call to investigate families beyond lattices, which currently dominate. Specific mentions included code-based cryptography (notably in the rank metric and code-based trapdoor functions) and multivariate cryptography (especially UOV/MAYO-style signatures).

2.2.2 Cryptanalysis and security

Cryptanalysis and security assessment of quantum-hard problems were mentioned prominently across all question categories. This reflects the widely shared feeling that advances in cryptanalysis – as a hot topic, as a source of major open problems, and as an area requiring more attention – are essential for building confidence in the hardness assumptions underlying PQC. One respondent emphasized the importance of publishing negative results (i.e., unsuccessful attacks) to further reinforce trust in these assumptions.

Several comments focused on family-specific cryptanalytic challenges. For lattices, many respondents highlighted the need to better understand the hardness of structured lattices (e.g., ideal lattices, ring/module LWE), as well as the concrete security of the problems underlying lattice-based KEMs and signature schemes, ML-KEM and ML-DSA in particular. Some respondents noted the existence of a "lattice assumption zoo" in the literature and called for more work to assess the real hardness of these assumptions.

Beyond lattices, several respondents mentioned open problems in code-based cryptography, including decoding of quasi-cyclic codes, the code equivalence problem, and rank-metric decoding. Multivariate cryptography was mentioned less frequently, mainly in relation to UOV-style signatures.

Quantum cryptanalysis was repeatedly identified as an area of critical/urgent open problems and requiring more attention. Respondents stressed the difficulty of validating quantum attacks, as exemplified by the fact that when a quantum attack on LWE is proposed, only a

Table 2.2.1: Summary of survey responses. For each topic, the table indicates whether the number of times it was mentioned in the responses to the first question (hot topics), the second question (open problems), or the third question (topics needing more attention). We only report numbers of occurrences ≥ 3.

	Hot topics	**Open problems**	**More attention**
Families of cryptosystems			
Isogeny-based cryptography	8	3	
MPC in the head	8		
Lattice-based cryptography	5		
Diversity of families & problems	3	4	3
Cryptanalysis and security			
Cryptanalysis / security of problems	9	14	10
Quantum cryptanalysis		5	7
Cryptanalysis / security of lattices		5	4
Cryptanalysis / security of codes			3
Implementations			
SCA & implementation security	14	10	5
Implementation & performances	7		
Formally verified implementations		4	
Basic cryptographic primitives			
Signature schemes	10	3	
KEM & signature schemes	3		
Advanced cryptographic primitives			
Advanced cryptographic primitives	10	4	
Blind signatures & anonymous credentials	7	4	
Fully homomorphic encryption (FHE)	6		
Privacy-enhancing technologies (PETs)	4		
Zero-knowledge proofs (ZKPs) & (zk-)SNARKs	3		
Real world aspects			
Transition to PQC / deployment of PQC	10	13	8
Hybrid schemes	7	8	4
Standardization	3		
PQC for IoT & embedded systems	3		

handful of experts can thoroughly evaluate it while the broader community holds its breath. Suggestions included closer collaboration between quantum computing specialists and cryptanalysts, as well as the development of concrete quantum-cost models for security evaluation. Hybrid classical-quantum attacks were also mentioned as an important open research direction.

2.2.3 Implementations

We grouped mentions of side-channel analysis (SCA) and implementation security – including the study of side-channel attacks and the design of countermeasures – into a single category. This category was among the most frequently cited across all three question types. While attacks were discussed to some extent, most mentions concerned countermeasures and secure implementations. In addition to SCA, some respondents mentioned fault injection attacks (FIA) and micro-architectural attacks. Although many answers remained general (e.g., "secure implementations against SCA"), some respondents specifically highlighted the need for provably secure masked implementations and higher-order masking to achieve strong assurance levels.

A second implementation-related category covers performance and optimization aspects (including hardware acceleration and dedicated PQC instructions). This was cited primarily as a hot topic. Finally, formally verified implementations were mentioned several times as a critical/urgent open problem.

2.2.4 Basic cryptographic primitives

Key encapsulation mechanisms (KEMs) and signatures were occasionally mentioned as a combined category, but signatures alone received significantly more citations, especially as a hot topic. This is likely due (and was sometimes explicitly attributed) to the ongoing NIST standardization process currently focusing on signatures. Respondents also emphasized the critical importance of PKI and certificates across many applications, which makes signatures crucial for the broader PQC transition. For both signatures and KEMs, respondents underscored the need for improvement, particularly in terms of reducing public-key sizes, signature sizes, and ciphertext sizes for KEMs. One respondent argued that IND-CCA2-secure KEMs, as standardized by NIST, may be unnecessarily strong for many applications where more efficient IND-CPA-secure schemes could suffice.

2.2.5 Advanced cryptographic primitives

Advanced cryptographic primitives were mentioned extensively across all three categories, underscoring the perceived importance of this research area. These included advanced signatures (e.g., blind, group, ring, deniable, and aggregate signatures); advanced encryption schemes (e.g., IBE, ABE, proxy re-encryption); multi-party computation (MPC); threshold cryptography; oblivious pseudorandom functions (OPRFs); private set intersection (PSI); fully homomorphic encryption (FHE); zero-knowledge proofs (ZKPs) and succinct non-interactive arguments of knowledge (SNARKs); privacy-enhancing technologies (PETs); and anonymous credentials.

Respondents referred to these primitives either generically (e.g., "advanced primitives" or "advanced functionalities"), by listing some examples, or by mentioning one or a few specific primitives. One may also note that several of the primitives mentioned below overlap conceptually, and some refer to broad categories (e.g., MPC, PETs). For this reason, the counts reported in Table 2.2.1 may also overlap and should be interpreted only as indicative of general trends.

2.2.6 Real-world aspects

We grouped together mentions relating to PQC transition or migration as well as PQC integration or deployment in real-world applications. This category was among the most frequently cited across all questions, and particularly in the "critical/urgent open problems" category. This emphasizes the widely shared feeling of importance and urgency of this area. Respondents highlighted the need for practical migration strategies and concrete crypto-agility solutions (including secure update mechanisms), as well as rigorous assessments of PQC's impact on system performance and network bandwidth, especially given the larger key sizes, signatures, and ciphertexts involved. Several respondents expressed concerns about readiness for the transition, particularly in view of the ambitious timelines set by the EU PQC roadmap and the challenges posed by legacy systems, some of which have struggled even to adopt modern traditional cryptography.

Hybrid schemes (or protocols, implementations) – combining traditional public-key cryptosystems (RSA, ECC) with post-quantum ones – were also widely mentioned in all three categories.

Standardization was mentioned several times, primarily as a hot topic. Respondents pointed to the NIST process as a major driver of research. Some emphasized the need for standardization efforts beyond NIST, particularly in Europe, to ensure autonomy and diversity. One respondent explicitly called for establishing a European PQC standardization task force to coordinate such efforts.

2.2.7 Applications and use-cases

Several respondents mentioned PQC applications in IoT and embedded systems, especially as a hot topic. Due to the limited memory available in many IoT / embedded devices, they stressed the need for schemes with sufficiently small RAM footprints. Achieving this while also supporting high-assurance implementations (e.g., with higher-order masking) was noted as particularly challenging. Other application areas mentioned included blockchain technologies, electronic identity, DNS, satellite ground segments, messaging applications, and e-voting systems.

2.2.8 Other topics

Finally, a few additional themes emerged from the survey. Some respondents emphasized the strategic importance of PQC in the current geopolitical climate and expressed concern that cryptographic capabilities may become tools of power. Regarding quantum risk, several respondents questioned the likelihood of large-scale quantum computers materializing soon, while one respondent highlighted the possibility that advances in AI could accelerate progress in quantum hardware research, potentially creating pressure for rapid PQC adoption.

The need for education was also raised: respondents stressed the importance and difficulty of educating current and future generations about PQC, given its greater complexity compared to traditional cryptography and its multidisciplinary nature.

Chapter 3

Selected topics

This chapter presents a selection of topics that we identified as currently hot in the field and/or for which important open problems remain to be solved. These topics were chosen based on the responses to the community survey reported in Chapter 2, as well as internal discussions within the PQCSA consortium and proposals from external contributors. Each topic is presented in a structured manner, highlighting its importance, summarizing the current state of the art, and outlining the key open problems that need to be addressed.

A first set of topics focuses on specific families of post-quantum cryptographic schemes. We include lattice-based cryptography as the most mature and widely researched family of post-quantum schemes, as well as isogeny-based cryptography and MPC in the Head, which are currently particularly active research areas.

A second set of topics addresses the security of post-quantum cryptography. We cover general cryptanalysis, quantum cryptanalysis, cryptanalysis with extra information, and side-channel analysis and protected implementations.

We then present a set of advanced post-quantum cryptographic primitives and protocols, including blind signatures and anonymous credentials, and fully homomorphic encryption, which were particularly emphasized in the survey. We also include threshold cryptography, currently a hot topic in cryptographic research, and oblivious pseudorandom functions, which have recently received increased attention.

Finally, we consider real-world aspects of post-quantum cryptography, including the PQC transition and hybrid cryptographic schemes, as well as two exemplary use cases for which the transition is crucial: digital identity and e-voting.

We stress that this selection is not exhaustive, and many other important topics in post-quantum cryptography exist. In particular, code-based cryptography and multivariate cryptography are also essential families that contribute to the diversity of the post-quantum ecosystem. Numerous other advanced primitives, protocols, and use cases are likewise relevant and significant. The topics selected here are intended as illustrative examples, providing insight into some of the most pressing challenges and opportunities in post-quantum cryptography today.

3.1 Families of post-quantum cryptographic schemes

3.1.1 Lattice-based cryptography

Lattice-based cryptography represents the most extensively researched area within post-quantum cryptography. Euclidean lattices, which consist of regularly spaced discrete points in multidimensional space, serve as the underlying mathematical structure. These discrete structures were investigated as mathematical objects well before their application to cryptography. They provide a rich source of hard mathematical problems that are conjectured resistant to quantum attacks, like the shortest vector problem (SVP). In the past decades, particular cases and variants of the SVP have become the basis for designing post-quantum cryptographic primitives and protocols, including public-key encryption schemes, digital signatures and more.

Why is this topic important? Lattice-based cryptography was the first family of post-quantum cryptography to attain efficient algorithms making them suitable for practical applications. The structured variants of hard lattice problems allow designing schemes with competitive sizes and computation time comparable to traditional schemes based on factorization or discrete logarithm assumptions. Moreover, lattice structures can be used for advanced functionalities, such as fully homomorphic encryption, which allows computations on encrypted data without decryption, enabling new applications in secure data processing and cloud computing. The number of researchers and research projects has spectacularly increased since 2010 and lattice-based cryptography is now considered as one of the most mature field in post-quantum cryptography. The NIST standardization process for post-quantum cryptography has selected three lattice-based schemes as first standards. These selections highlight the practical viability and importance of lattice-based cryptography in the post-quantum ecosystem.

Overview of the state of the art. The state of the art of lattice-based cryptographic is very rich. Two of the key contributions of the domain were the worst-case hardness reduction, as introduced by Ajtai in 1996 [Ajt96], and the introduction of the Learning With Errors (LWE) problem by Regev in 2005 [Reg05], which has become a foundational assumption for many lattice-based cryptographic constructions. The constructions of public-key encryption schemes, such as the one by Peikert in 2009 [Pei09], and digital signature schemes, like the GPV signature scheme by Gentry, Peikert, and Vaikuntanathan in 2008 [GPV08] or the Fiat-Shamir with aborts [Lyu12], have demonstrated the practical viability of lattice-based cryptography. In recent years, there has been significant progress in optimizing lattice-based schemes for efficiency and security. Techniques such as ring-LWE and module-LWE have been introduced to reduce key sizes and improve computational efficiency, making lattice-based cryptography more practical for real-world applications. One can cite the selected NIST standard ML-KEM, ML-DSA or FN-DSA [SAB+22, LDK+22, PFH+22] as concrete state-of-the-art implementations. Additionally, the development of advanced functionalities, such as fully homomorphic encryption schemes (see Section 3.3.2) has opened new avenues for secure computation on encrypted data.

Open problems. Despite the significant advancements in lattice-based cryptography, many open problems and challenges remain. One of the primary concerns is the need for further analysis of the security of lattice-based problems. While exponential, the complexity of the current best attacks based on lattice reduction is still not fully understood, preventing precise parameter dimensioning. This research track is also related to the analysis of residual security in the presence of extra information (see Section 3.2.3).

Another open problem is the estimation of the security of the structured variants of lattice problems. While these variants offer improved efficiency, their security is conjectured to be close to the standard unstructured lattice-problems. Further research is needed to establish a more comprehensive understanding of the security implications of these structured variants.

Finally, there is a need for continued exploration of new lattice-based constructions and protocols that can provide enhanced functionalities. This includes the exploration of new applications in areas such as broadcast encryption, attribute based encryption, secure multi-party computation or zero-knowledge proofs.

3.1.2 Isogeny-based cryptography

Isogeny-based cryptography is a post-quantum family that is built on findings from both algebraic number theory and algebraic geometry. It can be seen as the post-quantum successor of elliptic curve cryptography, as it mainly studies elliptic curves and maps between them, called isogenies. This is the most fast-growing and fast-moving area of PQC at the moment, mainly because recent advances have brought many new computational tools, resulting in even more new cryptographic schemes. There are however cryptographic schemes that have received a good level of scrutiny in this area, namely the CSIDH [CLM+18] group action that allows for a Diffie-Hellman key exchange, incl. static-static exchanges, and the SQIsign [DKL+20] digital signature scheme.

Why is this topic important? The cryptographic schemes whose security relies on the hardness of isogeny-related problems have particular use cases. They usually offer very small signatures and public key sizes, but have one of the longest running times. As such, they are suitable for applications where having small sizes is a requirement, while it is possible to handle longer running times. Prominent examples of this are the SQIsign signature scheme developed originally in 2020, and PRISM [BBC+25], a signature scheme introduced this year. Isogeny-based cryptography is also known for offering the only post-quantum commutative group action, hence being the only family that has a post-quantum key exchange protocol with the well-known Diffie-Hellman construction.

Overview of the state of the art. The earliest appearances of isogenies in cryptography are in 2006 with the proposal of the CGL hash function [CLG09] and the Couveignes-Rostovtsev-Stolbunov [Cou06, RS06] construction for a quantum-resistant key-exchange protocol. The CGL hash function is too slow to use in practice and its significance mainly lies in showing that interesting and robust cryptographic solutions can be constructed based on the hardness of the isogeny path-finding problem. The same could be said initially for the Couveignes-Rostovtsev-Stolbunov construction. However, a series of advances starting in 2010 led to this proposal being the cornerstone for building the two most well-known key-exchange solutions, that is SIDH [JD11] and CSIDH [CLM+18]. The SIDH construction was later turned into a KEM and the concrete instance named SIKE was submitted to the NIST call for standardization. SIKE reached the fourth round before suffering from a polynomial-time attack and being deemed insecure beyond repair [CD23, MMP+23, Rob23]. This attack however did not affect, neither CSIDH, nor the then less explored SQIsign. Hence, the focus was turned to these two cryptosystems and the related problems. Interestingly, the tools used in the attack on SIDH were immediately put to use for constructive applications and have led to significant improvements on SQIsign [DLRW24, NOC$^+$24, BDD$^+$24] and the development of many new cryptographic schemes. As previously mentioned, isogeny-based cryptosystems battle with significant computational efforts, but offer very favorable sizes. Notably, SQIsign, one of the isogeny-based digital signature schemes is currently in the second round of the NIST call for additional signatures. It has public key sizes of only 65 bytes and yields 148-byte long signatures for the first level of security. The signing times were prohibitive in the first round, but they have significantly dropped in the second round, down to 101 megacycles. Verification times have also improved to 5 megacycles.

Open problems. Isogeny-based cryptography is currently one of the fastest growing research areas with new computational approaches discovered continuously. This is evidenced, for instance, by the significant change in performance of SQIsign mentioned above, which also indicates that there are unexplored venues for optimization of isogeny-based systems. The most pressing challenges are making isogeny computations (referred to in this area as *representations*) more efficient and gaining more confidence in the security. The former challenge is the most studied, but not unique, part of a bigger challenge, that is, making isogeny-based schemes more efficient. Recent discoveries that stemmed from cryptanalysis have been used extensively for constructive purposes in the past three years. They have opened an abundance of new directions, and they are all focused on building more functionalities out of isogeny-based constructions, optimizing the existing ones and generally getting a better understanding of the rich underlying structure of the mathematics used in this area. For the latter, cryptographers often pair up with pure number theorists to discover new directions. Thus, this notably small community continues to grow. The security challenges are focused on one side on understanding better the quantum security of CSIDH and on obtaining reductions to the core isogeny path-finding problem for other schemes including SQIsign. In the CSIDH setting, there is also a growing focus on protection against physical attacks.

3.1.3 MPC in the head

In their seminal work [IKOS07], Ishai, Kushilevitz, Ostrovsky and Sahai introduced a generic paradigm for constructing zero-knowledge proofs of knowledge using techniques from secure multiparty computation. This paradigm now commonly known as MPC-in-the-Head (MPCitH) has considerably evolved since its introduction in 2007. While mostly of theoretical interest at first it now consists of a rich family of practical zero-knowledge proof systems, applicable to prove any statements and whose security solely relies on symmetric primitives, based on constructions such as GGM trees or Merkle trees.

Why is this topic important? The MPCitH paradigm has recently become a hot topic in post-quantum cryptography, as it underpins several modern signature schemes, including candidates in the ongoing NIST process (see, e.g., [BBB$^+$24, BBFR24, ABB$^+$24]). Applying MPCitH (combined with the Fiat-Shamir transform) to any one-way function or hard problem yields a signature scheme with competitive performance in both signature size and computational cost. This generality is particularly attractive today, as the community seeks to diversify the hardness assumptions supporting post-quantum cryptography. In particular, it enables the use of conservative assumptions without trapdoors or algebraic structure, and even the construction of efficient signature schemes based solely on symmetric primitives (e.g., FAEST), thereby avoiding the need for hybridization and achieving a better performance profile than SLH-DSA (SPHINCS$^+$). Beyond signatures, MPCitH also provides versatile post-quantum zero-knowledge proofs which are instrumental to privacy-enhancing technologies (PETs) and actively secure MPC.

Overview of the state of the art. The first practical instantiation of MPCitH was introduced by ZKBoo [GMO16], which later yield Picnic, a candidate in the first NIST PQC standardization process [ZCD$^+$20]. A significant improvement came with the introduction of GGM trees to substantially reduce signature sizes [KKW18]. Since 2020, starting notably with [BN20], research on MPCitH has grown rapidly. The most efficient modern variants are the VOLE-in-the-Head framework [BBD$^+$23] and the Threshold-Computation-in-the-Head framework [FR25b]. Notably, six of the fourteen candidates selected in round 2 of the ongoing NIST process rely on these techniques. These schemes achieve signatures as small as 2.5–5 kB, extremely short public keys (often a few hundred bytes), and signing times of only a few milliseconds on modern hardware.

Beyond signatures, MPCitH-based proof systems such as Ligero [AHIV17, AHIV23] and TCitH-MT [FR25b] offer highly efficient provers and relatively succinct proofs for a broad range of circuits, beyond the small circuits typically used in signature schemes. These systems are particularly effective in applications such as proving possession of private keys in lattice-based schemes, among many other zero-knowledge use cases.

Open problems. Although several MPCitH schemes now achieve small communication costs, the implementation aspects remain underexplored. Important challenges include producing highly optimized implementations across different platforms, understanding the behavior of MPCitH schemes under physical attacks, and developing robust side-channel protections. In addition, while some works have begun to analyze certain MPCitH schemes in the quantum random-oracle model (QROM) [AHJ$^+$23, BBB$^+$25b], further research is required to deepen our understanding of their security against quantum adversaries. Finally, although substantial new improvements in proof size or computational efficiency may be more difficult to attain as the field has matured, such improvements remain an important and open direction for future works.

3.2 Security of post-quantum cryptography

3.2.1 Cryptanalysis

Cryptanalysis is the study of the security of cryptosystems. It refers to developing attacks on cryptosystems and algorithms for solving their underlying problems, as well as an analysis on their time and (sometimes) memory complexity. The end goal is to derive parameter sizes that achieve the desired level of security while optimizing for a target criterion, such as small sizes, efficiency, or the best trade-off for both. State-of-the-art algorithms with the best time complexity are used as reference for deriving these parameters.

Why is this topic important? It can not be overstressed how important cryptanalysis is, as the cryptographic systems being secure against attacks is crucial. All the other criteria like efficiency and advanced functionality can only come secondary to having confidence in the security of systems before they are deployed for real-world use. Cryptosystems that are deployed currently or in the future should be protected against both attackers with a regular machine and attackers equipped with a quantum computer to ensure sensitive data remains confidential and for the digital world to continue to function.

Overview of the state of the art. Cryptanalysis encompasses both regular cryptanalysis, that is, attack using a non-quantum computer only, and quantum cryptanalysis where the core part of the attack relies on quantum operations. We take a closer look at the latter in Section 3.2.2. For regular cryptanalysis, there usually exist two approaches for gaining confidence in the security of the cryptosystem. When the security of a cryptosystem relies on the hardness of a well-known computationally hard problem, and this is formally proven, the cryptosystem is called provably secure. This gives stronger confidence in its security, since we are able to prove that attacking the system is at least as hard as solving the relevant long-standing problem. In this case, the cryptanalysis tasks are focused around developing best algorithms for solving the underlying problem and exact complexity analysis. For cryptographic designs where such a formal reduction has not been proven, the systems are often referred to as "ad-hoc". The only way to gain confidence in their security is by extensive cryptanalysis, by looking carefully into the cryptographic constructions and finding all possible points of entry. Cryptographic attacks in post-quantum can have several flavors, with general appraoches ranging from purely combinatorial algorithms to the algebraic cryptanalysis approach where the problem at hand is reduced to the problem of solving a quadratic system of polynomial equations, and specialized approaches using advanced mathematics specific to the attacked system.

Open problems. The security analysis of all families except for hash-based cryptography needs to receive extensive attention and the survey responses agree with this reasoning. The hardness of the lattice problems is considered to be well understood at a high level, but exact cryptanalysis is still needed for many algorithms. In code-based cryptography, the decoding problem in the Hamming metric has the most extensive analysis. The rank metric is also better understood in recent years, and there are other metrics with early cryptanalysis results. There is another side of code-based cryptography that focuses on the *equivalence problem.* This area is newer in cryptanalysis and has seen rapid development recently. Understanding the hardness of this problem in the Hamming metric is the most urgent currently. The cryptanalysis in multivariate cryptography focused heavily on the Unbalanced Oil and Vinegar (UOV) family. Understanding the security of all modified UOV variants is still considered an open problem. In isogeny-based crypto, the hardness of the unmodified isogeny path-finding problem is well understood, but an exact complexity analysis is still needed. An equally pressing matter is to analyze the novel constructions that have been developed recently and understand how tightly they are connected to the core isogeny problem. Better algorithms for solving the multivariate quadratic (MQ) problem are also an important direction as many areas in cryptography rely on algebraic cryptanalysis. In PQC, the most notable are code-based and multivariate cryptography. Understanding the complexity of these algorithms in a precise manner is an even more complex and urgent task.

3.2.2 Quantum cryptanalysis

Several of the respondents mentioned quantum cryptanalysis as a pressing open problem, beyond the need for cryptanalysis in general, as covered in Section 3.2.1. Quantum cryptanalysis refers to studying attacks using the additional power of quantum operations. While, in principle, non-quantum attacks are included, the term is typically used only for attacks that have a significant component of the quantum algorithm.

Why is this topic important? Post-quantum cryptography addresses the challenge to protect data and communication against attacks by quantum computers. Hence, quantum cryptanalysis should be at the core of research in PQC. However, there is a problem with finding funding for performing cryptanalysis and the time investment needed to research *quantum* cryptanalysis is even greater as the researchers need to become experts in quantum algorithms, a field which still is heavily drawing on notations from physics, as well in cryptanalysis. It is much easier to understand the cryptosystem than to imagine all possible ways to attack it. However, PQC systems are now being deployed and we must get a better understanding of their security. Deploying PQC along with pre-quantum systems mitigates the direct impact if the PQC system turns out to be less secure than assumed, however, the current feeling is still that there might be devastating attacks that have so far simply been overlooked due to the lack of expertise and task force.

Even if there are no new attacks that lead to exponential improvements, subexponential attacks require very different scaling of parameters, as we know well from the contrast of ECC and RSA key sizes among the pre-quantum systems. In the other direction, our current estimates might be giving too much power to quantum computers, putting their clock speeds at par with conventional computers and assuming quasi unlimited scalability. Hence, more precise quantum cryptanalysis might even lead to decisions that parameters can be scaled down (assuming that the quantum attack caused the recommendations rather than the regular cryptanalysis).

In summary, we need research in quantum cryptanalysis to answer if we can scale down some parameters, must scale up some parameters, or must even completely remove a problem from the zoo of PQC systems.

Overview of the state of the art. All major categories of PQC systems have received some study to assess if quantum attacks apply, in particular, if (a part of) the solution can be reformulated in a way that Shor's attack can be applied. Negative results typically do not get published, and these studies go back to the very early days of PQC and are reported only in the introduction to those early papers, giving no details of how the study was executed. A notable exception is [DMR11] from Crypto 2011 which studied applicability of the quantum Fourier transform, the main ingredient in Shor's algorithm, to some component of decoding attacks on the McEliece system and concluded that no quantum speedup was possible. However, this paper is also a prime case for the need for collaboration between cryptanalysts and researchers in quantum algorithms, as the part that was scrutinized in the paper is not the hard part in the McEliece cryptosystem and is even efficiently solved by Sendrier's support-splitting algorithm [Sen00]. More meaningful collaborations have in the meantime led to studies of quantum attacks on the main PQC systems which work out the details of how to apply Grover or quantum walks to speed up existing non-quantum attacks, at different levels of granularity of the result. This still leaves the feeling that novel approaches remain to be found when departing from these known attack strategies. In several cases, the quest for better quantum attacks on PQC has led to breakthroughs in finding *non-quantum* attacks, but there are also cases like the attack by Campbell, Groves, and Shepherd [CGS14] on 1-dimensional cyclotomic lattices and generalizations of the Soliloquy attack that are inherently quantum attacks. This is a good example of an attack that required expertise in number theory, lattices, and quantum computing. Similarly, Childs, Jao, and Soukharev showed in [CJS14] how to apply Kuperberg's algorithm for solving the hidden-shift problem to CRS, an isogeny-based system proposed 8 years earlier. This results in a subexponential quantum attack on the system while the best known non-quantum attack on the system has exponential time.

Open problems. One open problem, that also got highlighted in the survey answers, is to define the basic cost model. A relatively recent example of this relates to the just mentioned attacks on CRS. These are known to apply to the CSIDH system [CLM+18], as pointed out by the designers, meaning that the system has a subexponential quantum attack. Some papers [BS20, Pei20] (in particular their early preprint versions) focused on studying optimizations of Kuperberg's algorithm and counted cost in the number of oracle queries, concluding that the parameters were chosen way too small. However, [BLMP19] developed quantum circuits to compute the oracle function and showed that each oracle call involves 2^{40} quantum operations for the CSIDH-512 parameter set, a significant cost that cannot be ignored. Additionally, the same discussions play out as in non-quantum attacks regarding the costs of memory access and whether to count operations at gate/bit level or in larger units like computer words. This is already a disputed question for non-quantum attacks and even harder to agree on for quantum attacks where the very hardware that they will run on is still in the research state.

Obvious open problems are better quantum attacks on codes, isogenies, lattices, and MQ systems, both asymptotically and in a concrete cost model counting qubits and gates. The latter are needed to settle which parameters to choose, but might feel premature when the best attacks are still evolving. Nevertheless, research in exact or fine-grained cryptanalysis needs to evolve and reach a maturity of computer-verified counts and (proof-of-concept) implementations in quantum programming languages, which can happen in parallel with improvements in asymptotic algorithms. Furhtermore, the quantum proramming languages and options for simulations may need to be upgraded, creating open problems on a meta level.

Finally, a very understudied area is how to use smaller or near-term quantum computers. This puts a severe limit on the number of qubits and on the maximum depth of the computation. For attacks on the pre-quantum system RSA the paper [BBM17] studies how to use a small quantum computer to aid factorization. An open problem for each of the PQC systems is whether a quantum speedup can be achieved with such a smaller scale computer by investigating a different part of the trade-off curve or if a quantum computer could be used as coprocessor within a larger, otherwise non-quantum attacks. Given that the term "hybrid" is overloaded, we refer to such attacks as "quantum-assisted" attacks. Whatever the name, the impact of such attacks on pre- and post-quantum cryptography is a big open problem.

3.2.3 Cryptanalysis with extra information

The security of post-quantum schemes is based on clearly defined hard mathematical problems conjectured resistant to quantum attacks. Their analysis is at the core of the theoretical research in post-quantum cryptography: while theoretical security reductions provide confidence in the security, the complexity analysis of the best attack techniques allows choosing concrete parameters. However, in practical settings, these assumptions must be considered within the broader context of cryptographic algorithms, themselves inside protocols and physical implementations. A large emerging domain in post-quantum cryptanalysis is the study of the residual security of post-quantum schemes in the presence of different types of extra information about the secret key, often called hints. By exploiting these additional sources of information, attackers can potentially compromise the security of post-quantum cryptographic schemes that are otherwise considered secure. The extra information can take various forms, that can be classified into 2 families: the hints coming from side-channel analysis, and the hints coming from the protocol design. In the first one, the information is often a noisy measurement that is correlated to a function (Hamming weight for example) of the secret key; it can also be an a posteriori probability distribution on the secret key (see Section 3.2.4). In the second one, the hints can be derived from leakages intrinsic to the execution of the protocol, such as aborts or extra outputs.

Why is this topic important? The study of cryptanalysis with extra information is crucial for ensuring the robustness and reliability of post-quantum cryptographic systems in real-world scenarios. For side-channel hint analysis, the certification of products often requires providing a criticality level of a measured leakage. To be able to assess the criticality, the measured leakage should be translated to the remaining cryptanalytic attack. The fine analysis of the hints allows for a better understanding of the overall security level of a given implementation. For the protocol-based hints, such an understanding directly leads to more efficient designs, by allowing well-chosen hints to be given to the attacker, going towards even better performance without sacrificing security.

Overview of the state of the art. It is a domain at the intersection of the side-channel attacks and the mathematical study of the post-quantum assumptions. Such an analysis requires expertise in both domains, which are often disjoint communities. It has nevertheless been studied in ad-hoc manners either on specific side-channel attacks or on the assumptions side. An attempt of systematic analysis was done in the context of lattice-based schemes in [DDGR20] and follow-ups. But, this research track is limited to specific types of hints. On the code-based side, a first work proposing the inclusion of hints in the ISD framework was proposed in [HPR+21].

Open problems. Several research directions remain open in this area. First, while the analysis has begun for code-based and lattice-based schemes, it needs to be extended to cover all post-quantum assumptions, including multivariate, hash-based, MPCitH, and isogeny-based cryptography. Second, there is a need for developing systematic frameworks and open-source tools to assess the impact of hints on the security of post-quantum assumptions. Finally, achieving greater generality remains the major challenge, requiring the study of new types of hints from both side-channel analysis and protocol designs, and the development of unified models for leakages and hints.

3.2.4 Side-channel analysis and protected implementations

Side-channel analysis (SCA) encompasses a range of techniques that exploit unintended physical information leakage from cryptographic implementations to compromise their security.

This leakage can manifest through timing variations, power consumption patterns, electromagnetic emissions, acoustic signals, temperature measurement, etc. Side-channel attacks have become a significant concern in the field of cryptography, as they can bypass traditional black-box security and exploit vulnerabilities in the implementation rather than the underlying mathematical foundations. The protected implementations aim to mitigate the risks associated with side-channel attacks by employing various countermeasures at the algorithmic level. One prominent example is masking, which involves randomizing intermediate values during computations to obscure the correlation between the secret data and the observable side-channel information.

Why is this topic important? Understanding and mitigating side-channel vulnerabilities for these wide-spread applications is crucial for ensuring the overall security of daily-life products such as smart cards, IoT devices, mobile phones and so on. Given the devastating impact that side-channel attacks can have on cryptographic systems, governments and standardization bodies have recognized the importance of addressing these threats. Standards such as FIPS and Common Criteria include requirements for side-channel resistance, prompting manufacturers to implement robust countermeasures in their products.

Overview of the state of the art. The SCA concept was introduced independently of the post-quantum threat and can target any cryptographic algorithm [Koc96]. The avenue of new post-quantum algorithms and new underlying structures is of particular importance in the context of SCA since many post-quantum schemes have high computational and memory requirements, new structures with sometimes a lot of redundancy. All these features can exacerbate side-channel leakage. On the attack side, various powerful techniques have been developed, demonstrating the important vulnerabilities of various post-quantum cryptographic algorithms. One can cite for example [ACK+23, RHHM17, BFM+19] among the many published works on the domain. This study is also close to the cryptanalysis with side information in Topic 3.2.3. On the constructive side, numerous countermeasures have been proposed and implemented. Masking techniques have been extensively studied and refined to be applied to post-quantum cryptographic algorithms. Notable advancements include high-order masking schemes, which provide enhanced security against sophisticated attacks, e.g. [BBE+18, BGR+21, DR24]. Additionally, algorithmic modifications and implementation strategies have been developed to minimize side-channel leakage, such as constant-time implementations and noise generation techniques. One can cite [HPRR20] for example. However, the protected implementations lead to significant overheads in terms of performance and resource consumption.

Another line of research focuses on designing PQC algorithms that are inherently compatible with the efficient application of side-channel countermeasures, masking in particular. For instance, some lattice-based cryptographic schemes have been designed by leveraging their mathematical properties to ease the application of masking [dEK+23]. The performance of these schemes is often better than generic schemes with protected implementations.

Open problems. Balancing security and efficiency remains a critical challenge in the field of side-channel analysis and protected implementations. One open problem is the development of more efficient masking schemes that can provide robust security without incurring significant performance penalties. One other open problem would be to design new post-quantum algorithms that are inherently resistant to side-channel attacks, reducing the need for complex countermeasures. Finally, the evaluation and certification of side-channel resistant implementations remain an ongoing challenge. Developing standardized methodologies for assessing the effectiveness of countermeasures and ensuring compliance with security standards is crucial for the widespread adoption of secure cryptographic implementations.

3.3 Advanced primitives and protocols

3.3.1 Blind signatures and anonymous credentials

Blind signatures and anonymous credentials are two common building blocks of cryptographic protocols that are frequently used to achieve strong privacy guarantees for users. In the 1980s Chaum introduced both of these concepts (blind signatures [Cha82], anonymous credentials [Cha85, CE87, CL01]), which share related motivations but are applied in different use cases. Namely, they are both solutions to the challenge of proving the authenticity of some user attribute/credential (in the case of anonymous credentials) or the validity of a digital token (in the case of blind signatures), while also allowing the user to maintain their privacy/anonymity.

In [Cha82], blind signatures provided a mechanism to create electronic cash (e-cash) that protects customer anonymity against a curious bank wishing to surveil their payment activity. This is analogous to the unlinkability between withdrawal and spending that customers enjoy with physical cash. Customers in Chaum's system use digital coins, each containing a unique serial number. A digital signature on this serial number from the bank assures third parties of the coin's validity. However, to prevent banks from being able to link the withdrawal of coins to their subsequent use, this identifier is "blinded" during the signing process, preventing the bank from initially learning its value. Later when the coin is spent, the bank will have no way of linking the unblinded serial number with the value it signed, but the unblinded coin will still possess a valid signature.

Anonymous credentials solve the problem of demonstrating that we meet some qualification to obtain goods and services, or to exercise certain privileges, but without revealing more information than is strictly required. The standard example of this is proving you are legally old enough to buy age-restricted products like alcohol. However, showing a government issued ID also reveals other information such as a person's name and address. Anonymous credential schemes solve this problem, allowing users to prove possession of only those credentials necessary to satisfy the verifier, without revealing any other information.

Why is this topic important? The number of our daily activities that involve networked, digital systems continues to grow, leading to the nightmare of ubiquitous surveillance by governments and private enterprises. These surveillance systems affect people's lives offline as well, impacting their ability to afford goods, access services, and enjoy basic human rights. Digital systems that ensure user privacy by design are therefore fundamental to alleviating existing surveillance harms and preventing their exacerbation. Building blocks like blind signatures and anonymous credentials serve exactly the purpose of making these solutions possible and are likely to remain fundamental pieces of ongoing privacy research.

Overview of the state of the art. Among blind signature schemes based on pre-quantum cryptography, Chaum's original RSA blind signatures and blind signatures based on elliptic curve cryptography are still used in real world systems, for example in GNU Taler [Dol19], a significant extension of Chaum's original e-cash. In the context of post-quantum cryptography, the majority of proposed blind signature schemes use lattices [BLNS23a, AGJ$^+$24, JS25], and they almost all follow the framework proposed by Fischlin [Fis06] for building a blind signature scheme from a standard digital signature scheme and an IND-CPA encryption scheme. Proposed schemes based on other post-quantum families like isogenies [KLLQ23, HLM$^+$25], error-correcting codes [LP25a] and multivariate quadratic systems [BFM$^+$25] have all recently emerged as well. The currently proposed post-quantum schemes are all much larger and much slower than their pre-quantum counterparts. RSA blind signatures are the same size as regular RSA signatures (256 – 512 bytes) and require a few tens or a hundred microseconds (less than 100,000 CPU cycles on a 5.2GHz CPU) on a laptop to compute. By comparison, current lattice-based blind signatures are on the order of tens of kilobytes and minimally require several seconds for signing and verification.

Current research on anonymous credentials is quite broad in scope, with recent work driven by both application-specific needs (e.g., threshold schemes) and also to address general challenges relating to online anonymity. For example, anonymity can be compromised if the revealed credentials themselves associate their bearer with a small anonymity set. A recent paper by Katz and Sefranek [KS25] explored enhancing privacy by hiding not just the unrevealed attributes of a credential but the credential issuer as well. Existing real-world implementations of anonymous credentials include the digital wallet app Yivi [1], which is an implementation of an RSA-based anonymous credential scheme developed by Camenisch and Lysyanskaya [CL01]. In the post-quantum setting, recent works have proposed anonymous credential schemes based on lattices [BLNS23b, BLNS23c, AGJ$^+$24, DKLW25] and arithmetization-friendly symmetric primitives [FR25a], following similar design principles as pre-quantum schemes, but their proof sizes and computational costs are still significantly larger than their pre-quantum counterparts.

Open problems. The main open problem for both blind signatures and anonymous credentials is improving the size and performance of schemes that resist attacks by quantum computers. As mentioned above, the computation time and signature size of post-quantum schemes is much larger than their pre-quantum counterparts, which means that a service which uses post-quantum blind signatures would incur significantly higher costs in terms of computation, data storage, and network traffic.

There are also open questions on the provable security side for blind signatures as well. Blind signature schemes usually have slightly different notions of unforgeability compared to their standard digital signature counterparts. Among post-quantum schemes based on Fischlin's construction, there also seems to be a trade-off between the performance quality and the complexity of the underlying security assumptions.

3.3.2 Fully homomorphic encryption

Fully Homomorphic Encryption (FHE) is a cryptographic technique allowing a server to perform computations directly over encrypted data, without requiring decryption. Data is encrypted by the user and sent to the server, along with an *evaluation key* that the server can use to run some computation *homomorphically*, without getting any information about

[1] https://web.archive.org/web/20251116124537/https://yivi.app/en/. Accessed: 2025-11-27.

the actual content of the data. The output of the homomorphic computation is an encrypted result that is sent back to the user, who can decrypt it using their secret key.

Why is this topic important? FHE potentially allows any client/server application to operate on encrypted data. Thus, the server has no access to any sensitive material, offering strong guarantees to the user against data breaches and malicious behavior from the server. An example of a use case for FHE would be privacy-preserving AI systems, where a user could call a model without revealing its input nor the result. Another example is Private Information Retrieval (PIR), in which the user can query a database without revealing the content of its query. FHE is more generally a building block for PETs with many applications in fields where sensitive data have to be manipulated, such as finance or healthcare. Finally, FHE begins to be used in the blockchain space to improve the privacy of transactions and smart contracts. FHE has seen impressive technological development in recent years, and a number of startups have emerged that demonstrate its scientific maturity and growing industrial adoption.

Overview of the state of the art. The concept of FHE was first formalized by Rivest, Adleman and Dertouzos [RAD78]. Early homomorphic schemes were only *partial*, that is to say only a limited class of programs could be evaluated homomorphically. In 2009, Craig Gentry [Gen09] published the first *fully* homomorphic encryption scheme. Since then, a lot of research has iterated on Gentry's original concept to improve the performance of FHE. All modern FHE schemes rely on lattice-based cryptography, where the encryption process introduces noise into the data, and this noise grows as homomorphic computations are performed. To avoid an overflow of noise in the data, Gentry introduced the notion of *bootstrapping*, which resets the noise level of a ciphertext by homomorphically applying decryption, enabling further computations. As of today, research in FHE has gathered around two main families of schemes that yield very different trade-offs in performance and homomorphic capabilities:

- **FHEW/TFHE**: These schemes [DM15, CGGI16, CGGI17, CGGI20] are known for their very efficient bootstrapping. They are particularly well-suited for applications requiring a relatively low latency. They operate on data chunks of small precision (typically less than 8 bits) and perform exact computation.
- **BFV/BGV/CKKS**: This family of schemes [Bra12, FV12, BGV12, CKKS17] relies on powerful packing capabilities, allowing a large amount of data to be processed in parallel and showcasing better amortized performance than the former. However, this comes at the cost of a more noticeable latency to retrieve the computation results. Among them, CKKS has the particularity of offering floating-point arithmetic for approximate computations on larger precisions.

The discrepancy in capabilities of these two families is reflected in the type of applications they target: it seems that TFHE is easier to compile with dedicated toolchains directly from "cleartext" programming, which makes it better suited for, e.g., blockchain applications. On the other hand, CKKS is preferred for processing large datasets (with a tolerable level of approximation) making it a better fit for machine learning and AI. Recent works have mostly focused on extending capabilities and improving the performance of schemes (in particular bootstrapping, which is by far the most costly operation). See for example [CHK$^+$18, CCS19, LLK$^+$22, AKP25] for CKKS and [CLOT21, BBB$^+$23, GBA21] for TFHE. Another important line of work is transciphering [NLV11, GHS12, CCF+16, BBB+25a]: a technique to improve the bandwidth overhead caused by ciphertext expansion in FHE. A more theoretical active area of research is to define precise security definitions for FHE [LM21, CSBB24, MN24].

Some community efforts to organize the research have emerged with the organizations `fhe.org` and `homomorphicencryption.org`. Some proposal of standard is currently being discussed at ISO while NIST has recently issued a call for proposals for Multi-Party Threshold Cryptography (MPTC) with a large scope that includes FHE [BP25].

Open problems. The most important perspective for FHE is improving performance: it is commonly accepted that the current overhead of homomorphic computations is around 4 orders of magnitude. Beyond algorithmic improvements, we have seen some work on hardware specifically tailored for FHE computations: such hardware targets, in particular, an acceleration of the Fast-Fourier Transform (FFT) or the Number-Theoretic Transform (NTT), which are essential building blocks of FHE (see, e.g., [BDTV23]). We can expect to see this line of work develop in the future. Another challenge for the adoption in practice of FHE is the automatic compilation of homomorphic programs to help developers integrate this technology, with some open-source tools currently under development [GSPH+21, Zam22]. Finally, another long-term perspective is to reconcile the two branches, TFHE and CKKS, in a common framework, to form a ”Theory of Everything” of FHE.

3.3.3 Threshold cryptography

Threshold cryptography is an advanced technique based on secret sharing in which a secret key is split into n components, called the shares. The scheme is parameterized by a threshold t: any set of at least t shares can reconstruct the secret, while any set of fewer than t shares reveals no information about it. These n shares are distributed among n distinct entities, typically called parties, with each party holding exactly one share.

Threshold cryptography is a type of MPC that enables cryptographic operations (e.g., decryption, signing) to be performed using a shared secret key without ever recombining the secret key. The computation is distributed across the parties, and no party learns the full secret at any point. This approach has many applications: for example, threshold decryption is useful in e-voting, while threshold signatures are used in blockchain systems.

Why is this topic important? Threshold cryptography is an essential tool to protect secret keys against device compromise. If a secret key is stored on a single device, it is immediately exposed once that device is compromised. One approach to mitigate this risk is to rely on secure hardware to prevent compromise (i.e., achieve compromise resistance), but relying on secure hardware is costly and might not always be possible. Threshold cryptography offers a flexible solution by distributing the secret across multiple devices while still allowing it to be used securely. An adversary must compromise several devices to recover the secret key, thereby significantly reducing the risk of full-key exposure.

Threshold cryptography is also valuable in scenarios that require distributed authority or collective governance. In applications such as e-voting or blockchain governance, it may be unacceptable for a single entity to hold a key that enables a sensitive or high-impact operation. A malicious or coerced party could otherwise misuse such a key to access confidential information or to perform unauthorized actions. Threshold cryptography mitigates this risk by distributing the key among multiple independent entities, ensuring that no single party can act alone. Instead, a predefined threshold of participants must cooperate to reconstruct or use the shared secret.

Threshold cryptography is currently a very active area of research and development, as it provides security guarantees that cannot be achieved otherwise. Several companies are working on deploying threshold solutions, and standardization efforts are ongoing [CKGW24, BP25].

Overview of the state of the art. Threshold cryptosystems have been studied since the late 1980s [DF90]. The first series of works focused on extending traditional cryptosystems –such as RSA, ElGamal, and DSA– to the threshold setting. Today, efficient pre-quantum solutions exist, including threshold ElGamal for encryption [CGS97] and FROST for signatures [KG20].

For post-quantum schemes, the state of the art is less mature, while the landscape of underlying assumption families is more diverse. Research on post-quantum threshold cryptography has mostly focused on lattice-based constructions. Some threshold variants of lattice-based encryption [LP25b] and signature schemes [DKM$^+$24] have been proposed, although they remain relatively complex. In contrast, hash-based and MPCitH-based schemes are significantly harder to adapt to the threshold setting, due to their heavy reliance on symmetric primitives and the structure of their underlying protocols. Moreover, impossibility results have been established for certain classes of such schemes [DKR24]. UOV-like multivariate schemes have been identified as promising candidates for thresholdization [CS19, CEN25], although no concrete schemes have been published yet.

Open problems. Many open problems remain in this research area, particularly concerning threshold post-quantum schemes. A central challenge is to design efficient post-quantum threshold protocols, where efficiency encompasses the number of rounds, communication bandwidth, ciphertext and signature sizes, and computational cost. Another important direction is the efficient thresholdization of emerging post-quantum standards, such as ML-KEM and ML-DSA. Additional research is also needed to develop practical post-quantum distributed key generation (DKG) protocols. Finally, substantial effort should be devoted to analyzing the security of threshold constructions in the presence of quantum adversaries, which remains largely unexplored.

3.3.4 Oblivious pseudorandom functions

Oblivious Pseudorandom Functions (OPRFs) enable a client to evaluate a pseudorandom function using a server's key without the client learning the key or the server learning the input or output.

Why is this topic important? OPRFs serve as fundamental building blocks for privacy-preserving protocols. Unlike blind signatures, OPRFs are *privately verifiable*: only the key holder can verify correctness. Whenever a protocol requires sending a hash, using an OPRF instead can provide stronger privacy guarantees. For example, rather than transmitting hashed passwords for authentication, protocols like OPAQUE [JKX18] use OPRFs to authenticate with a password without revealing the password to the server. OPRFs are particularly effective for private set intersection with unbalanced sets, where one party holds a significantly larger dataset than the other. Another application is rate-limiting and abuse prevention: the

PrivacyPass protocol [DIW24] uses OPRFs to mitigate DDoS attacks while preserving user anonymity. While some deployments use publicly verifiable variants for auditability, other deployments favor OPRFs' computational efficiency, as these operations are in the hot path and must be as fast as possible.

Overview of the state of the art. The dominant classical approach is the 2HashDH (and its verifiable variant 3HashDH-POPRF), which is *round-optimal*: each party speaks only once. The 2HashDH protocol involves three steps: the client blinds their input; the server evaluates it with their key; the client unblinds the result. This requires only a handful of elliptic curve operations and less than 100 bytes of communication.

Recent works have proposed post-quantum constructions of OPRF. Building 2HashDH OPRFs from lattices requires clients to prove their inputs are well-formed in zero-knowledge, which is computationally expensive. Despite optimizations, communication overhead remains above 100 kilobytes [AG24, ESTX24]. Power residue PRFs offer an alternative, mapping $x \bmod (2^{\lambda} \cdot g + 1)$ to $(k + x)^{g} \bmod p$. The most efficient power-residue OPRF called GoldOPRF [YBH+25], leverages recent advances in Vector Oblivious Linear Evaluation (VOLE) correlations for improved efficiency. Naor-Reingold PRFs provide a more generic approach requiring only an Abelian group action and oblivious transfer. The constructions are simpler with implicit hash-to-group operations and minimal computational overhead. However, existing constructions lack full malicious security and require large public keys. Round-optimal variants remain unattractive [HHM+24], while the efficient lattice-based construction [HKL+25] requires six communication rounds.

Open problems. Some post-quantum OPRFs now match or exceed classical computational performance. However, communication overhead remains the primary deployment barrier. Current constructions shift computation to preprocessing phases requiring hundreds of kilobytes of transmission, stemming from dependence on bandwidth-expensive oblivious transfer protocols. Improved oblivious transfer would directly benefit both lattice-based and power residue implementations. Additionally, current post-quantum constructions lack partial verifiability properties needed for certain security models.

Recent progress has been substantial, and concerns that blind signatures might supersede OPRFs have not materialized. Despite remaining preprocessing and bandwidth challenges, efficiency improvements have reaffirmed OPRFs' distinct value in the post-quantum ecosystem.

3.4 Real-world aspects and use cases

3.4.1 Post-quantum cryptography transition

According to [Ins24] a majority of experts expect a cryptographically relevant quantum computer within 10 to 15 years. Given the experience, that transition of cryptographic primitives takes a long period, the process should be started already now.

Why is this topic important? As [ENI22] states, adversaries can already capture encrypted traffic today and decrypt it in the future once quantum capabilities exist ("harvest now, decrypt later", HNDL), which is especially critical for data with long confidentiality lifetimes (health, IP, state, financial data). For "essential" and "important" entities under NIS-2 ([Dat]), cryptography and encryption are core risk-management measures; failing to adapt as the threat landscape changes can lead to non-compliance, regulatory scrutiny, and fines. The HNDL attack poses such a threat that needs to be considered by those entities already. [ENI22] also states that starting such a transition early reduces long-term cyber risk, avoids rushed, costly migrations later. So to foster migration and create incentives for the industry, the EU, via the NIS Cooperation Group, has already set expectations and timelines ([Com25]) for moving to quantum-resistant cryptography via a coordinated roadmap, especially for critical and regulated sectors. The EU roadmap describes PQC migration as a multi-year effort involving asset inventories, supply-chain coordination, protocol changes, and testing, which cannot be done safely at the last minute. [PQS25]

Overview of the state of the art. PQC guidance falls into two main categories: migration guides, which detail specific steps for implementation, and roadmaps, which emphasize timelines and phased strategies.

Migration guidelines. Key migration guides handbooks and guidelines include:

- The PQC Migration Handbook 2nd edition [ADD^{+}23] – practical, step-by-step migration guide.
- ENISA "Post-Quantum Cryptography: Current state and quantum mitigation" [BDH^{+}21] and the ENISA "Post-Quantum Cryptography – Integration Study" [BHLR22] offering EU-level advice on risk, mitigation options, and integration aspects.
- "Preparing for the quantum era" from Cyber Security Coalition [Bel25] provides a practical guide emphasizing the urgent strategic need for organizations to assess quantum risks, plan, and implement post-quantum cryptography migration through phased steps to protect data, ensure compliance, and maintain security amid the evolving quantum threat landscape.
- NIST NCCoE "Migration to Post-Quantum Cryptography" [NCC, NCC23]: Detailed U.S. technical playbooks that are also useful for EU organizations.

Roadmaps. Although the roadmaps of the US and UK are not directly applicable to EU organizations, they are nevertheless influential due to global interoperability needs in interconnected digital ecosystems. Key roadmaps include:

- CNSA 2.0 Framework: The U.S. National Security Agency (NSA) updated its Commercial National Security Algorithm Suite (CNSA) [(NS22] to version 2.0, which includes a phased roadmap for migrating National Security Systems to quantum-resistant algorithms by 2033, with incremental milestones for hybrid modes and full PQC algorithm deployment.
- NIST PQC Transition Planning: NIST published the draft [Nat24] that proposes disallowance of quantum-vulnerable algorithms from 2035 on.
- United Kingdom: NCSC guidance [UK 25] announcing a phased PQC migration timeline for UK organizations, outlining a multiphase roadmap towards quantum-resistant encryption by the 2030s.

PQC transition in the EU. For EU member states no such definite timelines exist. The last two years (2024-2025) have yet seen some key developments in setting a more articulated direction for the PQC transition in the EU. Most notably, following the 2024 publication of the European Commission Recommendation on the creation of a coordinated PQC transition roadmap within two years [EC24], a dedicated Workstream within the NIS Cooperation Group presented in June 2025 a first high-level iteration of such a roadmap setting transition timelines for various use-cases and indicating a set of concrete governance steps to be taken by the Member States in enacting this migration [CG25]. It acts as a proposal for member state roadmaps and indicates transition of high risk use cases until 2030 and medium risk use cases until 2035.

Besides, in 2024, a joint statement by a host of national cybersecurity authorities emphasized that organizations must make the PQC transition a top priority [BSI25]. Alongside, the EU started allocating funding not only to the development of PQC solutions, but also to various aspects of the implementation of the transition process [ECC23, ECC25]. In addition, a legal framework is in place consisting of a number of legal acts in the digital and cybersecurity realm that contain state-of-the-art security requirements. Various guidelines that have been made available by competent bodies indicate that deployment of PQC is now considered to be best practice [Tel19, Tel25, ENI24a].

However, these efforts do not seem to have been sufficient so far, as surveys reveal not only low current rates of initiation of quantum-readiness processes within industry, but also significant lack of intention to invest in quantum-safe measures even in critical sectors [ENI24b, BSI24]. For some people, this advocates for clearer and more explicit regulatory requirements to prompt the necessary scale of adoption of this technology. This would notably require to address the existing divergence among national cybersecurity authorities of the endorsed PQC schemes.

Other perspectives caution against relying on regulatory mandates as primary drivers of adoption, arguing that such requirements may prove ineffective or premature, and instead advocate prioritizing targeted mitigations (e.g. HNDL-focused measures) while allowing time for more mature PQC solutions to emerge.

Open problems. Although first steps and efforts have been done for transitioning Europe infrastructure to PQC, there are several open issues. The lack of binding deadlines and concrete regulatory mandates may lead to uncertainty and a “wait and see” stance among many organizations awaiting clearer compliance requirements and sector-specific guidance ([Eve25]). A second issue is the lack of completed protocol standards. Although PQC algorithm standards are published e.g. by NIST, their integration into protocol standards is still ongoing. One example is Hybrid Key Exchange for TLS [SFG25], that is already used by some peers on the internet but still in draft status. A third issue is the limited availability of certified, widely supported PQC solutions and incomplete certification schemes, which slow deployment and increase operational risk during migration ([Ins25]). As a fourth issue, monitoring, audit, and compliance tools lag behind, making it hard to verify and enforce secure PQC usage throughout complex IT and network environments ([Eve25]). Finally, the transition is hardened by organizational barriers including lack of skilled personnel, complexity of cryptographic inventories, long migration times, and funding/resource challenges for coordinated multi-year projects ([VSL24]).

3.4.2 Hybrid cryptographic schemes

The first proposals for hybrid schemes with the explicit intention to “hedging our bets” when the security of newer primitives is not yet certain [BHMS17] occurred in 2017. The concept has since evolved and also applied to digital signatures.

Why is this topic important? Hybrid cryptographic schemes combining traditional (e.g., ECC, RSA) and PQC algorithms (e.g., ML-KEM, ML-DSA) are vital during migration, as they ensure security if either component fails. As also stated in [Mar25], PQC schemes lack full trust due to their relative mathematical immaturity –recently standardized after NIST competitions– and unproven long-term resilience against novel attacks, unlike decades-proven traditional algorithms. Also, implementation risks, like side-channel vulnerabilities in new PQC libraries, further necessitate hybrids for defense-in-depth. Also, EU agencies, including ENISA, mandate hybrid approaches in guidance to integrate PQC safely into existing protocols without disruption, see e.g, [NIS25].

Overview of the state of the art. There are already several standards and advanced drafts that allow using hybrid post-quantum/traditional (PQ/T) cryptography, e.g. by combining traditional (e.g., ECC/RSA) and post-quantum algorithms (e.g., ML-KEM/ML-DSA). Papers like [BH23] and [DPH25] try to categorize different approaches to hybridization.

Key hybrid schemes include:

- Quantum-safe Hybrid Key Exchanges: [ETS25] specifies several methods for deriving cryptographic keys from multiple shared secrets that are established by traditional and PQC algorithms.
- Multiple Key Exchanges for IKEv2 [TTB$^+$23], enhancing the IKE protocol to use several key exchange algorithms to derive a channel key.
- TLS HybridKEM [SFG25], integrating traditional and PQ KEMs in TLS handshakes per protocol extensions.
- Chimera certificates (X.509 §9.8 ”Catalyst” [Key25]), embedding PQ keys/signatures in traditional certificates for backward compatibility.
- CMS multi-signatures [TS10], enabling co-signing with PQ and traditional algorithms for robust message authentication.
- HPKE, with PQ-hybrid KEMs for flexible message encryption [BC25].
- PKIX Composites, defining hybrid KEM and DSA elements in PKIs [OGP$^+$25b, OGP$^+$25a].
- JOSE composite signatures [PSGR25], hybrid signatures combining ML-DSA with ECDSA or EdDSA.
- Intelligent composed algorithms [BWN21] are advanced cryptographic constructs that combine multiple component algorithms - signatures or KEMs - to provide flexible, robust security by leveraging complementary strengths and mitigating individual weaknesses in a unified framework.

Open problems. Although there is a strong push by agencies and industry to use PQ/T hybrids, the combination of different algorithms that often have different security properties needs to be better understood. For example does the X-Wing Hybrid KEM [BCD⁺24] offer such proofs for X448/X25519 with ML-KEM combinations. Such proofs for other KEM combinations in [OGP⁺25b] are still work in progress and more complicated. Moreover, there are disputes over the usefulness of schemes like Chimera certificates [Key25] that were not adopted by IETF for security concerns (see [TGF⁺23]). Another issue is that the number of PQC algorithms and variants, when combined with multiple traditional algorithms, results in combinatorial complexity that creates interoperability challenges. Finally, there is still a wide variety of ideas and approaches to hybridization, which makes it difficult for vendors to decide which one is worth supporting.

3.4.3 Digital identity

Digital identity systems enable individuals and organizations to prove who they are online, serving as the backbone of secure access to public and private services. There is a clear trend toward moving away from passwords and instead adopting device-bound, cryptographically backed credentials, mainly relying on signature-based authentication. Many European electronic identities (eIDs) already use digital signatures due to eIDAS compliance, and similar ideas have become widespread in consumer technologies, for example through Passkeys and standards like FIDO2/WebAuthn. This shift marks a welcome improvement in security since it mitigates phishing, credential theft, and the systemic weaknesses of password-based authentication. However, from a privacy perspective, this trend is not automatically beneficial: many current schemes introduce stable identifiers, central points of trust, or metadata patterns that make users more traceable across services unless privacy-preserving mechanisms are deliberately designed in. Deploying systems that reconcile strong authentication with unlinkability and privacy-preserving identity management therefore remains an open challenge.

Why is this topic important? In the European Union, digital identity initiatives such as eIDAS 2.0 aim to establish a unified and privacy-preserving framework that empowers citizens to use their credentials seamlessly across borders. Central to this effort is the European Digital Identity (EUDI) framework and the EUDI Wallet, which provide a standardized and interoperable mechanism for citizens to securely store and present verified attributes, such as IDs, diplomas, or financial information, under their own control. Because the EU's digital identity ecosystem depends heavily on cryptography, in particular on digital signatures, the emergence of quantum computers poses a serious long-term risk. Research into post-quantum digital identity therefore focuses on ensuring that the cryptographic foundations required to realize a privacy-preserving EUDI Wallet and related infrastructures remain secure against future quantum adversaries.

Overview of the state of the art. Privacy-preserving identity management can cryptographically be realized by so-called anonymous credentials. They combine advanced primitives such as zero-knowledge proofs and sophisticated signature schemes and were first envisioned by Chaum [Cha86], later realized by Camenisch and Lysyanskaya [CL01] as well as Brands [Bra00] in the early 2000s, and have since become well studied and well understood by the research community. Unfortunately, while we now see the first NIST standards for public-key encryption and signatures, we are still far from having a clear picture of candidates for post-quantum anonymous credentials, let alone a path to their standardization. However, it is strongly advisable to consider post-quantum aspects in any current design, for example in the ongoing discussions about the EUDI Wallet, so that future reliance on post-quantum anonymous credentials will not require a partial or complete redesign. In other words, cryptographic agility is essential.

There are some recent constructions of lattice-based anonymous credentials [BLNS23c, AGJ^{+}24, DKLW25], and first proof-of-concept implementations are available from IBM [LSS24] and from the EU QUBIP project.[2] There is also an increasing body of work on advanced signatures (such as blind signatures), general-purpose non-interactive zero-knowledge (NIZK) proof systems (e.g., zk-SNARKs), and "zero-knowledge-friendly" signatures and related cryptographic primitives.

Open problems. While we now have the first constructions of lattice-based anonymous credentials, they do not yet appear to be sufficiently well studied in terms of security and efficiency. Moreover, it is important to have constructions from alternative assumptions, a diversity argument that is essential to withstand unexpected cryptanalytic breakthroughs. Building full-fledged anonymous credentials from alternative classes of post-quantum assumptions, however, seems challenging, as these assumptions typically lack the rich algebraic structure available in lattices. Nevertheless, feature-reduced anonymous credentials may already suffice for many applications and seem within reach. Alternatively, a generic way to construct anonymous credentials is to combine any secure signature scheme, such as the standardized ML-DSA, with a NIZK proof system. Given the enormous progress in zk-SNARKs in the past decade, this makes the construction of practical anonymous credential schemes relying on existing (post-quantum) signature schemes feasible. This has recently been demonstrated for pre-quantum anonymous credentials built using ECDSA or RSA signatures by Google [Fs24] and Microsoft [PPZ24]. We hope that significant research will continue in the coming years to advance these directions and ultimately make a privacy-preserving post-quantum digital identity a reality.

3.4.4 Electronic voting

Secure electronic voting (e-voting) aims at using cryptographic mechanisms to provide voters with verifiability of the election outcome while preserving ballot secrecy in order to have trustworthy election results capturing the the true will of the voters.

Why is this topic important? Elections form the very basis of our democracies, but have increasingly been under threat from parties contesting election results or trying to influence the elections. This calls for verifiable and secret elections.

Most constructions in e-voting rely on a public append-only bulletin board storing the encrypted votes. This, firstly, allows voters to check that their encrypted vote is stored correctly and, secondly, allows the authority to prove that the election outcome was correctly computed from the encrypted votes. However, this also means that e-voting systems are especially prone to store-now-decrypt-later attacks, making the development of post-quantum schemes urgent.

[2] https://github.com/Cybersecurity-LINKS/pqzk-blns

Overview of the state of the art. Over the last ten years, we have seen strong progress on post-quantum e-voting (PQ e-voting) both in terms of systems and PQC building blocks. As an example post-quantum verifiable mixnets have been developed, see e.g. [HSS24, ABGS23], together with efficient decryption techniques [GHM$^+$22] which can be used to anonymize the ballots and decrypt them verifiably to obtain the election result. Also, homomorphic properties of post-quantum encryption have been used to obtain election results by summing under encryption [BHM21]. Other schemes have used less standard constructions and some have already been broken.

Open problems. A critical gap in secure PQ e-voting is the lack of formal security definitions for e-voting in the presence of quantum attackers. This is not surprising since e-voting security definitions are still an active research area even without quantum-capable attackers. Overall, improving the efficiency of PQ e-voting schemes is an open challenge, especially when capturing complex social choice functions and many voters considering that voting clients need to be lightweight and the resulting proofs of correct tally should be verifiable by everybody. Another important open problem is designing PQ e-voting systems that are receipt-free and coercion-resistant: only a preliminary attempt was made [HPR20]. For this purpose, efficient rerandomisable signatures over ciphertexts would be a useful primitive to develop. Finally, hybrid schemes that combine the security of pre- and post-quantum cryptographic primitives for breakdown resilience are still largely unsolved. A recent result provides a composed construction [Gol25], but it lacks efficiency in generality.

Chapter 4

Conclusion

This report has provided an overview of the current hot topics and open problems in PQC. Through a community survey and internal discussions within the PQCSA consortium, we have identified key research areas that are critical for advancing the field.

While lattice-based cryptography is predominant and currently offers some of the best trade-offs for KEMs and signatures, along with promising support for advanced functionalities, the diversity of cryptographic families remains crucial to ensure robust fallback options, should underlying assumptions be compromised. Isogeny-based cryptography and MPC-in-the-Head are two families that have seen significant recent progress and are likely to play important roles in the post-quantum ecosystem.

A major area of focus for assessing the security of post-quantum schemes is cryptanalysis, including quantum cryptanalysis and cryptanalysis with extra information. The study of side-channel analysis and protected implementations is equally essential to ensure the robustness of post-quantum schemes deployed in real-world devices. Both our survey results and internal discussions within the PQCSA consortium indicate a broad consensus that these topics require sustained and increased attention to build confidence and trust in the post-quantum schemes that will ultimately be deployed in practice.

Continued research on basic post-quantum primitives such as KEMs and signatures remains necessary to improve their efficiency, particularly with respect to key and ciphertext/signature sizes. Deploying the first NIST PQC standards poses significant challenges for constrained devices and low-bandwidth environments. At the same time, many advanced primitives and protocols developed in the traditional setting to provide privacy in a wide range of applications are not yet fully adapted to the post-quantum context. Advancing these constructions is essential to ensuring that PQC can meet the needs of modern systems.

Finally, the challenges associated with the transition to post-quantum cryptography, including the need for hybrid schemes, are of paramount importance. This topic extends beyond pure cryptographic research, encompassing issues of governance, interoperability, and legacy systems. Recent EU and international initiatives highlight that PQC migration is a multi-year, system-wide effort requiring early preparation, coordinated roadmaps, and clear regulatory expectations. Yet binding deadlines, mature protocol standards, and widely supported certified implementations are still lacking. Hybrid cryptographic mechanisms, increasingly present in standards and draft specifications, will be essential during this period to ensure continuity and defense-in-depth, even though their security properties and practical applicability remain active areas of investigation. Addressing these transition challenges will require sustained collaboration among researchers, standardization bodies, policymakers, and industry to enable the safe and scalable deployment of PQC across real-world infrastructures.

Acknowledgements

While the report was primarily authored by the PQCSA consortium members listed on the title page, we benefited from contributions and feedback from various external experts and community members. We would particularly like to thank Lena Heimberger and Christian Rechberger for their contribution to the OPRF topic, Daniel Slamanig for his contribution to the digital identity topic, Peter Roenne for his contribution to the e-voting topic, and Laima Jančiūtė for her contribution on the PQC transition in the EU.

We further extend our acknowledgements to all respondents to our community survey for their valuable input, which greatly informed the selection of topics and the perspectives presented in this report, namely (in alphabetical order): Martin Albrecht, Diego F. Aranha, Jean-Philippe Aumasson, Marco Baldi, Gustavo Banegas, Manuel Barbosa, Paulo L. Barreto, Carsten Baum, Thomas Bellebaum, Diana Gratiela Berbecaru, Loïc Bidoux, Joppe W. Bos, Charles Bouillaguet, Lennart Braun, Chitchanok Chuengsatiansup, Christine Cloostermans, Giuseppe D’Alconzo, Jintai Ding, David Domingo, Pierre-Alain Fouque, Andreas Hülsing, Simon Josefsson, François Koeune, Stefan Kölbl, Akis Kourtis, Mukul Kulkarni, Christian Majenz, John Preuß Mattsson, René Mayrhofer, Diego Napp, Lorenz Panny, Chris Peikert, Federico Pintore, Thomas Pornin, Axel Poschmann, Peter Roenne, Paolo Santini, Sven Schäge, Peter Schwabe, Leonel Sousa, Christoph Striecks, Patrick Struck, Damien Vergnaud, Pascal Veron, Violetta Weger, as well as all the respondents who preferred to remain anonymous.

Bibliography

[ABB$^+$24] Carlos Aguilar Melchor, Slim Bettaieb, Loïc Bidoux, Thibauld Feneuil, Philippe Gaborit, Nicolas Gama, Shay Gueron, James Howe, Andreas Hülsing, David Joseph, Antoine Joux, Mukul Kulkarni, Edoardo Persichetti, Tovohery H. Randrianarisoa, Matthieu Rivain, and Dongze Yue. SDitH — Syndrome Decoding in the Head. Technical report, National Institute of Standards and Technology, 2024. available at https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures.

[ABGS23] Diego F. Aranha, Carsten Baum, Kristian Gjøsteen, and Tjerand Silde. Verifiable mix-nets and distributed decryption for voting from lattice-based assumptions. In Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda, editors, *ACM CCS 2023: 30th Conference on Computer and Communications Security*, pages 1467–1481, Copenhagen, Denmark, November 26–30, 2023. ACM Press.

[ACK$^+$23] Thomas Aulbach, Fabio Campos, Juliane Krämer, Simona Samardjiska, and Marc Stöttinger. Separating oil and vinegar with a single trace side-channel assisted kipnis-shamir attack on UOV. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2023(3):221–245, 2023.

[ADD$^+$23] Thomas Attema, João Diogo Duarte, Vincent Dunning, Matthieu Lequesne, Ward van der Schoot, Marc Stevens, and AIVD Cryptologists & Security Advisors. The pqc migration handbook: Guidelines for migrating to post-quantum cryptography. Technical report, TNO, CWI, Netherlands National Communications Security Agency, December 2023. https://ir.cwi.nl/pub/32988/PQC_migration_handbook_EN_2.0.pdf.

[AG24] Martin R Albrecht and Kamil Doruk Gur. Verifiable oblivious pseudorandom functions from lattices: Practical-ish and thresholdisable. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 205–237. Springer, 2024.

[AGJ$^+$24] Sven Argo, Tim Güneysu, Corentin Jeudy, Georg Land, Adeline Roux-Langlois, and Olivier Sanders. Practical post-quantum signatures for privacy. In Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie, editors, *ACM CCS 2024: 31st Conference on Computer and Communications Security*, pages 1523–1537, Salt Lake City, UT, USA, October 14–18, 2024. ACM Press.

[AHIV17] Scott Ames, Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam. Ligero: Lightweight sublinear arguments without a trusted setup. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 2017: 24th Conference on Computer and Communications Security*, pages 2087–2104, Dallas, TX, USA, October 31 – November 2, 2017. ACM Press.

[AHIV23] Scott Ames, Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam. Ligero: lightweight sublinear arguments without a trusted setup. *Designs, Codes and Cryptography*, 91(11):3379–3424, 2023.

[AHJ+23] Carlos Aguilar Melchor, Andreas Hülsing, David Joseph, Christian Majenz, Eyal Ronen, and Dongze Yue. SDitH in the QROM. In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology – ASIACRYPT 2023, Part VII*, volume 14444 of *Lecture Notes in Computer Science*, pages 317–350, Guangzhou, China, December 4–8, 2023. Springer, Singapore, Singapore.

[Ajt96] Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *28th Annual ACM Symposium on Theory of Computing*, pages 99–108, Philadephia, PA, USA, May 22–24, 1996. ACM Press.

[AKP25] Andreea Alexandru, Andrey Kim, and Yuriy Polyakov. General functional bootstrapping using CKKS. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology – CRYPTO 2025, Part III*, volume 16002 of *Lecture Notes in Computer Science*, pages 304–337, Santa Barbara, CA, USA, August 17–21, 2025. Springer, Cham, Switzerland.

[BBB+23] Loris Bergerat, Anas Boudi, Quentin Bourgerie, Ilaria Chillotti, Damien Ligier, Jean-Baptiste Orfila, and Samuel Tap. Parameter optimization and larger precision for (T)FHE. *Journal of Cryptology*, 36(3):28, July 2023.

[BBB+24] Carsten Baum, Lennart Braun, Ward Beullens, Cyprien Delpech de Saint Guilhem, Michael Klooß, Christian Majenz, Shibam Mukherjee, Emmanuela Orsini, Sebastian Ramacher, Christian Rechberger, Lawrence Roy, and Peter Scholl. FAEST. Technical report, National Institute of Standards and Technology, 2024. available at https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures.

[BBB+25a] Jules Baudrin, Sonia Belaïd, Nicolas Bon, Christina Boura, Anne Canteaut, Gaëtan Leurent, Pascal Paillier, Léo Perrin, Matthieu Rivain, Yann Rotella, and Samuel Tap. Transistor: a TFHE-friendly stream cipher. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology – CRYPTO 2025, Part V*, volume 16004 of *Lecture Notes in Computer Science*, pages 530–565, Santa Barbara, CA, USA, August 17–21, 2025. Springer, Cham, Switzerland.

[BBB+25b] Carsten Baum, Ward Beullens, Lennart Braun, Cyprien Delpech de Saint Guilhem, Michael Klooß, Christian Majenz, Shibam Mukherjee, Emmanuela Orsini, Sebastian Ramacher, Christian Rechberger, Lawrence Roy, and Peter Scholl. Shorter, tighter, FAESTer: Optimizations and improved (QROM) analysis for VOLE-in-the-head signatures. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology – CRYPTO 2025, Part VI*, volume 16005 of *Lecture*

Notes in Computer Science, pages 124–156, Santa Barbara, CA, USA, August 17–21, 2025. Springer, Cham, Switzerland.

[BBC+25] Andrea Basso, Giacomo Borin, Wouter Castryck, Maria Corte-Real Santos, Riccardo Invernizzi, Antonin Leroux, Luciano Maino, Frederik Vercauteren, and Benjamin Wesolowski. PRISM: Simple and compact identification and signatures from large prime degree isogenies. In Tibor Jager and Jiaxin Pan, editors, *PKC 2025: 28th International Conference on Theory and Practice of Public Key Cryptography, Part III*, volume 15676 of *Lecture Notes in Computer Science*, pages 300–332, Røros, Norway, May 12–15, 2025. Springer, Cham, Switzerland.

[BBD+23] Carsten Baum, Lennart Braun, Cyprien Delpech de Saint Guilhem, Michael Klooß, Emmanuela Orsini, Lawrence Roy, and Peter Scholl. Publicly verifiable zero-knowledge and post-quantum signatures from VOLE-in-the-head. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology – CRYPTO 2023, Part V*, volume 14085 of *Lecture Notes in Computer Science*, pages 581–615, Santa Barbara, CA, USA, August 20–24, 2023. Springer, Cham, Switzerland.

[BBE+18] Gilles Barthe, Sonia Belaïd, Thomas Espitau, Pierre-Alain Fouque, Benjamin Grégoire, Mélissa Rossi, and Mehdi Tibouchi. Masking the GLP lattice-based signature scheme at any order. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 354–384, Tel Aviv, Israel, April 29 – May 3, 2018. Springer, Cham, Switzerland.

[BBFR24] Ryad Benadjila, Charles Bouillaguet, Thibauld Feneuil, and Matthieu Rivain. MQOM — MQ on my Mind. Technical report, National Institute of Standards and Technology, 2024. available at https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures.

[BBM17] Daniel J. Bernstein, Jean-François Biasse, and Michele Mosca. A low-resource quantum factoring algorithm. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017*, pages 330–346, Utrecht, The Netherlands, June 26–28, 2017. Springer, Cham, Switzerland.

[BC25] Richard Barnes and Deirdre Connolly. Post-Quantum and Post-Quantum/Traditional Hybrid Algorithms for HPKE. Internet-Draft draft-ietf-hpke-pq-03, Internet Engineering Task Force, November 2025. https://datatracker.ietf.org/doc/draft-ietf-hpke-pq/03/.

[BCD+24] Manuel Barbosa, Deirdre Connolly, João Diogo Duarte, Aaron Kaiser, Peter Schwabe, Karoline Varner, and Bas Westerbaan. X-Wing: The hybrid KEM you've been looking for. Cryptology ePrint Archive, Report 2024/039, 2024.

[BDD+24] Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. SQIsign2D-West - the fast, the small, and the safer. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology – ASIACRYPT 2024, Part III*, volume 15486 of *Lecture*

Notes in Computer Science, pages 339–370, Kolkata, India, December 9–13, 2024. Springer, Singapore, Singapore.

[BDH⁺21] Ward Beullens, Jan-Pieter D'Anvers, Andreas Hülsing, Tanja Lange, Lorenz Panny, Cyprien de Saint Guilhem, Nigel P. Smart, Evangelos Rekleitis, Angeliki Aktypi, and Athanasios-Vasileios Grammatopoulos. Post-quantum cryptography: Current state and quantum mitigation. Technical report, ENISA, May 2021. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation.

[BDTV23] Michiel Van Beirendonck, Jan-Pieter D'Anvers, Furkan Turan, and Ingrid Verbauwhede. FPT: A fixed-point accelerator for torus fully homomorphic encryption. In Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda, editors, *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS 2023, Copenhagen, Denmark, November 26-30, 2023*, pages 741–755. ACM, 2023.

[Bel25] Cybersecurity Coalition Belgium. Preparing for the quantum era – a practical guide to post-quantum cryptography, 2025. https://cybersecuritycoalition.be/wp-content/uploads/CSC-WP-Post-Quantum-Crypto_300925_FINAL.pdf.

[BFM⁺19] Joppe W. Bos, Simon Friedberger, Marco Martinoli, Elisabeth Oswald, and Martijn Stam. Assessing the feasibility of single trace power analysis of Frodo. In Carlos Cid and Michael J.: Jacobson, Jr., editors, *SAC 2018: 25th Annual International Workshop on Selected Areas in Cryptography*, volume 11349 of *Lecture Notes in Computer Science*, pages 216–234, Calgary, AB, Canada, August 15–17, 2019. Springer, Cham, Switzerland.

[BFM⁺25] Charles Bouillaguet, Thibauld Feneuil, Jules Maire, Matthieu Rivain, Julia Sauvage, and Damien Vergnaud. Blinding post-quantum hash-and-sign signatures. Cryptology ePrint Archive, Report 2025/895, 2025.

[BGR⁺21] Joppe W. Bos, Marc Gourjon, Joost Renes, Tobias Schneider, and Christine van Vredendaal. Masking Kyber: First- and higher-order implementations. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(4):173–214, 2021.

[BGV12] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In Shafi Goldwasser, editor, *ITCS 2012: 3rd Innovations in Theoretical Computer Science*, pages 309–325, Cambridge, MA, USA, January 8–10, 2012. Association for Computing Machinery.

[BH23] Nina Bindel and Britta Hale. A note on hybrid signature schemes. Cryptology ePrint Archive, Report 2023/423, 2023.

[BHLR22] Daniel J. Bernstein, Andreas Hülsing, Tanja Lange, and Evangelos Rekleitis. Post-quantum cryptography integration study. Technical report, ENISA, 2022. https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study.

[BHM21] Xavier Boyen, Thomas Haines, and Johannes Müller. Epoque: Practical end-to-end verifiable post-quantum-secure E-voting. In *2021 IEEE European Symposium on Security and Privacy*, pages 272–291, Vienna, Austria, September 6–10, 2021. IEEE Computer Society Press.

[BHMS17] Nina Bindel, Udyani Herath, Matthew McKague, and Douglas Stebila. Transitioning to a quantum-resistant public key infrastructure. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017*, pages 384–405, Utrecht, The Netherlands, June 26–28, 2017. Springer, Cham, Switzerland.

[BLMP19] Daniel J. Bernstein, Tanja Lange, Chloe Martindale, and Lorenz Panny. Quantum circuits for the CSIDH: Optimizing quantum evaluation of isogenies. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019, Part II*, volume 11477 of *Lecture Notes in Computer Science*, pages 409–441, Darmstadt, Germany, May 19–23, 2019. Springer, Cham, Switzerland.

[BLNS23a] Ward Beullens, Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Gregor Seiler. Lattice-based blind signatures: Short, efficient, and round-optimal. In Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda, editors, *ACM CCS 2023: 30th Conference on Computer and Communications Security*, pages 16–29, Copenhagen, Denmark, November 26–30, 2023. ACM Press.

[BLNS23b] Jonathan Bootle, Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Alessandro Sorniotti. A framework for practical anonymous credentials from lattices. Cryptology ePrint Archive, Report 2023/560, 2023.

[BLNS23c] Jonathan Bootle, Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Alessandro Sorniotti. A framework for practical anonymous credentials from lattices. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology – CRYPTO 2023, Part II*, volume 14082 of *Lecture Notes in Computer Science*, pages 384–417, Santa Barbara, CA, USA, August 20–24, 2023. Springer, Cham, Switzerland.

[BN20] Carsten Baum and Ariel Nof. Concretely-efficient zero-knowledge arguments for arithmetic circuits and their application to lattice-based cryptography. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020: 23rd International Conference on Theory and Practice of Public Key Cryptography, Part I*, volume 12110 of *Lecture Notes in Computer Science*, pages 495–526, Edinburgh, UK, May 4–7, 2020. Springer, Cham, Switzerland.

[BP25] Luís T. A. N. Brandão and René Peralta. NIST First Call for Multi-Party Threshold Schemes - Second Public Draft. NIST Internal Report, NISTIR 8214C 2pd, 2025.

[Bra00] Stefan A. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy.* MIT Press, Cambridge, MA, USA, 2000.

[Bra12] Zvika Brakerski. Fully homomorphic encryption without modulus switching from classical GapSVP. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances* *in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 868–886, Santa Barbara, CA, USA, August 19–23, 2012. Springer Berlin Heidelberg, Germany.

[BS20] Xavier Bonnetain and André Schrottenloher. Quantum security analysis of CSIDH. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 493–522, Zagreb, Croatia, May 10–14, 2020. Springer, Cham, Switzerland.

[BSI24] BSI. Market Survey: Cryptography and Quantum Computing. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Marktumfrage_EN_Kryptografie_Quantencomputing.pdf, 2024.

[BSI25] BSI and Partner Agencies. Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography. A joint statement from partners from 21 European states. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement-2025.pdf, 2025.

[BWN21] Frank Byszio, Dr. Klaus-Dieter Wirth, and Dr. Kim Nguyen. Intelligent composed algorithms. Cryptology ePrint Archive, Report 2021/813, 2021.

[CCF$^+$16] Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, and Renaud Sirdey. Stream ciphers: A practical solution for efficient homomorphic-ciphertext compression. In Thomas Peyrin, editor, *Fast Software Encryption – FSE 2016*, volume 9783 of *Lecture Notes in Computer Science*, pages 313–333, Bochum, Germany, March 20–23, 2016. Springer Berlin Heidelberg, Germany.

[CCS19] Hao Chen, Ilaria Chillotti, and Yongsoo Song. Improved bootstrapping for approximate homomorphic encryption. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019, Part II*, volume 11477 of *Lecture Notes in Computer Science*, pages 34–54, Darmstadt, Germany, May 19–23, 2019. Springer, Cham, Switzerland.

[CD23] 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.

[CE87] David Chaum and Jan-Hendrik Evertse. A secure and privacy-protecting protocol for transmitting personal information between organizations. In Andrew M. Odlyzko, editor, *Advances in Cryptology – CRYPTO'86*, volume 263 of *Lecture Notes in Computer Science*, pages 118–167, Santa Barbara, CA, USA, August 1987. Springer Berlin Heidelberg, Germany.

[CEN25] Sofía Celi, Daniel Escudero, and Guilhem Niot. Share the MAYO: Thresholdizing MAYO. In Ruben Niederhagen and Markku-Juhani O. Saarinen, editors, *Post-Quantum Cryptography - 16th International Workshop, PQCrypto 2025, Part I*, pages 165–198, Taipei, Taiwan, April 08–10, 2025. Springer, Cham, Switzerland.

[CG25] European Commission and NIS Cooperation Group. A coordinated implementation roadmap for the transition to post-quantum cryptography. Technical report, European Union, June 2025. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology – ASIACRYPT 2016, Part I*, volume 10031 of *Lecture Notes in Computer Science*, pages 3–33, Hanoi, Vietnam, December 4–8, 2016. Springer Berlin Heidelberg, Germany.

[CGGI17] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. Faster packed homomorphic operations and efficient circuit bootstrapping for TFHE. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 377–408, Hong Kong, China, December 3–7, 2017. Springer, Cham, Switzerland.

[CGGI20] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. TFHE: Fast fully homomorphic encryption over the torus. *Journal of Cryptology*, 33(1):34–91, January 2020.

[CGS97] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A secure and optimally efficient multi-authority election scheme. In Walter Fumy, editor, *Advances in Cryptology – EUROCRYPT'97*, volume 1233 of *Lecture Notes in Computer Science*, pages 103–118, Konstanz, Germany, May 11–15, 1997. Springer Berlin Heidelberg, Germany.

[CGS14] Peter Campbell, Michael Groves, and Dan Shepherd. Soliloquy: A cautionary tale, 2014. https://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf.

[Cha82] David Chaum. Blind signatures for untraceable payments. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology – CRYPTO'82*, pages 199–203, Santa Barbara, CA, USA, 1982. Plenum Press, New York, USA.

[Cha85] David Chaum. Security without identification: transaction systems to make big brother obsolete. *Commun. ACM*, 28(10):1030–1044, October 1985.

[Cha86] David Chaum. Showing credentials without identification: Signatures transferred between unconditionally unlinkable pseudonyms. In Franz Pichler, editor, *Advances in Cryptology – EUROCRYPT'85*, volume 219 of *Lecture Notes in Computer Science*, pages 241–244, Linz, Austria, April 1986. Springer Berlin Heidelberg, Germany.

[CHK$^+$18] Jung Hee Cheon, Kyoohyung Han, Andrey Kim, Miran Kim, and Yongsoo Song. Bootstrapping for approximate homomorphic encryption. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018, Part I*, volume 10820 of *Lecture Notes in Computer Science*, pages 360–384, Tel Aviv, Israel, April 29 – May 3, 2018. Springer, Cham, Switzerland.

[CJS14] Andrew M. Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *J. Mathematical Cryptology*, 8(1):1–29, 2014. https://arxiv.org/abs/1012.4019.

[CKGW24] Deirdre Connolly, Chelsea Komlo, Ian Goldberg, and Christopher A. Wood. The Flexible Round-Optimized Schnorr Threshold (FROST) Protocol for Two-Round Schnorr Signatures. RFC 9591, June 2024. https://www.rfc-editor.org/info/rfc9591.

[CKKS17] Jung Hee Cheon, Andrey Kim, Miran Kim, and Yong Soo Song. Homomorphic encryption for arithmetic of approximate numbers. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 409–437, Hong Kong, China, December 3–7, 2017. Springer, Cham, Switzerland.

[CL01] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Birgit Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 93–118, Innsbruck, Austria, May 6–10, 2001. Springer Berlin Heidelberg, Germany.

[CLG09] Denis Xavier Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, January 2009.

[CLM$^+$18] 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.

[CLOT21] Ilaria Chillotti, Damien Ligier, Jean-Baptiste Orfila, and Samuel Tap. Improved programmable bootstrapping with larger precision and efficient arithmetic circuits for TFHE. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2021, Part III*, volume 13092 of *Lecture Notes in Computer Science*, pages 670–699, Singapore, December 6–10, 2021. Springer, Cham, Switzerland.

[Com25] European Commission. A coordinated implementation roadmap for the transition to post-quantum cryptography, 2025. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

[Cou06] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006.

[CS19] Daniele Cozzo and Nigel P. Smart. Sharing the LUOV: Threshold post-quantum signatures. In Martin Albrecht, editor, *17th IMA International Conference on Cryptography and Coding*, volume 11929 of *Lecture Notes in Computer Science*, pages 128–153, Oxford, UK, December 16–18, 2019. Springer, Cham, Switzerland.

[CSBB24] Marina Checri, Renaud Sirdey, Aymen Boudguiga, and Jean-Paul Bultel. On the practical CPA^D security of “exact” and threshold FHE schemes and libraries. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology – CRYPTO 2024, Part III*, volume 14922 of *Lecture Notes in Computer Science*, pages 3–33, Santa Barbara, CA, USA, August 18–22, 2024. Springer, Cham, Switzerland.

[Dat] DataGuard. NIS2 Requirements: A Complete Guide to Compliance & Encryption. https://www.dataguard.com/nis2/requirements/.

[DDGR20] Dana Dachman-Soled, Léo Ducas, Huijing Gong, and Mélissa Rossi. LWE with side information: Attacks and concrete security estimation. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020, Part II*, volume 12171 of *Lecture Notes in Computer Science*, pages 329–358, Santa Barbara, CA, USA, August 17–21, 2020. Springer, Cham, Switzerland.

[dEK$^+$23] Rafael del Pino, Thomas Espitau, Shuichi Katsumata, Mary Maller, Fabrice Mouhartem, Thomas Prest, Mélissa Rossi, and Markku-Juhani Saarinen. Raccoon. Technical report, National Institute of Standards and Technology, 2023. available at https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures.

[DF90] Yvo Desmedt and Yair Frankel. Threshold cryptosystems. In Gilles Brassard, editor, *Advances in Cryptology – CRYPTO’89*, volume 435 of *Lecture Notes in Computer Science*, pages 307–315, Santa Barbara, CA, USA, August 20–24, 1990. Springer, New York, USA.

[DIW24] Alex Davidson, Jana Iyengar, and Christopher A. Wood. The Privacy Pass Architecture. RFC 9576, June 2024.

[DKL$^+$20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact post-quantum signatures from quaternions and isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020, Part I*, volume 12491 of *Lecture Notes in Computer Science*, pages 64–93, Daejeon, South Korea, December 7–11, 2020. Springer, Cham, Switzerland.

[DKLW25] Adrien Dubois, Michael Klooß, Russell W. F. Lai, and Ivy K. Y. Woo. Lattice-based proof-friendly signatures from vanishing short integer solutions. In Tibor Jager and Jiaxin Pan, editors, *PKC 2025: 28th International Conference on Theory and Practice of Public Key Cryptography, Part I*, volume 15674 of *Lecture Notes in Computer Science*, pages 452–486, Røros, Norway, May 12–15, 2025. Springer, Cham, Switzerland.

[DKM$^+$24] Rafaël Del Pino, Shuichi Katsumata, Mary Maller, Fabrice Mouhartem, Thomas Prest, and Markku-Juhani O. Saarinen. Threshold raccoon: Practical threshold signatures from standard lattice assumptions. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology – EUROCRYPT 2024, Part II*, volume 14652 of *Lecture Notes in Computer Science*, pages 219–248, Zurich, Switzerland, May 26–30, 2024. Springer, Cham, Switzerland.

[DKR24] Jack Doerner, Yashvanth Kondi, and Leah Namisa Rosenbloom. Sometimes you can't distribute random-oracle-based proofs. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology – CRYPTO 2024, Part V*, volume 14924 of *Lecture Notes in Computer Science*, pages 323–358, Santa Barbara, CA, USA, August 18–22, 2024. Springer, Cham, Switzerland.

[DLRW24] Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. SQIsignHD: New dimensions in cryptography. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology – EUROCRYPT 2024, Part I*, volume 14651 of *Lecture Notes in Computer Science*, pages 3–32, Zurich, Switzerland, May 26–30, 2024. Springer, Cham, Switzerland.

[DM15] Léo Ducas and Daniele Micciancio. FHEW: Bootstrapping homomorphic encryption in less than a second. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 617–640, Sofia, Bulgaria, April 26–30, 2015. Springer Berlin Heidelberg, Germany.

[DMR11] Hang Dinh, Cristopher Moore, and Alexander Russell. McEliece and Niederreiter cryptosystems that resist quantum Fourier sampling attacks. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 761–779, Santa Barbara, CA, USA, August 14–18, 2011. Springer Berlin Heidelberg, Germany.

[Dol19] Florian Dold. The GNU Taler System: Practical and Provably Secure Electronic Payments. Doctoral Thesis, L'Université de Rennes, 2019. https://taler.net/papers/thesis-dold-phd-2019.pdf.

[DPH25] Flo D, Michael P, and Britta Hale. Terminology for Post-Quantum Traditional Hybrid Schemes. RFC 9794, June 2025. https://www.rfc-editor.org/info/rfc9794.

[DR24] Loïc Demange and Mélissa Rossi. A provably masked implementation of BIKE key encapsulation mechanism. *IACR Communications in Cryptology (CiC)*, 1(1):23, 2024.

[EC24] European Commission. Commission Recommendation (EU) 2024/1101. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401101, 2024. Official Journal of the European Union.

[ECC23] European Cybersecurity Competence Centre (ECCC). Cyber Digital Europe Programme: EUR 84m to Support Cybersecurity Deployment Actions. https://cybersecurity-centre.europa.eu/news/

cyber-digital-europe-programme-eur-84m-support-cybersecurity-deployment-actions
en, 2023.

[ECC25] European Cybersecurity Competence Centre (ECCC). New ECCC Funding Opportunities under Digital Europe and Horizon Europe Programmes are Open. https://cybersecurity-centre.europa.eu/news/new-eccc-funding-opportunities-under-digital-europe-and-horizon-europe-programm
en, 2025.

[ENI22] ENISA. Post-quantum cryptography: Anticipating threats and preparing the future, 2022. https://www.enisa.europa.eu/news/enisa-news/post-quantum-cryptography-anticipating-threats-and-preparing-the-future.

[ENI24a] ENISA. European Cybersecurity Certification Group Sub-group on Cryptography. Agreed Cryptographic Mechanisms (Version 2). https://certification.enisa.europa.eu/document/download/a845662b-aee0-484e-9191-890c4cfa7aaa_en?filename=ECCG%20Agreed%20Cryptographic%20Mechanisms%20version%202.pdf, 2024.

[ENI24b] ENISA. NIS Investments 2024. https://www.enisa.europa.eu/sites/default/files/2024-11/CSPA-NISInvestments-2024_0.pdf, 2024.

[ESTX24] Muhammed F Esgin, Ron Steinfeld, Erkan Tairi, and Jie Xu. Leopard: Towards practical post-quantum oblivious prfs via interactive lattice problems. *Cryptology ePrint Archive*, 2024.

[ETS25] ETSI TC CYBER. Quantum-safe cryptography (qsc); quantum-safe hybrid key establishment. Technical Report TS 103 744 V1.2.1, ETSI, March 2025. https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.02.01_60/ts_103744v010201p.pdf.

[Eve25] Evertrust. Post-quantum cryptography enterprise migration 2025: Why european enterprises lag behind, 2025. https://evertrust.io/pqc-center/post-quantum-cryptography-enterprise-migration-2025/.

[Fis06] Marc Fischlin. Round-optimal composable blind signatures in the common reference string model. In Cynthia Dwork, editor, *Advances in Cryptology – CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 60–77, Santa Barbara, CA, USA, August 20–24, 2006. Springer Berlin Heidelberg, Germany.

[FR25a] Thibauld Feneuil and Matthieu Rivain. CAPSS: A framework for SNARK-friendly post-quantum signatures. Cryptology ePrint Archive, Report 2025/061, 2025.

[FR25b] Thibauld Feneuil and Matthieu Rivain. Threshold Computation in the Head: Improved Framework for Post-Quantum Signatures and Zero-Knowledge Arguments. *J. Cryptol.*, 38(3):28, 2025.

[Fs24] Matteo Frigo and abhi shelat. Anonymous credentials from ECDSA. Cryptology ePrint Archive, Report 2024/2010, 2024.

[FV12] Junfeng Fan and Frederik Vercauteren. Somewhat practical fully homomorphic encryption. Cryptology ePrint Archive, Report 2012/144, 2012.

[GBA21] Antonio Guimarães, Edson Borin, and Diego F. Aranha. Revisiting the functional bootstrap in TFHE. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(2):229–253, 2021.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In Michael Mitzenmacher, editor, *41st Annual ACM Symposium on Theory of Computing*, pages 169–178, Bethesda, MD, USA, May 31 – June 2, 2009. ACM Press.

[GHM+22] Kristian Gjøsteen, Thomas Haines, Johannes Müller, Peter B. Rønne, and Tjerand Silde. Verifiable decryption in the head. In Khoa Nguyen, Guomin Yang, Fuchun Guo, and Willy Susilo, editors, *ACISP 22: 27th Australasian Conference on Information Security and Privacy*, volume 13494 of *Lecture Notes in Computer Science*, pages 355–374, Wollongong, NSW, Australia, November 28–30, 2022. Springer, Cham, Switzerland.

[GHS12] Craig Gentry, Shai Halevi, and Nigel P. Smart. Homomorphic evaluation of the AES circuit. Cryptology ePrint Archive, Report 2012/099, 2012.

[GMO16] Irene Giacomelli, Jesper Madsen, and Claudio Orlandi. ZKBoo: Faster zero-knowledge for Boolean circuits. In Thorsten Holz and Stefan Savage, editors, *USENIX Security 2016: 25th USENIX Security Symposium*, pages 1069–1083, Austin, TX, USA, August 10–12, 2016. USENIX Association.

[Gol25] Oskar Goldhahn. On composing generic voting schemes for improved privacy. Cryptology ePrint Archive, Report 2025/069, 2025.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th Annual ACM Symposium on Theory of Computing*, pages 197–206, Victoria, BC, Canada, May 17–20, 2008. ACM Press.

[GSPH+21] Shruthi Gorantala, Rob Springer, Sean Purser-Haskell, William Lam, Royce Wilson, Asra Ali, Eric P. Astor, Itai Zukerman, Sam Ruth, Christoph Dibak, Phillipp Schoppmann, Sasha Kulankhina, Alain Forget, David Marn, Cameron Tew, Rafael Misoczki, Bernat Guillen, Xinyu Ye, Dennis Kraft, Damien Desfontaines, Aishe Krishnamurthy, Miguel Guevara, Irippuge Milinda Perera, Yurii Sushko, and Bryant Gipson. A general purpose transpiler for fully homomorphic encryption. Technical report, Google LLC, 2021.

[HHM+24] Lena Heimberger, Tobias Hennerbichler, Fredrik Meisingseth, Sebastian Ramacher, and Christian Rechberger. Oprfs from isogenies: designs and analysis. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, pages 575–588, 2024.

[HKL+25] Lena Heimberger, Daniel Kales, Riccardo Lolato, Omid Mir, Sebastian Ramacher, and Christian Rechberger. Leap: A fast, lattice-based oprf with application to private set intersection. In *Annual International Conference on the*

Theory and Applications of Cryptographic Techniques, pages 254–283. Springer, 2025.

[HLM+25] Lucjan Hanzlik, Yi-Fu Lai, Marzio Mula, Eugenio Paracucchi, Daniel Slamanig, and Gang Tang. Tanuki: New frameworks for (concurrently secure) blind signatures from post-quantum groups actions. Cryptology ePrint Archive, Report 2025/1100, 2025.

[HPR20] Thomas Haines, Olivier Pereira, and Peter B. Rønne. Short paper: An update on marked mix-nets: An attack, a fix and PQ possibilities. In Matthew Bernhard, Andrea Bracciali, L. Jean Camp, Shin'ichiro Matsuo, Alana Maurushat, Peter B. Rønne, and Massimiliano Sala, editors, *FC 2020 Workshops*, volume 12063 of *Lecture Notes in Computer Science*, pages 360–368, Kota Kinabalu, Malaysia, February 14, 2020. Springer, Cham, Switzerland.

[HPR+21] Anna-Lena Horlemann, Sven Puchinger, Julian Renner, Thomas Schamberger, and Antonia Wachter-Zeh. Information-set decoding with hints. Cryptology ePrint Archive, Report 2021/279, 2021.

[HPRR20] James Howe, Thomas Prest, Thomas Ricosset, and Mélissa Rossi. Isochronous gaussian sampling: From inception to implementation. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020*, pages 53–71, Paris, France, April 15–17, 2020. Springer, Cham, Switzerland.

[HSS24] Patrick Hough, Caroline Sandsbråten, and Tjerand Silde. More efficient lattice-based electronic voting from NTRU. *IACR Communications in Cryptology (CiC)*, 1(4):10, 2024.

[IKOS07] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-knowledge from secure multiparty computation. In David S. Johnson and Uriel Feige, editors, *39th Annual ACM Symposium on Theory of Computing*, pages 21–30, San Diego, CA, USA, June 11–13, 2007. ACM Press.

[Ins24] Global Risk Institute. Quantum threat timeline report 2024. Technical report, Global Risk Institute, 2024. https://globalriskinstitute.org/mp-files/quantum-threat-timeline-report-2024.pdf/.

[Ins25] The Quantum Insider. Eu presses for quantum-safe encryption by 2030 as risks grow, June 2025. https://thequantuminsider.com/2025/06/30/eu-presses-for-quantum-safe-encryption-by-2030-as-risks-grow/.

[JD11] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, *Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011*, pages 19–34, Tapei, Taiwan, November 29 – December 2 2011. Springer Berlin Heidelberg, Germany.

[JKX18] Stanislaw Jarecki, Hugo Krawczyk, and Jiayu Xu. OPAQUE: An asymmetric PAKE protocol secure against pre-computation attacks. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018,* *Part III*, volume 10822 of *Lecture Notes in Computer Science*, pages 456–486, Tel Aviv, Israel, April 29 – May 3, 2018. Springer, Cham, Switzerland.

[JS25] Corentin Jeudy and Olivier Sanders. Improved lattice blind signatures from recycled entropy. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology – CRYPTO 2025, Part I*, volume 16000 of *Lecture Notes in Computer Science*, pages 477–513, Santa Barbara, CA, USA, August 17–21, 2025. Springer, Cham, Switzerland.

[Key25] Keyfactor. Pqc glossary - chimera certificates, 2025. https://docs.keyfactor.com/solution-areas/latest/pqc-glossary.

[KG20] Chelsea Komlo and Ian Goldberg. FROST: Flexible round-optimized Schnorr threshold signatures. In Orr Dunkelman, Michael J. Jacobson, Jr., and Colin O'Flynn, editors, *SAC 2020: 27th Annual International Workshop on Selected Areas in Cryptography*, volume 12804 of *Lecture Notes in Computer Science*, pages 34–65, Halifax, NS, Canada (Virtual Event), October 21-23, 2020. Springer, Cham, Switzerland.

[KKW18] Jonathan Katz, Vladimir Kolesnikov, and Xiao Wang. Improved non-interactive zero knowledge with applications to post-quantum signatures. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *ACM CCS 2018: 25th Conference on Computer and Communications Security*, pages 525–537, Toronto, ON, Canada, October 15–19, 2018. ACM Press.

[KLLQ23] Shuichi Katsumata, Yi-Fu Lai, Jason T. LeGrow, and Ling Qin. CSI-Otter: Isogeny-based (partially) blind signatures from the class group action with a twist. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology – CRYPTO 2023, Part III*, volume 14083 of *Lecture Notes in Computer Science*, pages 729–761, Santa Barbara, CA, USA, August 20–24, 2023. Springer, Cham, Switzerland.

[Koc96] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Neal Koblitz, editor, *Advances in Cryptology – CRYPTO'96*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113, Santa Barbara, CA, USA, August 18–22, 1996. Springer Berlin Heidelberg, Germany.

[KS25] Jonathan Katz and Marek Sefranek. Issuer hiding for BBS-based anonymous credentials. Cryptology ePrint Archive, Paper 2025/2080, 2025.

[LDK+22] 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, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

[LLK+22] Yongwoo Lee, Joon-Woo Lee, Young-Sik Kim, Yongjune Kim, Jong-Seon No, and HyungChul Kang. High-precision bootstrapping for approximate homomorphic encryption by error variance minimization. In Orr Dunkelman and Stefan

Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022, Part I*, volume 13275 of *Lecture Notes in Computer Science*, pages 551–580, Trondheim, Norway, May 30 – June 3, 2022. Springer, Cham, Switzerland.

[LM21] Baiyu Li and Daniele Micciancio. On the security of homomorphic encryption on approximate numbers. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021, Part I*, volume 12696 of *Lecture Notes in Computer Science*, pages 648–677, Zagreb, Croatia, October 17–21, 2021. Springer, Cham, Switzerland.

[LP25a] Yi-Fu Lai and Edoardo Persichetti. LEAF: Compact and efficient blind signature from code-based assumptions. Cryptology ePrint Archive, Report 2025/1585, 2025.

[LP25b] Oleksandra Lapiha and Thomas Prest. A lattice-based ind-cca threshold kem from the bchk+ transform. In *Advanced in Cryptology - ASIACRYPT 2025*, Lecture Notes in Computer Science, 2025.

[LSS24] Vadim Lyubashevsky, Gregor Seiler, and Patrick Steuer. The LaZer library: Lattice-based zero knowledge and succinct proofs for quantum-safe privacy. In Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie, editors, *ACM CCS 2024: 31st Conference on Computer and Communications Security*, pages 3125–3137, Salt Lake City, UT, USA, October 14–18, 2024. ACM Press.

[Lyu12] Vadim Lyubashevsky. Lattice signatures without trapdoors. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 738–755, Cambridge, UK, April 15–19, 2012. Springer Berlin Heidelberg, Germany.

[Mar25] Marin Ivezic. Hybrid Cryptography for the Post-Quantum Era. https://postquantum.com/post-quantum/hybrid-cryptography-pqc/, 2025.

[MMP+23] 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.

[MN24] Mark Manulis and Jérôme Nguyen. Fully homomorphic encryption beyond IND-CCA1 security: Integrity through verifiability. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology – EUROCRYPT 2024, Part II*, volume 14652 of *Lecture Notes in Computer Science*, pages 63–93, Zurich, Switzerland, May 26–30, 2024. Springer, Cham, Switzerland.

[Nat24] National Institute of Standards and Technology. Transition to post-quantum cryptography standards. Technical Report IR 8547 Initial Public Draft, NIST, November 2024. https://csrc.nist.gov/pubs/ir/8547/ipd.

[NCC] NIST NCCoE. Frequently asked questions about post-quantum cryptography. https://pages.nist.gov/nccoe-migration-post-quantum-cryptography/.

[NCC23] NIST NCCoE. Nist special publication 1800-38b: Migration to post-quantum cryptography, December 2023. https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf.

[NIS25] NIS EU PQC Workstream. European Commission. Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography, 2025.

[NLV11] Michael Naehrig, Kristin E. Lauter, and Vinod Vaikuntanathan. Can homomorphic encryption be practical? In Christian Cachin and Thomas Ristenpart, editors, *Proceedings of the 3rd ACM Cloud Computing Security Workshop, CCSW 2011, Chicago, IL, USA, October 21, 2011*, pages 113–124. ACM, 2011.

[NOC$^+$24] Kohei Nakagawa, Hiroshi Onuki, Wouter Castryck, Mingjie Chen, Riccardo Invernizzi, Gioella Lorenzon, and Frederik Vercauteren. SQIsign2D-East: A new signature scheme using 2-dimensional isogenies. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology – ASIACRYPT 2024, Part III*, volume 15486 of *Lecture Notes in Computer Science*, pages 272–303, Kolkata, India, December 9–13, 2024. Springer, Singapore, Singapore.

[(NS22] United States National Security Agency (NSA). Commercial national security algorithm suite 2.0 (cnsa 2.0), September 2022. https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF.

[OGP$^+$25a] Mike Ounsworth, John Gray, Massimiliano Pala, Jan Klaußner, and Scott Fluhrer. Composite ML-DSA for use in X.509 Public Key Infrastructure. Internet-Draft draft-ietf-lamps-pq-composite-sigs-13, Internet Engineering Task Force, October 2025. https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/13/.

[OGP$^+$25b] Mike Ounsworth, John Gray, Massimiliano Pala, Jan Klaußner, and Scott Fluhrer. Composite ML-KEM for use in X.509 Public Key Infrastructure. Internet-Draft draft-ietf-lamps-pq-composite-kem-10, Internet Engineering Task Force, November 2025. https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-kem/10/.

[Pei09] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In Michael Mitzenmacher, editor, *41st Annual ACM Symposium on Theory of Computing*, pages 333–342, Bethesda, MD, USA, May 31 – June 2, 2009. ACM Press.

[Pei20] Chris Peikert. He gives C-sieves on the CSIDH. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 463–492, Zagreb, Croatia, May 10–14, 2020. Springer, Cham, Switzerland.

[PFH+22] 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, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

[PPZ24] Christian Paquin, Guru-Vamsi Policharla, and Greg Zaverucha. Crescent: Stronger privacy for existing credentials. Cryptology ePrint Archive, Report 2024/2013, 2024.

[PQS25] PQShield. Eu pqc workstream publishes 'a coordinated implementation roadmap for the transition to post-quantum cryptography', 2025. https://pqshield.com/eu-pqc-workstream-publishes-a-coordinated-implementation-roadmap-for-the-transi

[PSGR25] Lucas Prabel, Sun Shuzhou, John Gray, and Tirumaleswar Reddy.K. PQ/T Hybrid Composite Signatures for JOSE and COSE. Internet-Draft draft-prabel-jose-pq-composite-sigs-04, Internet Engineering Task Force, August 2025. https://datatracker.ietf.org/doc/draft-prabel-jose-pq-composite-sigs/04/.

[RAD78] Ronald L. Rivest, Len Adleman, and Michael L. Dertouzos. On data banks and privacy homomorphisms. In *Foundation of Secure Computations*, pages 169–180. Academic Press, 1978. https://archive.org/details/foundationsofsec0000unse/page/n9/mode/2up.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th Annual ACM Symposium on Theory of Computing*, pages 84–93, Baltimore, MA, USA, May 22–24, 2005. ACM Press.

[RHHM17] Melissa Rossi, Mike Hamburg, Michael Hutter, and Mark E. Marson. A side-channel assisted cryptanalytic attack against QcBits. In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems – CHES 2017*, volume 10529 of *Lecture Notes in Computer Science*, pages 3–23, Taipei, Taiwan, September 25–28, 2017. Springer, Cham, Switzerland.

[Rob23] 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.

[RS06] Alexander Rostovtsev and Anton Stolbunov. Public-Key Cryptosystem Based On Isogenies. Cryptology ePrint Archive, Report 2006/145, 2006.

[SAB+22] Peter Schwabe, Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, Damien Stehlé, and Jintai Ding. CRYSTALS-KYBER. Technical report, National Institute of Standards and Technology, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

[Sen00] Nicolas Sendrier. Finding the permutation between equivalent linear codes: The support splitting algorithm. *IEEE Trans. Inf. Theory*, 46(4):1193–1203, 2000.

[SFG25] Douglas Stebila, Scott Fluhrer, and Shay Gueron. Hybrid key exchange in TLS 1.3. Internet-Draft draft-ietf-tls-hybrid-design-16, Internet Engineering Task Force, September 2025. https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/16/.

[Tel19] TeleTrusT. Guideline: State of the Art in IT Security. https://www.teletrust.de/fileadmin/docs/fachgruppen/2019-02_TeleTrusT_Guideline_State_of_the_art_in_IT_security_ENG.pdf, 2019.

[Tel25] TeleTrusT. Guideline: State of the Art in IT Security. https://www.teletrust.de/fileadmin/user_upload/2025-09_TeleTrusT_Guideline_State_of_the_art_in_IT_security_EN.pdf, 2025.

[TGF+23] Alexander Truskovsky, Daniel Van Geest, Scott Fluhrer, Panos Kampanakis, Mike Ounsworth, and Serge Mister. Multiple Public-Key Algorithm X.509 Certificates. Internet-Draft draft-truskovsky-lamps-pq-hybrid-x509-02, Internet Engineering Task Force, August 2023. https://datatracker.ietf.org/doc/draft-truskovsky-lamps-pq-hybrid-x509/02/.

[TS10] Sean Turner and Jim Schaad. Multiple Signatures in Cryptographic Message Syntax (CMS). RFC 5752, January 2010. https://www.rfc-editor.org/info/rfc5752.

[TTB+23] C. Tjhai, M. Tomlinson, G. Bartlett, Scott Fluhrer, Daniel Van Geest, Oscar Garcia-Morchon, and Valery Smyslov. Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2). RFC 9370, May 2023. https://www.rfc-editor.org/info/rfc9370.

[UK 25] UK National Cyber Security Centre (NCSC). Pqc migration roadmap unveiled. https://www.ncsc.gov.uk/news/pqc-migration-roadmap-unveiled, 2025. UK's detailed roadmap for preparing and transitioning to post-quantum cryptography.

[VSL24] Valentin Vakarjuk, Ilya Snetkov, and Anne Laud. Identifying obstacles of post-quantum cryptography migration in e-estonia. In *Cyber Conflict (CyCon) 2024*, 2024. https://ccdcoe.org/uploads/2024/05/CyCon_2024_Vakarjuk_Snetkov_Laud-1.pdf.

[YBH+25] Yibin Yang, Fabrice Benhamouda, Shai Halevi, Hugo Krawczyk, and Tal Rabin. Gold oprf: Post-quantum oblivious power-residue prf. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 259–278. IEEE, 2025.

[Zam22] Zama. Concrete: TFHE Compiler that converts python programs into FHE equivalent, 2022. https://github.com/zama-ai/concrete.

[ZCD+20] 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`.