Literature Review

A Survey of Zero-Knowledge Proofs in a Post-Quantum Context

Sam Benoist[1], Alexa Krempa[2], Bryan Richiez[3], Jay Shah[4], and Gaia Sergent[5]

[1]Department of Computing Security, B. Thomas Golisano College of Computing and Information Sciences, Rochester Institute of Technology

May 2, 2022

Abstract

Research and development into quantum computing grow daily, yet they come at the expense of the cryptographic systems responsible for much of the security architecture that we rely on. As this technology progresses, so does the need to determine the quantum resilience of current protocols. Here we will look into the possible quantum resilience of zero-knowledge proofs (ZKPs). ZKPs have a number of implementations that focus on improving the security of the authentication process and protecting data privacy. To do this, we conducted a literature review of the current state of research on this subject and analyzed our findings. To reduce the scope of our research, we focused on the ZKP application with the post-quantum algorithm CRYSTALS, which is in NIST's competition to standardize quantum-resistant cryptosystems. We presented some of our findings as graphs and tables where we found these formats beneficial for the reader. Using frequency analysis of key phrases, we found the frequency of research papers that reference ZKPs, post-quantum cryptography (PQC), and CRYSTALS has increased over the past seven years. Our review indicates the need for cryptographers to conduct further research regarding ZKPs and other post-quantum algorithms. The quantum resilience of protocols is a crucial and time-sensitive topic to ensure the security of systems in a post-quantum world.

Keywords

Post-Quantum, Zero-knowledge, cryptography, Post-quantum cryptography, quantum-safe, CRYSTALS, Quantum computing

1 Introduction

One of the most pressing challenges currently facing the security community is the issue of preserving privacy, while also preparing for the ways quantum computing will reshape threats to privacy and security. The way we mitigate threats, especially relating to encryption and authentication, will change dramatically in a post-quantum context.

Security professionals deduce the issue of data privacy to many underlying factors. What they have found more often than not is that many implemented systems are insecure by design. The recent rise in popularity surrounding ZKPs has given way to newfound hope that data breaches could soon be a thing of the past. ZKPs are a mathematical technique to verify information while keeping the information completely confidential. ZKPs demonstrate the validity of data to third parties without revealing it, promise to privatize any transaction between any number of parties, and can be used by any encryption scheme [1]. ZKPs have been formally proven in classical computing, but face a larger variety of threats in a post-quantum context.

The rapid explosion of research in quantum computing has transformed what was once thought of as impossible into what may become one of the greatest scientific and engineering advancements of our generation. Inherent to the dramatic advances this technology has to offer, quantum computing threatens encryption as we know it [2]. Quantum computing works by replacing traditional binary calculations of 1's and 0's with qubits. Qubits can be likened to traditional bits. However, they have the ability to exist in a state of superposition, acting as both a 1 and 0 simultaneously. These properties supercharge computing power and render the pub-

lic key encryption algorithms that many systems rely upon irrelevant.

In this paper, we perform a literature review to outline the current state of research in post-quantum encryption and the use of our findings in zero-knowledge environments. We analyzed notions from top researchers and cryptographers who have studied PQCs and ZKPs. We also analyzed the current NIST Post Quantum Cryptography standardization process, specifying our focus on the CRYSTALS family of algorithms [3]. We explore patterns in our findings and acknowledge areas where those developing PQC and ZKP-based cryptosystems should further research. It is our belief that quantum-resistant encryption used in conjunction with a ZKP implementation offers the most benefit in securing data and protecting privacy in the post-quantum world. Attackers are more prevalent than ever, and this research is key in discovering design-level threats. We hope our findings are useful to those exploring the issues at hand as well as the industry professionals implementing these systems.

2 Background & Significance

The research problem our literature review focuses on is whether quantum resilient ZKP implementations exist. Due to both time and resource constraints, we chose to focus on one post-quantum algorithm family to answer this question: the CRYSTALS algorithm family. NIST features this algorithm in the 3rd round of their Post-Quantum Cryptography Standardization Process. This algorithm family best serves our research question, as it provides a candidate for both a public-key encryption algorithm (CRYSTALS-KYBER) and a digital signature algorithm (CRYSTALS-DILITHIUM). The CRYSTALS algorithm family is the only one within the competition to do so.[4]

Through this literature review, we aim to determine:

1. Whether quantum resilient ZKP implementations exist.
2. Whether the CRYSTALS algorithm family comprehensively satisfies the objectives of a zero-knowledge proof.
3. What trends exist in the research being done on PQCs, ZKPs, and CRYSTALS.

While the main question this survey seeks to answer is our core research question (1), we can answer both (2) and (3), and use these additional questions to frame the context (1) is answered within. Many popular ZKP implementations in classical computing are closely tied to network protocols, which need to implement Non-Interactive ZKP to function in the post-quantum landscape. Additionally, NIST ruled out most Non-Interactive ZKP implementations for both its digital signature and encryption PQC challenge. PICNIC, one implementation of a Non-Interactive ZKP, is an alternate in the third round of the competition.[5]

We chose this topic due to the uncertain future of cryptography. Given the impending creation of commercial quantum computers, it is vital that the quantum resilience of protocols be determined prior to this. We also believe that the issue of data privacy is one of the most vital challenges to overcome. In classical computing, ZKPs can be integrated into many underlying systems to confirm that the prover possesses the knowledge in any transaction without revealing this knowledge. However, for cryptosystems designed to operate within a post-quantum context, lattice-based cryptosystems seem to be a widely researched and verified alternative.[6]

CRYSTALS is a lattice-based algorithm family that has been widely tested and verified. Many researchers think that of the candidate algorithms, NIST will likely select an algorithm from this family [4]. As such, we feel that using the CRYSTALS algorithm family will be comprehensively implemented in the future. Therefore, it is crucial to analyze the research performed regarding CRYSTALS. Verification that the CRYSTALS algorithms fulfill the same goals in a quantum context that ZKPs do in classical computing would benefit the CRYSTALS developers. Doing so would increase its likelihood of being chosen by NIST for PQC Standardization. Further research may then be conducted on NIST's other final candidates as it relates to lattice-based cryptosystems and ZKP based cryptosystems.

We conducted our literature review through various forms of online research. Specifically, we utilized Google Scholar and the Rochester Institute of Technology Library's 'Summon' search engine. We optimized our results through the use of a variety of keyphrases and keywords. Resources were also provided to us by professors knowledgeable on this subject. Through our analysis of the high density of research papers we discovered, we were able to draw conclusions surrounding our research problems.

3 Related Work

There has been significant research into PQCs, and the field continues to develop each year. To

serve as a baseline for our understanding and analysis of current trends, as well as to consider under-searched areas, we found several literature reviews to analyze.

Recent developments in post-quantum algorithms help to compare the ZKP-based cryptosystems with NIST's designated third-round candidates for each category. NIST's third-round post-quantum candidates include Picnic and CRYSTALS [7]. Practitioners can implement the different cryptosystems introduced by these developments. These cryptosystems include post-quantum public-key and signing cryptosystems. The common types of cryptosystems that cryptographers are researching and developing are code-based, multivariate-based, and lattice-based cryptosystems. In the past, many researchers have proposed post-quantum code-based signing algorithms. The basis of some of the most relevant sub-types of these kinds of cryptosystems are the schemes from Niederreiter and CFS [8]. The signatures of such schemes are short in length and the verifier can verify them quickly. However, as with traditional McEliece's cryptosystems, the use of large key sizes requires significant computational resources and, therefore, signature generation may become inefficient. Code-based cryptographic schemes provide between 128 and 256 bits of classical security, but a significant reduction of security levels occurs when systems or protocols implement this algorithm in a quantum context [8]. On average, even when making use of compression techniques, the size of code-based scheme keys is clearly larger than the one required by current RSA-based encryption systems.

In multivariate-based signature schemes, the scheme generates the public key, which is generated through a trapdoor function that acts as the private key. Cryptographers often use this factor to create large public keys. However, it's also used to create very small signatures, where the size of the signature is comparable with the commonly used RSA signature. Multivariate-based schemes rely on the complexity of solving systems of multivariate equations, which can be NP-hard or NP-complete [8]. Despite the scheme's resistance to quantum attacks, cryptographers need to perform further research focusing on improving its decryption speed and reducing its large key size to make this scheme practical. The basis of cryptographic schemes in lattice-based cryptosystems are lattices, which are sets of points in n-dimensional spaces with a periodic structure. Lattice-based security schemes rely on the presumed hardness of lattice problems like the Shortest Vector Problem (SVP), which is an NP-hard problem whose objective is to find the shortest non-zero vector within a lattice. Among the different lattice-based signature schemes described in the literature, those based on the Short Integer Solution seem to be promising due to their reduced key size.

In summary, all related works mentioned are highly detailed, and many of them cover more sources than we had the ability to analyze in our limited research timeline. Despite this, we believe that our research is necessary and constructive as these sources primarily covered existing literature and research trends, with little focus on topics within post-quantum cryptography that require further research. We seek to both analyze existing research as well as indicate where it is lacking.

4 Research Method

To ensure that the information within the papers we used was accurate, we manually reviewed them. We did not limit the keyphrases that we could use as search query terms to discover papers, but we did enumerate fruitful keyphrases for further analysis. We used a subset of papers to provide a core knowledge base. The first stage of research focused specifically on expanding the core knowledge base and gaining an understanding of ZKPs and the post-quantum environment. The second stage of research focused on the CRYSTALS algorithm family and whether this algorithm family achieves zero-knowledge objectives. We then determined trends being done in research by analyzing the frequency of keyphrases in the abstracts of included papers.

We prioritized papers created within the last five years to accommodate our focus on recent trends. However, we could select papers created before that period if they were especially relevant or if we used the paper to expand the core knowledge base.

4.1 Limitations and Risks

We only had papers accessible to us that were available through 'Summon', which is our university library's website and journal search engine, and papers that are publicly available. The 10-week time frame within which we could perform this research was a limiting factor. Our team had limited background knowledge when it came to quantum computing and mechanics, and little-to-no knowledge of data science.

4.2 Procedures

We first established a core knowledge base we could establish an understood definition of both the current state and previous states of both ZKPs and PQCs. We formed a commonly understood timeline from our understanding of these states. If a paper did not align with our commonly understood timeline, we would need to revisit whether we should include the paper.

At the time of writing, NIST is also holding a large competition which focuses on establishing standards for post-quantum encryption and digital signature algorithms. We used the guidelines from the contest and the comments left on the algorithms to guide our understanding.

We then manually queried papers using both Summon and Google Scholar. This ensured that we only included literature that was in English, peer-reviewed, and accessible to either the public or specifically to RIT students. We also manually reviewed these papers to ensure that their contents were in-scope. This process also ensured that the literature used was free from any assumptions or biases that would affect the accuracy of our conclusions. We chose to place these limits so we would then have the best chance of understanding current, peer-reviewed literature.

We ranked the most effective keyphrases that we used in search queries by the number of papers found with queries that included the keyphrase. These queries could contain multiple keyphrases. We found this to be a useful indicator of topic popularity in included papers.

We then analyzed the trends that existed in the research being done on PQCs, ZKPs, and CRYSTALS. We performed keyphrase frequency analysis on the abstracts of the papers that we had included. We would first account for differentiation in the spellings or phrasings of especially important keyphrases, normalize the way the script represents these phrases, and would eliminate special characters. The script would then iterate through the words in the abstract, enumerate them as necessary, and parse them into keyphrases. The script will only add one keyphrase occurrence per abstract, and the script requires that the keyphrase occurs twice for it to note the keyphrase. This allows the script to avoid accounting for keyphrases unique to a paper.

The script and data used to perform this analysis are located at https://github.com/pws1453/pqc-paper-repo. We licensed the code and data in that repository under the third edition of the GNU Public License. This license allows anyone to derive projects and research from this work without needing to worry about restrictive terms.

Ranking	Search Query Keyphrase	Results
1	post quantum cryptography	18
2	zero knowledge proof	16
3	blockchain	10
4	protocols	8
5	post quantum	7
6	cryptography	7
7	nist	6
8	crystals	6
9	zkp	5
10	quantum computing	5
11	authentication	5
12	digital signature	5
13	public key encryption	4
14	quantum cryptography	4
15	zero knowledge	4
16	internet of things	4
17	security	4
18	digital signatures	3
19	quantum resistant	3
20	zero knowledge application	3
21	mutual authentication	3
22	post quantum signature	3
23	hash functions	3
24	elliptic curve cryptography	3
25	number theoretic transform	3
26	fpga	3
27	lattice based cryptography	3
28	quantum safe	2
29	interactive proof	2
30	range proof	2

Figure 1: The thirty most common keyphrases that we used in our search queries.

5 Findings

We provide our findings in this paper as five separate findings, each with different methods and objectives. Many novel zero-knowledge proof-based cryptosystems have been informally verified to be quantum resilient. However, these cryptosystems lack formal testing and verification. Because of this, many practitioners are choosing other cryptosystems that are formally tested and verified to implement.

The CRYSTALS algorithm family implements Fiat-Shamir with Aborts. This modified version of the commonly-implemented Fiat Shamir heuristic only differs in ways that are necessary to implement it successfully in a lattice-based cryptosystem. These changes include a process where the prover picks new commitments, the verifier picks a new challenge, and the prover picks a new response to the challenge. This process continues until the verifier accepts the conversation or the process exceeds a given time-bound [9]. As Fiat-Shamir with Aborts can also abort the process, these changes do not impact the overall security of the heuristic when compared to Fiat-Shamir. With this as evidence, we conclude that the CRYSTALS family of algorithms fulfills zero-knowledge objectives.

Analyzing the graph provided in Figure 2, located on page 6, we can see that when NIST's PQC contest began accepting nominations in December 2016, PQC-related and ZKP-related research began to slowly rise. The trends that

can be found in Figure 4 also indicate that PQCs and ZKP-based cryptosystems are being not only implemented but are also being optimized.

5.1 Finding 1

We were able to find many instances of novel post-quantum cryptosystems that implemented ZKPs. In one example, the author describes quantum accumulators that they made, that are compatible with Non-Interactive ZKPs. These accumulators were also able to construct logarithmic size ring signatures solely from symmetric-key primitives [10]. In another paper, the author builds a scheme based on Non-Interactive ZKPs on top of an Android message-sending application [11]. This is especially interesting with the ever-increasing number of Android-based devices. Additionally, another author built a quantum-resilient ZKP-based cryptosystem. It implements a version of the a Quantum Bit Commitment protocol that implements coherent states [12]. The author then implemented the protocol to solve the 3-colorable graph problem, which is NP-Complete. Being able to solve an NP-Complete problem is a noteworthy feat, as this denotes a problem for which no efficient solution has been found.

In the Second Round Status Report, NIST found that PICNIC had potential, and the algorithm's rapid evolution impressed them. However, NIST also found that this algorithm was not mature enough to become a candidate for standardization [3]. Of the zero-knowledge submissions presented to NIST, only PICNIC progressed to the first round. Even then, PICNIC was notably missing a formally-verified security proof under any model. As time progresses and researchers study ZKP-based cryptosystems further, these cryptosystems are good candidates for NIST or other standards bodies to standardize. The principles these schemes implement are well-regarded, but these schemes need to be further proven and hardened against attacks before they should be implemented.

5.2 Finding 2

In the short-term, lattice-based cryptosystems will likely be both the most popular and effective choices to implement in a post-quantum context. Lattice-based algorithms comprise the majority of the NIST final-round candidates [13]. This is due to how extensively researchers have studied lattice-based cryptosystems in post-quantum contexts. Both NIST candidates in the CRYSTALS family of algorithms, for example, have formal security proofs written in the Classical Random Oracle Model [7]. NIST progressed both of these schemes to the final round of their PQC competition. NIST claimed that CRYSTALS-KYBER was one of the most promising public-key encryption schemes they have considered and that CRYSTALS-DILITHIUM had strong performance and efficiency [3].

Research performed outside of the NIST competition also reflects favorably on the CRYSTALS family of algorithms. After the second-round submission of CRYSTALS-DILITHIUM was published, a team of researchers were able further optimize this submission [13]. This team noted that since the security analysis for the Quantum Random Oracle Model is well applied to CRYSTALS-DILITHIUM, they saw the algorithm as the most promising digital signature candidate in NIST's PQC competition. For ASICs and ARM-based systems, independent researchers have concluded that the security level 3 variant of CRYSTALS-DILITHIUM is the most secure version of the algorithm, and runs with little overhead [14]. Performance gains seen in one algorithm will benefit the other. This algorithm family is both secure and performant. Once standardized, practitioners should consider implementing this algorithm family in systems that need to be secure in a post-quantum context.

5.3 Finding 3

ZKPs are well known for accommodating secure transactions in contexts where privacy is not a given. Specifically, verifying whether or not a prover knows a secret without the secret being shared. Fiat-Shamir is a common heuristic that cryptographers use to convert generic ZKP schemes into non-interactive ZKPs [15]. This allows the prover to generate their challenge, which can be sent after the verifier sends their challenge. Lattice-based cryptosystems use a protocol that is commonly known as "Fiat-Shamir with Aborts" for widely the same purpose [16]. CRYSTALS-DILITHIUM implements this protocol, to ensure that security is persistent even if privacy is compromised.

Concluding that CRYSTALS meets the same objectives as a ZKP is dependent on whether Fiat-Shamir with Aborts is as effective as Fiat-Shamir. In Fiat-Shamir with Aborts, the prover only sends a response only if that response follows some condition [16]. The prover picks their commitment, the verifier picks their challenge, and the prover picks their response until the verifier accepts the conversation or until this process exceeds a given time-bound [9]. This change was

necessary, as there are attacks against lattice-based cryptosystems that exploit the transcript to get the signer's secret key[16]. As all parties regenerate these values repeatedly, the security of the system persists. As the security of both systems is similar when they're implemented in their respective cryptosystems, we conclude that CRYSTALS meets zero-knowledge objectives.

ZKP	PQC	CRYSTALS
zero-knowledge	post-quantum-cryptography	crystals-dilithium
zkp	pqc	dilithium
	post-quantum-cryptosystems	crystals-kyber
	post-quantum-cryptographic	crystals

Figure 3: Chart that maps keywords to keyphrases

5.4 Finding 4

As quantum computing progresses, the need for post-quantum cryptographic solutions increases. We performed frequency analysis on keyphrases found within the abstracts of the research that we included in the process of writing the paper [17]. The gradual increase in references to PQCs and the CRYSTALS family of algorithms is notable. This suggests a transition from focusing on classical ZKPs to focusing on PQCs and their implementations such as CRYSTALS. Through our analysis of keyphrases, we were able to create Figure 2, which identifies trends in the topics being discussed since 2015. Figure 3 gives an overview of the keyphrases and how we categorized them.

As displayed in Figure 2, the research performed focuses on ZKPs before the year 2018 with few mentions of PQCs or CRYSTALS until then. Furthermore, these topics have become more prevalent over time, with an increasing focus on PQCs rather than on classical cryptographic solutions [17]. It is worth noting that due to the varying phases our research underwent, the abstracts that underwent this analysis are inherently biased. However, as we analyzed a significant number of papers, we feel that the trends throughout the research likely do not deviate far from the results below.

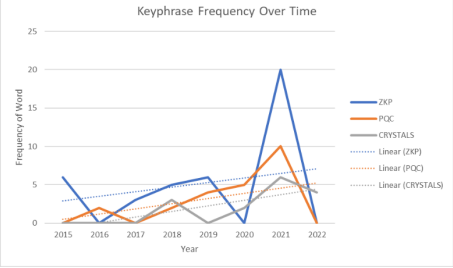

Figure 2: Frequency of keyphrases in abstracts over time

5.5 Finding 5

As knowledge of these algorithms progresses, the contexts in which cryptographers research them will also progress. We accounted for this, and enumerated the contexts that researchers had studied ZKPs, PQCs, or CRYSTALS within. This enumeration used a very similar frequency analysis process and some additional manual parsing to account for alternate variations of words [17]. We only measured frequencies until 2021 in this analysis, as the results for 2022 were both incomplete and did not point out larger trends. We chose these keyphrases to allow for trends in concepts and contexts to be easily visualized.

The trends found within this graph are telling. Research referencing the NIST competition became increasingly popular in 2018, as the competition began evaluating candidates [17]. Blockchain-related research became popular in 2019 and continues to be a very active context for research to be performed within. Abstracts with the words 'implementation' and 'performance' only became prevalent in 2020. This suggests that cryptosystems had initial implementations, which cryptographers then worked to optimize. References to 'attacks' increased dramatically in 2020, and only decreased slightly in 2021, which likely corresponds to validation and testing being done on implementations of cryptosystems.

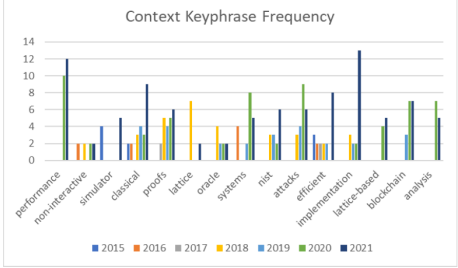

Figure 4: Frequency of context keyphrases in abstracts over time

6 Conclusions

As discussed in this paper, the dramatic advances of quantum computing have threatened classical encryption schemes and the concepts behind ZKPs. Through our analysis, we were able to identify trends in keyphrases within abstracts of research papers and see trends in the information presented in the past seven years. As we analyzed papers, we were able to identify multiple PQC algorithms. Algorithms detailed in NIST's PQC competition all try to solve the problem of authentication in a post-quantum context. We found that CRYSTALS, one of the most promising algorithm families participating in this competition, fulfills similar objectives as an algorithm that implements ZKPs in classical computing.

Our paper offers a comprehensive overview of the current state and trends of research in PQCs and ZKPs. Further validation of this research by professionals who have more experience in this area would allow the academic community to be sure of our results. Implementation of ZKP-based cryptosystems in a post-quantum context is possible, as proven by Picnic's success in the NIST competition. The comments that NIST has made regarding PICNIC are overwhelmingly positive. However, those developing these algorithms need to perform more research and formal validation so then practitioners may confidently implement these cryptosystems. NIST's comments align with this view. If ZKP-based cryptosystems become mature enough to gain formal verification in a post-quantum model, they could change the security landscape forever.

7 Acknowledgments

We'd like to thank those who supported us as we wrote this literature review. We want to specifically thank the Rochester Institute of Technology for the use of their library's resources. Also, a special thanks to our fellow teammates who put in the hard work to complete this literature review.

References

[1] Yang X, Li W. A zero-knowledge-proof-based digital identity management scheme in blockchain. Computers Security. 2020;99:102050. Available from: https://www.sciencedirect.com/science/article/pii/S0167404820303230.

[2] Ben-Sasson E, Bentov I, Horesh Y, Riabzev M. Scalable, transparent, and post-quantum secure computational integrity; 2018. https://ia.cr/2018/046. Cryptology ePrint Archive, Report 2018/046.

[3] Moody D, Alagic G, Apon D, Cooper D, Dang Q, Kelsey J, et al.. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD; 2020.

[4] Di Chiano N, Longo R, Meneghetti A, Santilli G. A survey on NIST PQ signatures. arXiv preprint arXiv:210711082. 2021.

[5] Picnic | SpringerLink. springerLink; 2020. Available from: https://link.springer.com/chapter/10.1007/978-3-030-57682-0_8.

[6] Morais E, Koens T, van Wijk C, Koren A. A survey on Zero knowledge range proofs and Applications - SN Applied Sciences. Springer International Publishing; 2019. Available from: https://link.springer.com/article/10.1007/s42452-019-0989-z.

[7] Alagic G, Alperin-Sheriff J, Apon D, Cooper D, Dang Q, Liu YK, et al.. Status report on the first round of the ... - TSAPPS at NIST. NIST; 2019. Available from: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303.

[8] Fernandez-Carames TM, Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE access. 2020;8:21091-116.

[9] Backendal M, Bellare M, Sorrell J, Sun J. The Fiat-Shamir Zoo: Relating the Security of Different Signature Variants. In: Gruschka N, editor. Secure IT Systems. Cham: Springer International Publishing; 2018. p. 154-70.

[10] Derler D, Ramacher S, Slamanig D. Post-quantum zero-knowledge proofs for accumulators with applications to ring signatures from symmetric-key primitives. In: International Conference on Post-Quantum Cryptography. Springer; 2018. p. 419-40.

[11] Martín-Fernández F, Caballero-Gil P, Caballero-Gil C. Authentication Based

on Non-Interactive Zero-Knowledge Proofs for the Internet of Things. Sensors. 2016;16(1). Available from: https://www.mdpi.com/1424-8220/16/1/75.

[12] do Nascimento JC, Ramos RV. Quantum protocols for Zero-knowledge systems - quantum information processing. Springer US; 2009. Available from: https://link.springer.com/article/10.1007/s11128-009-0127-8.

[13] Kim Y, Song J, Youn TY, Seo SC. Crystals-dilithium on armv8. Hindawi; 2022. Available from: https://www.hindawi.com/journals/scn/2022/5226390/.

[14] Deeprajnbsp;Soni, Kanadnbsp;Basu, Mohammednbsp;Nabeel, Najwanbsp;Aaraj, Marcosnbsp;Manzano, Rameshnbsp;Karri, et al.. Crystals-dilithium. Springer, Cham; 1970. Available from: https://link.springer.com/chapter/10.1007/978-3-030-57682-0_2.

[15] Morais E, Koens T, Van Wijk C, Koren A. A survey on zero knowledge range proofs and applications. SN Applied Sciences. 2019;1(8):1-17.

[16] Das D. Fiat-Shamir with Aborts: From Identification Schemes to Linkable Ring Signatures. In: Batina L, Picek S, Mondal M, editors. Security, Privacy, and Applied Cryptography Engineering. Cham: Springer International Publishing; 2020. p. 167-87.

[17] Sergent P, Richez B, Krempa A, Benoist S, Shah J. Trend Analyzing Algorithm designed alongside "A Survey of Zero-Knowledge Proofs in a Post-Quantum Context";.