

Program

Workshop on Quantum-Resistant Cryptography (QuRCry)

Proceedings (ProceedingsQuRCry.pdf)

Sunday, May 4

Facultad de Ciencias Matemáticas, Universidad Complutense de Madrid

- **9:00- 10:30 Keynote Presentation: Jintai Ding. Conquer the SVP 200 challenge**
- 10:30-11:00 *Coffee Break*
- 11:00-11:15 Jorge Munilla and An Braeken. Protecting against a semi-trusted third party with Hybrid Crypto
- 11:15-11:30 Christoph Striecks and Ludovic Perret. The Hybrid State-of-Play: How to Securely Combine Quantum and Classical Key Establishment Technologies
- 11:30-11:45 Édgar Pérez-Ramos, Omar Suárez-Doro, Candelaria Hernández-Goya and Pino Caballero-Gil. Leveraging kleptography to strengthen post-quantum cryptography
- 11:45-12:00 Robin Frot and Daniel Zentai. Solving LWE search from a dual attack equivalent
- 12:00-12:15 Mila Anastasova and Panos Kampanakis. The impact of MLWE on Web User Experience and mTLS Applications
- 12:15-12:30 Rodrigo Martín, Iván Blanco-Chacón and Raúl Durán. Extension of root-based attacks against PLWE instances
- 12:30-12:45 Alba Hernández Costoya, Alba Larraya Sancho and Miguel Ángel Marco Buzunáriz. CCA-attacks on lattice-based encryption-decryption schemes
- 12:45-13:00 Marcos Rodríguez-Vega and Pino Caballero-Gil. Exploring Non-Linear Activation Function Approximations in Fully Homomorphic Encryption
- 13:00-14:15 *Lunch*
- **14:15-15:15 Panel: Sofia Celi, Paco Martin-Fernandez, Eduardo Sáenz de Cabezón, and Pino Caballero-Gil (Moderator). Convergence of Quantum and Post-Quantum Cryptography**

- 15:15-15:45 *Coffee Break*
- 15:45-16:00 Daniel Escanez-Exposito, Pino Caballero-Gil, Eduardo Sáenz-de-Cabezón and Pablo Munarriz-Senosiain. A Zero-Knowledge Proof based on shellability of simplicial complexes
- 16:00-16:15 Jorge Garcia-Diaz, Daniel Escanez-Exposito, Pino Caballero-Gil and Jezabel Molina-Gil. BB84-Inspired Quantum Zero-Knowledge Proof for User Authentication over Quantum Channel
- 16:15-16:30 Sergejs Kozlovics, Elina Kalnina, Juris Viksna, Krisjanis Petrucena and Edgars Rencis. The Butterfly Protocol: QKD as a Service Without the "Weakest Link" Vulnerability
- 16:30-16:45 Daniel Escanez-Exposito and Pino Caballero-Gil. Entanglement-Based QKD Proposal Without Sharing Measurement Bases
- 16:45-17:00 Mariano Caruso, Daniel Escanez-Exposito, Pino Caballero-Gil and Carlos Kuchkovsky. Confidential QUBO solver
- 17:00-17:15 Julen Bernabé-Rodríguez, Iñaki Seco-Aguirre, Cristina Regueiro and Oscar Lage. On a Quantum Search for Short Vectors in Lattices using QRISP



Binter

Protecting against a semi-trusted third party with Hybrid Crypto

Jorge Munilla¹[0000–0003–2795–312X] and An Braeken²[0000–0002–9965–915X]

¹ Universidad de Málaga, ETSI de Telecomunicación, Málaga, 29071, Spain
jmf@uma.es

² Vrije Universiteit Brussel, INDI, Pleinlaan 2, Brussel, 1050, BE, Belgium
an.braeken@vub.be

Abstract. Hybrid protocols that combine Post-Quantum (PQ) and traditional primitives, allowing flexible switching based on the threat level, provide optimal trade-offs between efficiency and security. A recent scheme introduced a basic framework for this setup, but it fails to provide security against impersonation attacks by a semi-trusted TTP in some of its proposed modes. This vulnerability arises due to the asymmetric behavior of PQ primitives compared to traditional public-key primitives. We identify this threat and propose a solution that maintains the framework’s flexibility while ensuring security.

Keywords: Post-quantum security · Hybrid · ML-DSA · ML-KEM.

1 Extended Abstract

Post-Quantum (PQ) cryptography will be essential for protecting communications in the future when quantum computers become powerful enough to break current cryptosystems, particularly public-key cryptosystems such as Elliptic Curve Cryptography (ECC) and RSA [4, 6]. PQ primitives, however, come at a high communication and computational cost and may not be immediately necessary for applications with short-term security needs. Thus, until PQ computing arrives, hybrid security has been proposed as a means to provide more efficient solutions during this uncertain period, in which there exists a possibility of breaking either classical public-key cryptosystems or the newly designed post-quantum schemes [7]. These hybrid schemes combine contemporary public-key mechanisms and PQ algorithms, allowing flexible switching based on the threat level. The rationale behind this is to retain the time-tested trust in pre-quantum schemes while facilitating a smoother transition toward a PQ world [3].

Recently, a prominent hybrid-based and multifactor authentication and key agreement (AKA) framework has been proposed for IoT-based scenarios [2]. In this framework, the authentication and computation of the session key rely on both classical ECC and a quantum-secure key encapsulation mechanism (KEM) [1]. The system architecture consists of multiple users (U), a general-purpose IoT device (D), and a trusted third party (TTP). Particularly designed for IoT, the framework provides a high level of flexibility with five different derived versions, ranging from fully hybrid and partially hybrid to a purely classical construction, depending on whether ECC and/or KEM are used in registration and/or AKA

phases. The framework is also highly ambitious in its assumed threat model, offering, in addition to the standard security features, protection against an active semi-trusted third party. This TTP is assumed to perform the required security steps during registration, but is also considered curious, meaning it may attempt to derive the session key in order to access shared data for its own purpose and impersonate (active) one of the parties to the other.

The design of the protocol aims to enable the parallel use of the ECC and KEM primitives to provide symmetrical protection in both the classical and PQ worlds. However, in this paper, we show that the differing behavior of these primitives creates an asymmetry in the security, leading to a vulnerability in both the full PQ version (version 4) and the version (version 3) where PQ is used in registration and ECC in AKA, assuming ECC is compromised. To overcome this problem while preserving its excellent flexibility, security characteristics and two-phase communication structure, this paper proposes a modification to the protocol by introducing a PQ digital signature scheme (ML-DSA [5]) in U's registration and D's verification in the AKA (see Fig. 1). More specifically, in the original version, the adversarial TTP can impersonate a user, identified as Q_u , by generating a new key K_{i2} and computing new values r_i^* which D will accept as if they were sent by Q_u . The modified protocol prevents this attack by requiring U to sign K_{i2} during the registration.

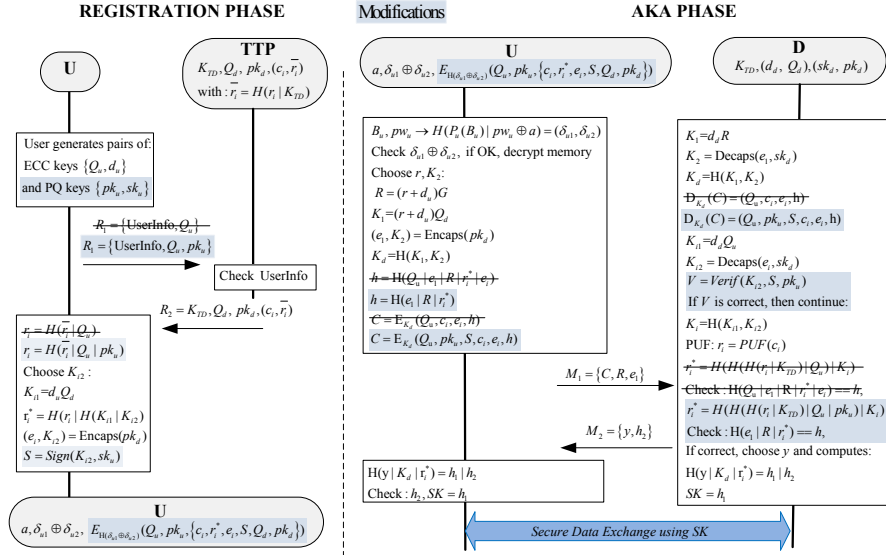


Fig. 1. Registration and AKA phases of the proposed protocol to achieve PQ security against semi-trusted TTPs. Modifications from the original protocol are highlighted on a solid background.

Acknowledgments. This work was possible thanks to the PID2022-138933OB-I00 ATQUE research project, and to the C065/23 Cybersecurity Chair of the University of La Laguna and INCIBE, funded by MCIN/AEI/10.13039/501100011033, and the Recovery, Transformation, and Resilience Plan (Next Generation), financed by the European Union.

References

1. Bos, J.W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS - kyber: A cca-secure module-lattice-based KEM. In: 2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, London, United Kingdom, April 24-26, 2018. pp. 353–367. IEEE (2018). <https://doi.org/10.1109/EuroSP.2018.00032>, <https://doi.org/10.1109/EuroSP.2018.00032>
2. Braeken, A.: Flexible hybrid post-quantum bidirectional multi-factor authentication and key agreement framework using ecc and kem. Future Generation Computer Systems (2025). <https://doi.org/10.1016/j.future.2025.01.012>
3. Giron, A.A., Custódio, R., Rodríguez-Henríquez, F.: Post-quantum hybrid key exchange: A systematic mapping study. Journal of Cryptographic Engineering **13**(1), 71–88 (2023). <https://doi.org/10.1007/s13389-022-00288-9>, <https://link.springer.com/article/10.1007/s13389-022-00288-9>
4. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96). pp. 212–219. ACM (1996). <https://doi.org/10.1145/237814.237866>, <https://arxiv.org/abs/quant-ph/9605043>
5. National Institute of Standards and Technology: Module-Lattice-Based Digital Signature Standard. Tech. Rep. FIPS 204, National Institute of Standards and Technology (Aug 2024), <https://doi.org/10.6028/NIST.FIPS.204>
6. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing **26**(5), 1484–1509 (1997). <https://doi.org/10.1137/S0097539795293172>, <https://arxiv.org/abs/quant-ph/9508027>
7. Stadler, S., Sakaguti, V., Kaur, H., Fehlhäber, A.L.: Hybrid signal protocol for post-quantum email encryption. Cryptology ePrint Archive, Paper 2021/875 (2021), <https://eprint.iacr.org/2021/875>

The Hybrid State-of-Play: How to Securely Combine Quantum and Classical Key Establishment Technologies

Christoph Striecks¹[0000–0003–4724–8022] and Ludovic Perret²

¹ AIT Austrian Institute of Technology, Vienna, Austria

`Christoph.Striecks@ait.ac.at`

<https://christophstriecks.com>

² EPITA, LRE, Le Kremlin-Bicêtre France

`Ludovic.Perret@epita.fr`

Abstract. Hybrid Authenticated Key Establishment (HAKE) use conventional, post-quantum, and quantum-based key material to establish an authenticated and confidential channel even in the event of cryptographically relevant quantum computers. Notably, such mechanisms can be fault-tolerant and versatile, meaning that even if all-but-one of the components fail or are turned off, the channel is still authenticate and confidential resulting in several options for a quantum-secure combination of key establishment technologies adjustable to specific use cases. Hybrid approaches are particularly motivated by a recent regulation and a roadmap in Europe. Concretely, in March 2023, the European Parliament and the Council published Regulation (EU) 2023/588 "Establishing the Union Secure Connectivity Programme for the period 2023-2027," which specifically mentions that a so-called hybrid approach combining conventional cryptographic solutions, PQC and possible Quantum Key Distribution (QKD) should be followed.³ Moreover, in April 2024, the European Commission published the Commission Recommendation (EU) 2024/1101 on a Coordinated Implementation Roadmap for the transition to PQC where hybrid approaches combining conventional cryptography with PQC or QKD were echoed.⁴ This talk will shed light on recent developments around such versatile hybrid approaches from the following angles:

- Motivation of authenticated hybrid key establishment in the transition to quantum-safe networks via (European) policies,
- Latest development in HAKE protocols covering Muckle, Muckle+, Muckle# (including recent works by the authors) achieving the important guarantees of forward and post-compromise security,
- Implementation and standardization efforts in terms of authenticated hybrid key establishment,
- Outlook and future works.

Keywords: Post-Quantum Cryptography · Quantum Cryptography · Hybrid Key Exchange · Forward Security · Post-Compromise Security.

³ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R0588>

⁴ https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401101

A boom in Post-Quantum Cryptography (PQC) standardization is currently ongoing. Besides NIST, basic PQC primitives are going to be standardized at ISO and will yield international post-quantum standards. Moreover, we see standardization efforts at IETF, ETSI's Quantum-Safe Cryptography group, and more to integrate those primitives into security protocols. Moreover, NCCoE/NIST is developing practical recommendations for migrating to PQC.

In addition, a new approach, so called Hybrid Authenticated Key Exchange (HAKE), for combining or hybridising Quantum Cryptography (QC⁵), PQC and conventional cryptography has recently been proposed [3–5], exploiting the features of all those approaches in one protocol following a versatile defence-in-depth paradigm. In such a combined setting, QC, PQC and conventional keys can be mixed to be used for secure communication while achieving quantum-safe authentication of the participants as well. The result is strong end-to-end forward and post-compromise security guarantees for quantum-safe networks.

By carefully designing the protocol, hybrid approaches reduce the all-or-nothing transition risk to quantum-safe networks allowing a versatile combination of quantum-safe technologies. For example, a combination of strongly secure QC confidentiality with PQC signatures results in a key establishment with security guarantees which were not possible with solely PQC or QC. Noteworthy, standards on QC/PQC hybridising are currently absent. The challenge lies not only in designing a functional protocol but also in providing security guarantees supported by formal proofs.

The talk will present recent developments in the area and will highlight the need for quantum-safe authenticated hybrid key exchanges in future quantum-safe networks, in particular:

(1) Present the recent developments in quantum-safe HAKE. Usually, it is not trivial to combine the mentioned technologies in one protocol (e.g., via key combiners which do not achieve authenticity straightforwardly). Consequently, modern HAKE protocols follow along the line of the Transport-Layer-Security (TLS) protocol to achieve forward and post-compromise security, confidentiality, authenticity, and integrity [3–5]. Moreover, available HAKE protocols have guarantees in terms of security proofs (under well-established assumptions such the availability of post-quantum KEMs and signatures) which is a de-facto standard nowadays for the design of novel security protocols.

(2) Raise awareness of hybrid techniques in near-term quantum-safe infrastructures such as the European Quantum Communication Infrastructure [6]. This is mainly driven by the European regulation and roadmap [1, 2]. The presentation highlights those documents as motivation for using HAKE in future quantum-safe protocols.

Acknowledgments. This work received funding from the European Union's Horizon Europe research and innovation programme under agreement number 101114043 ("QSNP"); the Digital Europe Program under grant agreement number 101091642 ("QCI-CAT"). The authors acknowledge support of the Institut Henri Poincaré (UAR 839 CNRS-Sorbonne Université) and LabEx CARMIN (ANR-10-LABX-59-01).

⁵ Most prominently instance thereof is often called Quantum Key Distribution (QKD).

References

1. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R0588>
2. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401101
3. Benjamin Dowling, Torben Brandt Hansen, and Kenneth G. Paterson. Many a Mickle Makes a Muckle: A Framework for Provably Quantum-Secure Hybrid Key Exchange. PQCrypto 2020.
4. Sonja Bruckner, Sebastian Ramacher, Christoph Striecks. Muckle+: End-to-End Hybrid Authenticated Key Exchanges. PQCrypto 2023.
5. Christopher Battarbee, Christoph Striecks, Ludovic Perret, Sebastian Ramacher, Kevin Verhaeghe. Quantum-Safe Hybrid Key Exchanges with KEM-Based Authentication. ArXiv 2024.
6. <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>

Leveraging kleptography to strengthen post-quantum cryptography

Édgar Pérez-Ramos^[0009–0008–0409–3079],
Omar Suárez-Doro^[0009–0000–7136–2170],
Candelaria Hernández-Goya^[0000–0002–9468–708X], and
Pino Caballero-Gil^[0000–0002–0859–5876]

University of La Laguna, Tenerife, Spain
{eperezra, alu0101483474, mchgoya, pcaballe}@ull.edu.es

Extended Abstract

A cryptographic backdoor is a covert mechanism embedded in a cryptographic system, often based on asymmetric cryptography, aiming to extract secret information, such as private keys, without the legitimate user’s awareness.

Kleptography was introduced by Adam Young and Moti Yung in 1997 in [1]. In that work, they defined a class of cryptographic backdoors called SETUP (Secretly Embedded Trapdoor with Universal Protection), which can be inserted into an asymmetric cryptosystem to covertly leak secret information through its output such that it remains secure against those who do not possess the trapdoor because only the attacker can exploit it. Also in that paper, the concept of Covert Key Exchange was introduced to refer to a cryptographic technique that allows an attacker to secretly derive a shared key while the legitimate parties appear to engage in a normal key exchange protocol. Kleptographic attacks began to generate increasing concern after 2010, when the same authors published [2], formalizing kleptographic backdoors from standard assumptions and making the concept more concrete and practical.

Attention to backdoors, and in particular for post-quantum algorithms, has been increasing since 2022 due to the NIST post-quantum cryptography standardization process. The first documented backdoor targeting post-quantum cryptography appeared in [3], focusing on the NTRU encryption scheme [4]. However, later research in [5] revealed that this backdoor was detectable. Despite that, the proposal played a crucial role in the beginning of the study of KEMs (Key Encapsulation Mechanisms) with embedded backdoors. The initial construction received several corrective measures in [6]. Independently, [7] and [8] introduced their own backdoor constructions for PKE (Public-Key Encryption) schemes based on the LWE (Learning With Errors) problem [9]. Recently, in 2024, [10] proposed three backdoor attacks on the Fujisaki-Okamoto transform [11], targeting KEMs with implicit rejection. The most recent research on backdoors in KEMs was presented in [12], which explores the insertion of backdoors into CRYSTALS-Kyber [13] and Classic McEliece [14]. Those works introduce the concepts of public and strict indistinguishability, aiming to formalize how backdoors can remain undetectable.

The present work extends and refines the findings of [15], which introduced the first practical backdoor installation in the CRYSTALS-Kyber KEM. In that study, the backdoor was embedded during the key generation phase by leveraging the LWE properties in CRYSTALS-Kyber. The author proposed two distinct types of backdoors: A classical backdoor using an elliptic curve scheme and a post-quantum backdoor. In this context, CRYSTALS-Kyber KEM was considered for encapsulation and decapsulation, while Classic McEliece in its version `mceliece460896` [16] was used for encrypting and decrypting texts.

In contrast to that paper, this work proposes to extend the application of the backdoor to a wider range of algorithms. Furthermore, several improvements and refinements to the post-quantum backdoor are introduced here to improve its mathematical correctness and ensure more coherent algorithmic implementations. Thus, the key contributions of this study are:

1. Implementation of the backdoor using Kyber KEM for encapsulation and decapsulation, with Classic McEliece to encrypt the target text. The backdoor has been applied to: `mceliece348864`, `mceliece460896`, `mceliece6960119`, `mceliece6688128`, and `mceliece8192182`.
2. Alternative implementation using the CRYSTALS-Kyber KEM for both encapsulation/decapsulation and CRYSTALS-Kyber for encryption. In this case, feasibility has been demonstrated for Kyber.CPAPKE.512 and polynomial matrix sizes where matrix sizes where $k = 3, 4$.
3. Proposal of an improved key recovery method, enabling a bijective mapping between the ciphertext polynomial and the user's altered public key.
4. Finally, it also proposed and corrected mathematical notation errors in the original article and provided a much more guided and didactic implementation.

Experimental results indicate that the most efficient backdoors are: Kyber512 + `mceliece468896`, Kyber768 + `mceliece468896` and Kyber512 + `mceliece348864`.

To detect potential backdoor attacks, the following approach is proposed. If a backdoor is suspected, the key generation phase should be carefully analysed, verifying compliance with the expected Kyber specification. Additionally, the execution time should be measured, as an anomalous delay (exceeding twice the average time, according to the performed experiments) could indicate the presence of a backdoor. In conclusion, this study enhances the understanding of the impact of kleptography on post-quantum cryptosystems, enabling anticipation and mitigation of major risks associated with cryptographic backdoors.

Acknowledgments.

This work was possible thanks to the projects: 2023DIG28 IACTA, PID2022-138933OB-I00 ATQUE, and SCITALA C064/23 ULL-INCIBE, and to the C065/23 Cybersecurity Chair of the University of La Laguna and INCIBE, funded by Cajacanarias la Caixa Foundations, MCIN/AEI/10.13039/501100011033, and the Recovery, Transformation, and Resilience Plan (Next Generation) financed by the European Union.

References

1. A. Young, M. Yung, “Kleptography: Using cryptography against cryptography”, *Advances in Cryptology—EUROCRYPT’97: International Conference on the Theory and Application of Cryptographic Techniques*, pp. 62–74, Springer, 1997.
2. A. Young, M. Yung, “Kleptography from Standard Assumptions and Applications” in *Security and Cryptography for Networks*, J. A. Garay and R. De Prisco, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 271–290, 2010.
3. R. Kwant, T. Lange, K. Thissen, “Lattice klepto: Turning post-quantum crypto against itself”, *International Conference on Selected Areas in Cryptography*, pp. 336–354, Springer, 2017.
4. A. Pellet-Mary, D. Stehlé, “On the hardness of the NTRU problem”, *Advances in Cryptology—ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part I* 27, pp. 3–35, Springer, 2021.
5. Z. Yang, T. Xie, Y. Pan, “Lattice klepto revisited”, *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, pp. 867–873, 2020.
6. T. Hemmert, A. May, J. Mittmann, C.R.T. Schneider, “How to Backdoor (Classic) McEliece and How to Guard Against Backdoors”, *International Conference on Post-Quantum Cryptography*, pp. 24–44, Springer, 2022.
7. D. Xiao, Y. Yu, “Klepto for ring-LWE encryption”, *The Computer Journal*, vol.61, no.8, pp. 1228–1239, Oxford University Press, 2018.
8. Z. Yang, R. Chen, C. Li, L. Qu, and G. Yang, “On the security of LWE cryptosystem against subversion attacks”, *The Computer Journal*, vol.63, no.4, pp. 495–507, Oxford University Press, 2020.
9. J. Ding, X. Xie, X. Lin, “A simple provably secure key exchange scheme based on the learning with errors problem”, *Cryptology ePrint Archive*, 2012.
10. A. Joux, J. Loss, B. Wagner, “Kleptographic Attacks against Implicit Rejection”, *Cryptology ePrint Archive*, 2024.
11. J. Lippert, J. Blömer, G. Domik, “The Fujisaki-Okamoto Transformation”, *University of Paderborn, The University of the Information Society, Faculty of Electrical Engineering, Computer Science and Mathematics*, 2014.
12. W. Xia, G. Wang, D. Gu, “Post-Quantum Backdoor for Kyber-KEM”, *Selected Areas in Cryptography*, vol. 2024, 2024.
13. R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, D. Stehlé, *CRYSTALS-Kyber: Algorithm Specifications And Supporting Documentation (version 3.02)*, 2021.
14. D.J. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, W. Wang, “Classic McEliece: conservative code-based cryptography. Project documentation”, 2017.
15. P. Ravi, S. Bhasin, A. Chattopadhyay, A. Aikata, S. Sinha Roy, “Backdooring post-quantum cryptography: Kleptographic attacks on lattice-based KEMs”, *Proceedings of the Great Lakes Symposium on VLSI 2024*, pp. 216–221, 2024.
16. D.J. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, otros, “Classic McEliece: Algorithm Specifications and Supporting Documentation”, 2022.

Solving LWE search from a dual attack equivalent

Robin Frot and Daniel Zentai

xtendr, Hungary

1 Introduction

The aim of this abstract is to provide a method to solve search LWE problems in a way similar to the dual attack for their decision counterpart. Our method requires a single lattice reduction analogous to the dual attack and only requires one additional linear algebra step.

Learning with Error The Learning With Error problem (LWE) (Definition 1) introduced by Regev [Reg09] is widely used in cryptography and especially in lattice cryptography like in FHE systems.

Definition 1 (RLWE). Let p be a prime number and $\mathcal{R}_p = \mathbb{Z}_p[X]/(X^n + 1)$ a cyclotomic ring, (χ_s, χ_e) a pair of distributions on \mathcal{R}_p . Define the RLWE distribution on \mathcal{R}_p^2 by pairs (a, b) such that $a \leftarrow \mathcal{U}$ and $b = a \cdot s + e$ with $s \leftarrow \chi_s$, $e \leftarrow \chi_e$ and \mathcal{U} the uniform distribution.

Decision problem: Given a random pair $(a, b) \in \mathcal{R}_p^2$, decide up to negligible probability if it has been generated by the LWE distribution or the uniform distribution on the product.

Search problem: Given a random pair $(a, b) \in \mathcal{R}_p^2$, find s if it has been generated by the LWE distribution.

The computational hardness of this problem has been studied extensively, giving rise to several classes of attacks (e.g. [AFG13], [Alb+17], [Alb+15], [Guo+19]).

In the following, we will assume that the distributions χ_s and χ_e are small: they are essentially Gaussian distributions centered at 0 with a standard deviation $\sigma = O(1)$.

The dual attack The dual lattice attack was introduced in [Alb17] and reduces the decision problem to the SIS problem. In order to solve decision LWE with short keys, it is enough to find a small vector in the lattice defined by the matrix

$$\begin{pmatrix} pI_n & A \\ & I_n \end{pmatrix}$$

where A is the embedding of a in $M_n(\mathbb{Z})$ and (a, b) is given by the instance or RLWE. Here the bases vectors are the columns.

Usual search to decision reduction The usual strategy for the search-to-decision reduction is to introduce a perturbation in the public key (a, b) in order to recover the secret s one coordinate at a time. In the case of small distributions, this requires $O(n)$ calls to a decision problem.

Our contribution In the rest of this paper we describe a method requiring a single lattice reduction identical to the one in the dual attack, which allows us to directly solve the search problem with only one instance of the reduction. The method makes use of the fact that short linear relations over $M_n(\mathbb{Z}_p)$ that are not independent may become independent after a lift to $M_n(\mathbb{Q})$. Therefore, by only finding two small vectors in the lattice reduction, it allows to solve search RLWE by solving a linear system.

2 Solving the search problem directly

Let us start by reducing the lattice given by the matrix

$$\begin{pmatrix} pI_n & A \\ 0_n & I_n \end{pmatrix}$$

as in the dual attack. We recover the two smallest vectors

$$\begin{pmatrix} v0 \\ \epsilon_0 \end{pmatrix}, \begin{pmatrix} v1 \\ \epsilon_1 \end{pmatrix}$$

where $\|v_i\|, \|\epsilon_i\| \ll p^{1-\eta}$. By lifting the problem to $\mathcal{R} := \mathbb{Q}[X]/(X^N + 1)$ we have

$$\tilde{b} = \tilde{a}\tilde{s} + \tilde{e} + qY \in \mathcal{R}$$

for some polynomial $Y \in \mathcal{R}$ and \tilde{X} being the lift with coefficients in $[-p/2, p/2[$. Since

$$v_i \tilde{b} \bmod p = (\epsilon_i s + v_i e) \bmod p.$$

and $ws + ve = O(p^{1-\delta})$, we have

$$v_i \tilde{b} = \epsilon_i s + v_i e \in \mathcal{R}.$$

This gives two independent relations in \mathcal{R} .

3 Experimental results

Here are some experimental results that are comparable to what is expected for the decision dual-attack. They have been conducted with $\log_2(p) = 30$ and $\sigma = 5$ with a LLL style algorithm provided by the Python flatter package.

$\log_2(N)$	secret key recovered	target rhf	effective rhf	wall time
6	<i>Yes</i>	1.073	1.0135	10.5s
7	<i>Yes</i>	1.036	1.0138	2min 9s
8	<i>Yes</i>	1.018	1.0144	15min 55s
9	<i>No</i>	1.0089	—	—

References

- [AFG13] Martin R. Albrecht, Robert Fitzpatrick, and Florian Göpfert. “On the Efficacy of Solving LWE by Reduction to Unique-SVP”. In: *Information Security and Cryptology - ICISC 2013 - 16th International Conference, Seoul, Korea, November 27-29, 2013, Revised Selected Papers*. Ed. by Hyang-Sook Lee and Dong-Guk Han. Vol. 8565. Lecture Notes in Computer Science. Springer, 2013, pp. 293–310. DOI: [10.1007/978-3-319-12160-4_18](https://doi.org/10.1007/978-3-319-12160-4_18). URL: https://doi.org/10.1007/978-3-319-12160-4%5C_18.
- [Alb+15] Martin R Albrecht et al. “On the complexity of the BKW algorithm on LWE”. In: *Designs, Codes and Cryptography* 74 (2015), pp. 325–354.
- [Alb+17] Martin R. Albrecht et al. “Revisiting the Expected Cost of Solving uSVP and Applications to LWE”. In: *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*. Ed. by Tsuyoshi Takagi and Thomas Peyrin. Vol. 10624. Lecture Notes in Computer Science. Springer, 2017, pp. 297–322. DOI: [10.1007/978-3-319-70694-8_11](https://doi.org/10.1007/978-3-319-70694-8_11). URL: https://doi.org/10.1007/978-3-319-70694-8%5C_11.
- [Alb17] Martin R Albrecht. “On dual lattice attacks against small-secret LWE and parameter choices in HELib and SEAL”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2017, pp. 103–129.
- [Guo+19] Qian Guo et al. “On the Asymptotics of Solving the LWE Problem Using Coded-BKW With Sieving”. In: *IEEE Trans. Inf. Theory* 65.8 (2019), pp. 5243–5259. DOI: [10.1109/TIT.2019.2906233](https://doi.org/10.1109/TIT.2019.2906233). URL: <https://doi.org/10.1109/TIT.2019.2906233>.
- [Reg09] Oded Regev. “On lattices, learning with errors, random linear codes, and cryptography”. In: *Journal of the ACM (JACM)* 56.6 (2009), pp. 1–40.

The impact of MLWE on Web User Experience and mTLS Applications

Mila Anastasova¹ and Panos Kampanakis¹

Amazon Web Services, USA
`{milaaws, kpanos}@amazon.com`

The integration of quantum-resistant, NIST-standardized ML-KEM and ML-DSA algorithms [1] in TLS connections will increase the handshake data transfer from server to client or vice versa by approximately 15KB. Studies [23456] have shown that the extra data may sometimes slow down the handshake by over 10%. That can potentially affect applications, especially in slow networks. This talk investigates the actual impact of these data-heavy handshakes on web user experience and applications using mTLS.

Web User Experience Impact

Although ML-DSA will affect TLS handshakes, given that most web connections involve much larger data transfers, an additional 15KB may not significantly impact user experience. In this talk, we provide a quantitative analysis of Web Performance Metrics of popular web pages and their relation to the TLS handshake. The metrics we focus on are related to Core Web Vitals [7] and include Time-to-First-Byte (TTFB), First Contentful Paint (FCP), Last Contentful Paint (LCP), and Document Complete (DC) times, which are directly related to user experience. We also look into the data sizes transferred by various popular web pages. By examining the web metrics and the data transfer sizes, we showcase that the additional 15KB in the handshake is likely to have a minimal effect on the overall user experience since that is dominated by transferring and rendering the web content and not by the initial TLS handshake.

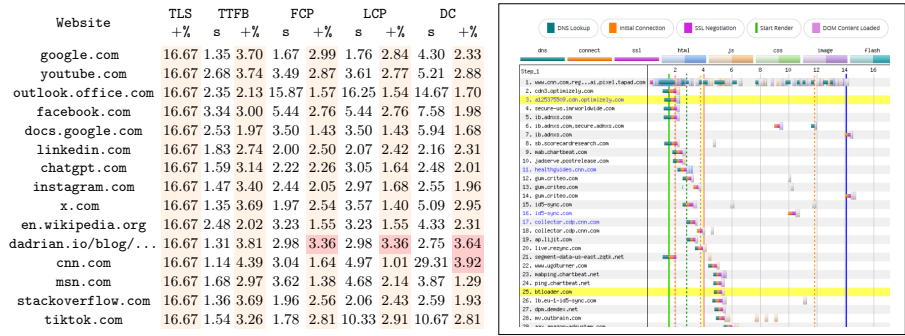


Fig.1: **Left:** Web Metric Slowdowns due to "trimmed" (10KB) ML-DSA authentication; **Right:** Parallel TLS connections when browsing to `cnn.com` (from `webpagetest.org`).

We also demonstrate how web page design, which includes multiple parallel connections, can minimize the slowdown. Additionally, our work exposes some intricacies of how web content is downloaded or uploaded, which includes slim connections that transfer non-rendered data. While ML-DSA does introduce communication overhead, we conclude that using simple techniques to trim the authentication data during the handshake can make the impact practically unnoticeable to web users ($< 2\%$). Figure 1 shows the estimated impact of ML-DSA authentication in a typical 3G scenario (1.6Mbps download, 768kbps upload, 300ms round-trip) on the TTFB, FCP, LCP, and DC times. It also breaks down the browser connections, transferring content from `cnn.com`, to show that the news organization’s website is served by multiple destinations over many parallelized connections, which will not have an additive impact on web user metrics.

mTLS Impact

In spite of multiple experiments on the impact of ML-KEM and ML-DSA on TLS 1.3 [28345], to our knowledge, there have been no studies on mTLS. This scenario is particularly relevant in Zero Trust Architecture (ZTA) and Machine-to-Machine communications. Our work explores the performance impact of ML-KEM and ML-DSA over the Time-To-First-Byte (TTFB) and Time-To-Last-Byte (TTLB) of mTLS connections, while transferring application data. The TTLB reflects the application performance impact by following the rationale in [4]. Our experiments involve different network conditions such as Round-Trip Time (RTT), connection speed, initial TCP congestion window ($icwnd$), and amount of transferred data. We demonstrate that MLWE algorithms will impact mTLS handshakes more than plain TLS, but for applications that transfer sizeable amounts of data, the impact will be acceptable. We also show that tweaking the network parameters ($icwnd$) and trimming the authentication data can improve application performance. Figure 2 illustrates 49.7% and 82.6% slower mTLS handshakes with an $icwnd = 10$ at $100Mbps$ and $1Mbps$, respectively. It also shows a 2.08%, 1.42%, and 1.25% slowdown of the mTLS TTLB when setting the $icwnd = 24$ for 0KB, 50KB, and 150KB of data transfer at 100Mbps.

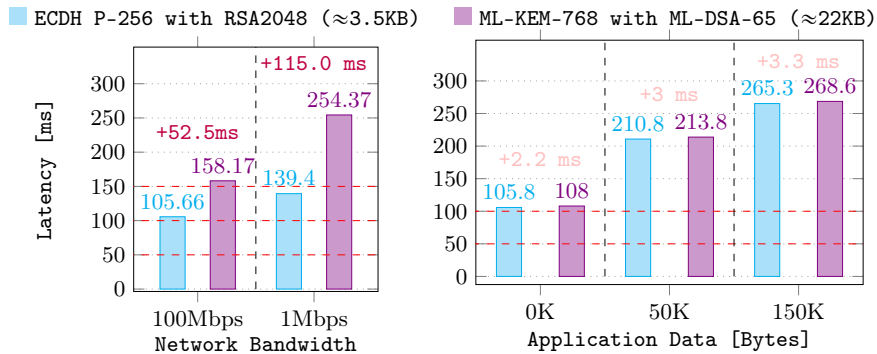


Fig. 2: 50ms RTT , **Left**: Handshake Time ($icwnd = 10$); **Right**: TTLB ($icwnd = 24$, @100Mbps)

References

1. NIST. NIST PQ project. <https://csrc.nist.gov/projects/post-quantum-cryptography>, August 2016.
2. Christian Paquin, Douglas Stebila, and Goutam Tamvada. Benchmarking post-quantum cryptography in TLS. In *Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings 11*, pages 72–91. Springer, 2020.
3. Dimitrios Sikeridis, Panos Kampanakis, and Michael Devetsikiotis. Post-quantum authentication in TLS 1.3: A performance study. In *27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23–26, 2020*. The Internet Society, 2020.
4. Panos Kampanakis and Will Childs-Klein. The impact of data-heavy, post-quantum TLS 1.3 on the Time-To-Last-Byte of real-world connections, 2024.
5. George Tasopoulos, Jinhui Li, Apostolos P Fournaris, Raymond K Zhao, Amin Sakzad, and Ron Steinfeld. Performance evaluation of post-quantum TLS 1.3 on resource-constrained embedded systems. In *International Conference on Information Security Practice and Experience*, pages 432–451. Springer, 2022.
6. Bas Westerbaan. Sizing Up Post-Quantum Signatures. <https://blog.cloudflare.com/sizing-up-post-quantum-signatures/>, November 2021.
7. Google LLC. Understanding Core Web Vitals and Google search results. <https://developers.google.com/search/docs/appearance/core-web-vitals>.
8. Kris Kwiatkowski. Towards Post-Quantum Cryptography in TLS, June 2019.

Extension of root-based attacks against PLWE instances

Iván Blanco Chacón¹[0000–0002–4666–019X], Raúl Durán
Díaz²[0000–0001–6217–4768], and
Rodrigo Martín Sánchez-Ledesma^{3,4}[0009–0001–1845–2959]

¹ Departamento de Física y Matemáticas, Universidad de Alcalá, Spain
`ivan.blancoc@uah.es`

² Departamento de Automática, Universidad de Alcalá, Spain
`rduran@uah.es`

³ Departamento de Álgebra, Universidad Complutense de Madrid, Spain
`rodrma01@ucm.es`

⁴ Indra Sistemas de Comunicaciones Seguras, Spain
`rmsanchezledesma@indra.es`

1 Extended abstract

Lattice-based cryptography is, as of today, one of the most important mathematical families regarding Post-Quantum Cryptography. A vast number of the quantum-resistant cryptographic schemes developed in the last decade base their security upon some paradigm of this family.

While a variety of constructions exists within this family, probably the more relevant distinction remains the one between *unstructured* and *structured* lattices. In other words, whether the construction employed makes use of any additional algebraic structure to achieve more efficient and compact schemes.

Within lattice-based cryptography one paradigm has gained more traction than the rest, due to its inherent simplicity and understanding: the *Learning With Error* paradigm and its structured variants, including the *Polynomial Learning With Errors* (PLWE).

Let q be a prime and let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree N . Let $R_q := \mathbb{F}_q[x]/(f(x))$ and choose an element $s(x) \in R_q$. A PLWE sample is a pair $(a(x), b(x)) \in R_q^2$ where $a(x)$ is chosen uniformly at random and $b(x) = a(x)s(x) + e(x)$ with the coefficients of $e(x)$ chosen from an R_q -valued random variable of mean 0 and small variance, typically the outcome of discretizing and reducing modulo q the samplings of a centered Gaussian distribution.

The set of all possible PLWE samples is referred to as the PLWE distribution and the PLWE problem, in its search version, consists in guessing, with non-negligible advantage, the element $s(x)$ from arbitrarily many samples of the PLWE distribution, while its decision version amounts to be able to distinguish PLWE samples from Uniform ones.

This problem is behind a good number of proposals presented to the NIST competition for standardization of quantum resistant primitives. Furthermore,

it is the foundation behind two out of the four first NIST PQC standards chosen in July 2022 for KEM and DSA. The PLWE problem as well as its germane problem Ring Learning With Errors (RLWE) presents a clear advantage over the Learning With Errors (LWE): the length of the keys necessary to grant (under certain hardness assumptions) the same level of security is essentially linear in N .

The presence of this additional structure, while beneficial to the practical deployability of the scheme, raises the question as to if/how it might increase the surface of attacks against them. As such, numerous works have been focused on providing answers to these questions. Among them, the approach defined in [1] and [2] is highlighted.

In them, the authors provide a set of algorithms to break PLWE in its decisional version, if there exists a root α of $f(x)$ in \mathbb{F}_q which has small enough order. From these conditions, a number of different attacks are constructed, based upon a variety of distinct distinguishing conditions:

The first attack is constructed upon the smallness of cardinal of the set of possibilities for the associated error values, under evaluation over the root α .

The second attack is constructed upon the smallness of the associated error values, when the resulting Gaussian distribution is enclosed in a certain sub-interval of \mathbb{F}_q .

The third attack follows upon the setting of the previous attack, without the need for the restriction over the image Gaussian.

In [3], the authors extend the first attack above to the case where $f(x)$ has a root over a quadratic extension of \mathbb{F}_q of suitable trace.

The present work extends all previous results in two fronts: first, following upon the trace setting, all the attacks are proven to be accept a generalization to an arbitrary degree extension of \mathbb{F}_q beyond quadratic. This means that no restriction is placed on the finite field extension in which the polynomial $f(x)$ has roots and, thus it allows the generalize the setting in which every attack can be applied.

Furthermore, this work also addresses some of the initial restrictions placed in [1–3] that result in an increased difficulty towards real-life applicability: mostly, the initial condition imposed on the Gaussian distribution of the PLWE problem to be bounded by 2σ , where σ^2 represents the variance of the distribution.

The use of finite field traces for the cryptanalysis of lattice-based primitives is not entirely new (see for instance [4] and [5]). However, to the best of our knowledge, the use we make of the traces of the roots of $f(x)$ is indeed new and the present contribution extends to a more general scenario the methods introduced in [3].

References

1. Y. ELIAS, K. E. LAUTER, E. OZMAN, AND K. E. STANGE, *Provably Weak Instances of Ring-LWE*, in Advances in Cryptology – CRYPTO 2015, R. Gennaro and M. Robshaw, eds., no. 9215 in Lecture Notes in Computer Science, Berlin, Heidelberg, 2015, Springer Berlin Heidelberg, pp. 63–92.

2. ———, *Ring-LWE Cryptography for the Number Theorist*, in Directions in Number Theory, E. E. Eischen, L. Long, R. Pries, and K. E. Stange, eds., vol. 3 of Association for Women in Mathematics Series, Cham, 2016, Springer International Publishing, pp. 271–290.
3. I. BLANCO-CHACÓN, R. DURÁN-DÍAZ, R. Y. NJAH NCHIWO, AND B. BARBERO-LUCAS, *Cryptanalysis of PLWE based on zero-trace quadratic roots*, submitted.
4. C. PEIKERT, *How (Not) to Instantiate Ring-LWE*, in Security and Cryptography for Networks, V. Zikas and R. De Prisco, eds., vol. 9841 of Lecture Notes in Computer Science, Springer International Publishing, 2016, pp. 411–430.
5. C. PEIKERT AND Z. PEPIN, *Algebraically Structured LWE, Revisited*. Cryptology ePrint Archive, Report 2019/878, 2019. <https://ia.cr/2019/878>.
6. H. CHEN, K. LAUTER, AND K. E. STANGE, *Attacks on the Search RLWE Problem with Small Errors*, SIAM Journal on Applied Algebra and Geometry, 1 (2017), pp. 665–682.
7. V. LYUBASHEVSKY, C. PEIKERT, AND O. REGEV, *On Ideal Lattices and Learning with Errors over Rings*, Journal of the ACM, 60 (2013), pp. 43:1–43:35.
8. M. ROSCA, D. STEHLÉ, AND A. WALLET, *On the Ring-LWE and Polynomial-LWE Problems*, in Advances in Cryptology – EUROCRYPT 2018, J. B. Nielsen and V. Rijmen, eds., Cham, 2018, Springer International Publishing, pp. 146–173.
9. K. E. STANGE, *Algebraic Aspects of Solving Ring-LWE, Including Ring-Based Improvements in the Blum–Kalai–Wasserman Algorithm*, SIAM Journal on Applied Algebra and Geometry, 5 (2021), pp. 366–387.

CCA-attacks on lattice-based encryption-decryption schemes

Alba Hernández Costoya¹, Alba Larraya Sancho^{1,2}, and Miguel Ángel Marco Buzunáriz³[0000–0002–6750–8971]

¹ Universidad del País Vasco, Bilbao, Spain

² Basque Center for Applied Mathematics, Bilbao, Spain

³ Universidad de Zaragoza, Zaragoza, Spain

1 Introduction

Kyber [6] is composed by a CPA-secure PKE, which is transformed into a CCA-secure KEM with the Fujisaki-Okamoto transform. The security of Kyber is based on the Module-LWE problem, although the security is only guaranteed for single use public keys, and not when we reuse it. In this paper we present a CCA-attack against the CPA-secure PK, this is, we assume that the secret key is being reused and that we have a Decryption Oracle. We will also present a comparative between our attack and the Key Mismatch attack against lattice KEMs presented in works as [5] [3] [4].

Other kinds of attacks have also been studied for LWE-based schemes. In [2], they propose a CPA^D attack against fully homomorphic encryption schemes, based on the LWE encryption scheme. For this attack, the attacker is allowed to demand the oracle to perform encryption, decryption and evaluation of plaintexts and ciphertexts. We present two different CCA attacks against fully homomorphic encryption schemes based on the LWE problem, and we also present a comparison between the results in [2] and one of our attacks adapted to the specific encryption scheme they attack.

2 CCA-attack against Kyber

In order to attack CRYSTALS-Kyber, we will use the following oracle

Definición 1. Let q, t, n be the scheme parameters. Given a secret key $\mathbf{s} \in R_q^k$, we define the CCA-oracle for Crystals-KYBER KEM as a function that takes as input $\mathbf{u} \in R_q^k$ and $v \in R_q$, and returns the result of the decipher operation:

$$\mathcal{O}_{q,d_u,d_v,n}^{CCA-Kyb}(\mathbf{u}, v) = \text{Compress}_q(\text{Decompress}_q(v, d_v) - \mathbf{s} \cdot \text{Decompress}_q(\mathbf{u}, d_u), 1) \quad (1)$$

In order to perform the attack, we will get each of the components of \mathbf{s} separately. To get \mathbf{s}_j , the j -th component of \mathbf{s} , we will send the pair $(\text{Compress}_q(\lfloor \frac{q}{8} \rfloor, d_u), v)$ where by $\text{Compress}_q(\lfloor \frac{q}{8} \rfloor, d_u)$ we denote the vector with all components equal to 0, and the j -th component is the constant polynomial $\text{Compress}_q(\lfloor \frac{q}{8} \rfloor, d_u)$; and v is a polynomial we will change for each query.

3 CCA-attacks against FHE

The oracle we use to attack a FHE scheme will depend on the specific decryption function of the scheme.

The first attack consists on bisecting the interval in which we know the secret key is located. This attack takes advantage of the parity of the secret key, which changes when we add or subtract enough such that $s_j \pm v$ exits the interval $[-\frac{q-1}{2}, \frac{q-1}{2}]$. For this attack, we take the big modulus q and the small modulus t to be coprime. Then, we will query to the oracle pairs of the form (\mathbf{e}_j, v) , where \mathbf{e}_j is the j -th canonical basis vector, and v is a constant that allows us to divide the interval in half.

The second attack is based on the following lemma:

Lemma 1. *Fix j , and suppose that, for private keys s_1 and s_2 , the oracle returns the same answers for the queries $\{(t^k \cdot \mathbf{e}_j, 0) | k = 1, \dots, \lceil \log_t q \rceil\}$, then the j 'th entries of s_1 and s_2 coincide.*

In this case, we will query the oracle pairs $(t^k \mathbf{e}_j, 0)$ and then compute the oracle's operation for all the possible values s_j can take and keep only those for which the solution coincides with the oracle's output.

4 Comparatives and Conclusions

After simulating the attacks and the oracles in SageMath[1], we were able to recover successfully 1000 secret keys. The results obtained, with the average number of queries per key are presented in the following tables:

Table 1. Comparison between the Key Mismatch attack and the CCA-attack against Kyber

	Key Mismatch theoretical queries	Key Mismatch experimental queries	CCA-attack theoretical queries	CCA-attack experimental queries
Kyber512	1312	1311	6	6
Kyber768	1774	1777	9	9
Kyber1024	2365	2368	12	12

Table 2. Comparison between the CPA^D attack and the CCA-attack against FHE

n	q	CPA^D			CCA-attack		
		Encryption queries	Evaluation queries	Decryption queries	Encryption queries	Evaluation queries	Decryption queries
8192	2^{240}	14593	6512218	6512218	0	0	1966080
16384	2^{240}	29016	12924174	12924174	0	0	3932160

Our attacks showcases the importance of not exposing the decryption function to a potential adversary in the used implementations. In particular, implementations of Crystals-Kyber in devices such as smartcards or Yubikeys should make sure that their interface does not expose the decryption function, since it would make them vulnerable to exfiltration of the secret keys.

References

1. Alba Hernandez Costoya, Alba Larraya Sancho, M.A.M.d.B.: Cca-kyber-attack. <https://github.com/Alarraya/CCA-Kyber-attack> (2025)
2. Checri, M., Sirdey, R., Boudguiga, A., Bultel, J.P.: On the practical cpad security of “exact” and threshold fhe schemes and libraries. In: Annual International Cryptology Conference. pp. 3–33. Springer (2024)
3. Ding, J., Cheng, C., Qin, Y.: A simple key reuse attack on lwe and ring lwe encryption schemes as key encapsulation mechanisms (kems). Cryptology ePrint Archive (2019)
4. Qin, Y., Cheng, C., Ding, J.: An efficient key mismatch attack on the nist second round candidate kyber. Cryptology ePrint Archive (2019)
5. Qin, Y., Cheng, C., Zhang, X., Pan, Y., Hu, L., Ding, J.: A systematic approach and analysis of key mismatch attacks on lattice-based nist candidate kems. In: Advances in Cryptology—ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part IV 27. pp. 92–121. Springer (2021)
6. Schwabe, P., Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Seiler, G., Stehle, D.: Crystals-kyber—algorithm specifications and supporting documentation. NIST Technical Report (2019)

Exploring Non-Linear Activation Function Approximations in Fully Homomorphic Encryption

Marcos Rodriguez-Vega¹^[0009-0004-2379-842X] and Pino Caballero-Gil¹^[0000-0002-0859-5876]

Universidad de La Laguna, San Cristóbal de La Laguna, Spain
{mrodrive, pcaballe}@ull.es

The growing use of Deep Neural Networks (DNNs) in sensitive applications, such as healthcare, finance, and security, has driven research into homomorphic encryption methods to enable the processing of encrypted data without decrypting it [7]. Using this type of encryption, inference and computation can be performed on fully encrypted neural networks [3]. However, if quantum-resistant cryptographic schemes are not employed, encrypted neural networks could become vulnerable to future adversaries with quantum capabilities [2]. In fact, the National Institute of Science and Technology (NIST) has highlighted the urgent need to transition to quantum-resistant cryptographic schemes to mitigate emerging quantum threats [6].

In order to perform fully encrypted neural network computation, including training, several requirements must be taken into account. First, a Fully Homomorphic Encryption (FHE) scheme with arbitrary evaluation capabilities must be employed to compute complex functions without decryption. This implies that sufficient consecutive multiplications need to be able to be performed on encrypted data before the result becomes unusable due to noise. Therefore, a sufficient multiplicative depth of the FHE scheme is required. Second, it is essential that the noise accumulated in a ciphertext can be removed without decryption in order to perform an unlimited number of operations on the encrypted data. This implies the need for efficient bootstrapping [1]. Third, high-performance computational resources along with optimized hardware and software are needed to mitigate the significant overhead of FHE operations [4]. Fourth, optimization algorithms in the neural network must be adapted to operate exclusively with additions and multiplications, since these are the only arithmetic operations natively supported by FHE schemes. Finally, nonlinear activation functions, which are critical for DNNs to capture complex relationships in data, must be approximated with low-degree polynomial expressions to minimize the computational complexity of FHE. This paper explores this strategy to pave the way for the use of quantum-resistant and fully encrypted deep neural networks.

A work close to this is [5], where a systematic method to construct HE activation functions for convolutional neural networks is presented. However, here the Chebyshev approximation method, based on Chebyshev polynomials, is used to model some of the most commonly used activation functions in DNNs, such as: Sigmoid, Hyperbolic Tangent, Rectified Linear Unit (ReLU), and Softplus.

The absolute error of these polynomial approximations have been systematically measured across their input domains, and extensive experiments have been conducted to assess the performance of DNNs that use these approximated activation functions in comparison with those employing the original functions. The results of the experiments provide some valuable insights into the trade-offs between approximation accuracy and computational efficiency.

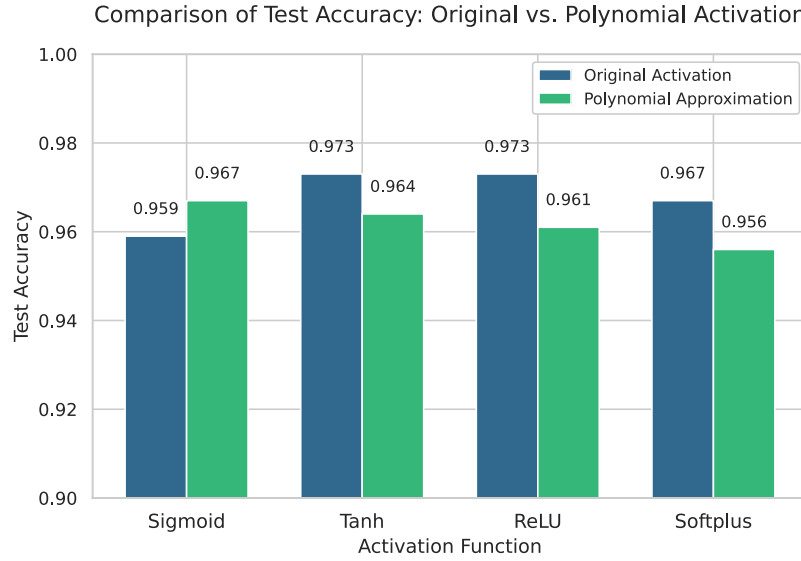


Fig. 1. Comparison of test accuracy

Based on the first experimental results and theoretical considerations, the conclusion is that it is preferable to use degree 5 polynomial approximations since higher degree approximations (such as degree 7 and 9) incur significantly greater homomorphic costs due to the increased multiplicative depth required by the encryption scheme. As can be seen in Figure 1 the results with degree 5 are quite similar compared to the original activation function. In addition, note that it is crucial to implement homomorphic encryption also in the backpropagation algorithm to adjust the DNN weights without decrypting the information. Thus, an appropriate choice of FHE enables its application in both training and inference so that they can be carried out completely in encrypted form, ensuring data privacy throughout the entire process.

In conclusion, this work proves that a lower-degree approximation allows for comparable performance while reducing homomorphic overhead, which represents a step toward fully encrypted, quantum-resistant deep neural networks.

Acknowledgments. This work was possible thanks to the projects: 2023DIG28 IACTA, PID2022-138933OB-I00 ATQUE, and SCITALA C064/23 ULL-INCIBE, and to the C065/23 Cybersecurity Chair of the University of La Laguna and INCIBE, funded by Cajacanarias la Caixa Foundations, MCIN/AEI/10.13039/501100011033, and the Recovery, Transformation, and Resilience Plan (Next Generation) financed by the European Union.

References

1. Ducas, L., Micciancio, D.: FHEW: bootstrapping homomorphic encryption in less than a second. In: Annual international conference on the theory and applications of cryptographic techniques. pp. 617–640. Springer (2015)
2. Han, K., Lee, W.K., Karmakar, A., Yi, M.K., Hwang, S.O.: Quripfenet: Quantum-resistant ipfe-based neural network. *IEEE Transactions on Emerging Topics in Computing* (2024)
3. Lee, J.W., Kang, H., Lee, Y., Choi, W., Eom, J., Deryabin, M., Lee, E., Lee, J., Yoo, D., Kim, Y.S., No, J.S.: Privacy-preserving machine learning with fully homomorphic encryption for deep neural network. *IEEE Access* **10**, 30039–30054 (2022)
4. Liu, C., Li, Z., Li, X.: Accelerating fully homomorphic encryption: A survey on hardware and software solutions. *IEEE Access* **9**, 123456–123470 (2021)
5. Obla, S., Gong, X., Aloufi, A., Hu, P., Takabi, D.: Effective activation functions for homomorphic evaluation of deep neural networks. *IEEE access* **8**, 153098–153112 (2020)
6. of Standards, N.I., Technology: Post-quantum cryptography. <https://www.nist.gov/programs-projects/post-quantum-cryptography>, accessed: 2025-02-16
7. Wood, A., Najarian, K., Kahrobaei, D.: Homomorphic encryption for machine learning in medicine and bioinformatics. *ACM Comput. Surv.* **53**(4) (2020)

A Zero-Knowledge Proof based on shellability of simplicial complexes

Daniel Escanez-Exposito¹[0000–0003–4215–0501],
Pino Caballero-Gil¹[0000–0002–0859–5876],
Eduardo Sáenz-de-Cabezón²[0000–0002–5615–4194], and
Pablo Munarriz-Senosian²[0009–0000–0450–9072]

¹ University of La Laguna, Tenerife, Spain
{jescaez, pcaballe}@ull.edu.es

² University of La Rioja, Logroño, Spain
{eduardo.saenz-de-cabezón, pamunarr}@unirioja.es

Extended Abstract

This paper describes a novel proposal for a Zero-Knowledge Proof based on the shellability property of simplicial complexes, which is quantum-resistant.

On the one hand, a Zero-Knowledge Proof (ZKP) is a two-party cryptographic protocol, where a prover *Alice* (A) can convince a verifier *Bob* (B) that some statement is true without revealing any information other than the validity of the statement itself [1]. This type of proofs, typically used for strong identification schemes [2], must satisfy three properties:

1. *Completeness*: B must accept as valid all the statements that are truly correct, with a probability greater than a given constant.
2. *Soundness*: B is protected against dishonest provers who seek to convince him of the truth of false statements, since it is guaranteed that B will almost never accept untrue statements (i.e., this event occurs with a very low probability).
3. *Zero-Knowledge*: For any honest verifier, there exists an algorithm called simulator that can be used to generate a transcript of the proof, which is indistinguishable from a real interaction, without requiring any secret input from the prover.

On the other hand, an abstract simplicial complex Δ on the vertex set $V = \{1, \dots, n\}$ is a collection of subsets of V such that i) $\emptyset \in \Delta$, and ii) if $\sigma \in \Delta$ and $\tau \subseteq \sigma$ then $\tau \in \Delta$. The elements of Δ are called faces of Δ and the maximal faces with respect to inclusion are called facets. A face σ has dimension d , $\dim(\sigma) = d$, if $d = |\sigma| - 1$. The dimension $\dim(\Delta)$ of Δ is defined as $\max\{\dim(\sigma) \mid \sigma \in \Delta\}$. A simplicial complex is called pure if all its facets have the same dimension d . A pure simplicial complex is called shellable if there exists an ordering $S = (\sigma_1, \dots, \sigma_m)$ of its facets such that, for every $i \geq 2$ we have $\sigma_i \cap \bigcup_{j < i} \sigma_j$ is a pure $(d - 1)$ -dimensional simplicial complex. Such an ordering is called a *shelling* or *shelling order*. Deciding if a pure simplicial complex is shellable is NP-complete for $d \geq 2$ [3]. The search version of that decisional problem, which is to find a shelling of a pure simplicial complex, is also NP-complete.

Since verifying a solution to an NP-complete problem can be done quickly, ZKPs allow the prover to demonstrate knowledge of the solution without disclosing it, ensuring privacy while maintaining security. This makes NP-complete problems a natural choice for constructing secure ZKP protocols [4]. Thus, in this work the NP-complete problem of finding a shelling of a pure simplicial complex is used as basis to define a ZKP.

In the proposed scheme (see Alg. 1), A and B follow a typical interactive ZKP scheme [5] based on *Compromise*, *Challenge*, *Response* and *Verification* steps after an *Initialization* phase [6], where a public username and a secret password are established. First, the prover A constructs a shellable simplicial complex Δ and its corresponding shelling S_Δ by building faces from the previous ones. In this construction, it must be guaranteed that given only Δ (which A will make public as her username in an identification scheme), it is NP-complete to find its shelling (which A will use as her password linked to her username). Next, the verifier B must ensure that A knows the password linked to Δ . To do this, A generates a random permutation of the vertices of the complex ($\Delta_i = P_i(\Delta)$), constructing an isomorphic simplicial complex that is sent as a public commitment of the secret. The verifier B randomly issues one of two possible challenges: either he asks A for the isomorphism P_i , or he asks for the shelling of Δ_i (which without the isomorphism confers no information from the original shelling). In both cases the verifier can check the correctness of what he receives.

Algorithm 1 Proposed Scheme

Initialization: A generates (Δ, S_Δ)

$A \xrightarrow{\Delta} B$

Iterations: $\forall i \in \{1, \dots, m\}$

Compromise: $\Delta_i := P_i(\Delta)$

$A \xrightarrow{\Delta_i} B$

Challenge: Random $b_i \in \{0, 1\}$

$B \xrightarrow{b_i} A$

Response: $r := (P_i, S_{\Delta_i})$

$A \xrightarrow{r[b_i]} B$

Verification: B verifies $r[b_i]$

This proposal fulfils the three properties of ZKP. The *Completeness* property is satisfied because B accepts all the statements that are truly correct, with probability 1, so in this proposal this is considered a deterministic property [7]. The *Soundness* property relies on the fact that after a large number m of iterations in the scheme, B can be sure that A knows a shelling of Δ . The probability that a dishonest prover managed to bypass the system is $\frac{1}{2^m}$, which for large m tends to zero. Lastly, *Zero-Knowledge* is achieved given that the verifier has obtained absolutely no information about the key in this procedure, satisfying the ZKP definition.

Acknowledgments.

This work was possible thanks to the projects: 2023DIG28 IACTA, PID2022-138933OB-I00 ATQUE, and SCITALA C064/23 ULL-INCIBE, and to the C065/23 Cybersecurity Chair of the University of La Laguna and INCIBE, funded by Cajacanarias la Caixa Foundations, MCIN/AEI/10.13039/501100011033, and the Recovery, Transformation, and Resilience Plan (Next Generation) financed by the European Union.

References

1. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof-systems. In: Symposium on the Theory of Computing (1985), <https://api.semanticscholar.org/CorpusID:209402113>
2. Fiege, U., Fiat, A., Shamir, A.: Zero knowledge proofs of identity. In: Proceedings of the nineteenth annual ACM symposium on Theory of computing. pp. 210–217 (1987)
3. Goaoc, X., Paták, P., Patáková, Z., Tancer, M., Wagner, U.: Shellability is NP-complete. *Journal of the ACM (JACM)* 66(3), 1–18 (2019)
4. Goldreich, O., Micali, S., Wigderson, A.: How to prove all NP statements in zero-knowledge and a methodology of cryptographic protocol design. In: *Advances in Cryptology—CRYPTO’86: Proceedings 6*. pp. 171–185. Springer (1987)
5. Impagliazzo, R., Yung, M.: Direct minimum-knowledge computations. In: *Conference on the Theory and Application of Cryptographic Techniques*. pp. 40–51. Springer (1987)
6. Caballero-Gil, P., Hernández-Goya, C.: Strong solutions to the identification problem. In: *International Computing and Combinatorics Conference*. pp. 257–261. Springer (2001)
7. Goldreich, O.: Zero-Knowledge twenty years after its invention. *IACR Cryptol. ePrint Arch.* 2002, 186 (2002)

BB84-Inspired Quantum Zero-Knowledge Proof for User Authentication over Quantum Channels

Jorge Garcia-Diaz^[0009–0006–4400–6836],
Daniel Escanez-Exposito^[0000–0003–4215–0501],
Pino Caballero-Gil^[0000–0002–0859–5876], and
Jezabel Molina-Gil^[0000–0001–7702–9264]

University of La Laguna, Tenerife, Spain
{jgarcidi, jescanez, pcaballe, jmmolina}@ull.edu.es

1 Extended Abstract

Zero-Knowledge Proofs (ZKPs) are a useful tool for strong user authentication protocols. Traditionally, these cryptographic mechanisms are based on mathematical problems that are typically classified as computationally intractable or NP-hard. However, with the rapid advancement of quantum computing, the complexity landscape of such problems has suffered significant changes. Certain problems, once deemed difficult with traditional computers, suddenly seem easily solvable with quantum algorithms running on quantum computers. Fundamental quantum algorithms in this sense are Grover’s search [1], which solves the unstructured search problem in databases or spaces of possible solutions, and Shor’s algorithm [2], which allows solving the integer factorization problem.

While there are some research efforts relating ZKPs to quantum computing attempting to leverage quantum computational advantages over classical systems [3] [4], there remains a notable scarcity of academic work exploring the implementation of ZKPs within the quantum paradigm and Quantum Key Distribution (QKD) frameworks [5]. Specifically, limited literature exists addressing ZKPs that operate independently of computationally hard mathematical assumptions, opening an intriguing avenue for further research in this field.

This work proposes a novel Quantum ZKP for user authentication based on ideas similar to those underlying the QKD protocol called BB84 [6]. In particular, the security of the protocol fundamentally relies on the inherent randomness of the output when a given quantum state undergoes projection in an incorrectly chosen basis [7]. This randomness ensures that any deviation from the intended projection basis compromises the ability to extract meaningful information, thereby safeguarding the integrity of the protocol.

In this proposal, both the prover (Alice) and the verifier (Bob) pre-share a secret key consisting of two n -bit strings $a = \{a_i\}_{i=1}^n$ and $b = \{b_i\}_{i=1}^n$. The first step is the challenge generation where the verifier generates a quantum state $|\psi\rangle$ using the secret quantum bases defined by b to encode the secret bits a . Considering that the bits 0 and 1 of b are related, respectively, to the Hadamard and the computational basis, using the algebraic notation introduced in [8], the quantum state resulting from this first step is $|\psi\rangle = |a\rangle H_{\{i|b_i=1\}}$.

Next, Bob generates a random bit string $c \in \{0, 1\}^n$ and applies a Hadamard gate on the qubits where $c_i = 1$. Mathematically, this can be expressed as $|\psi\rangle H_\Omega$, $\Omega = \{i \mid c_i = 1\}$. Bob then sends this *challenge state* to Alice. Alice's aim is to provide a sufficiently accurate estimation c' of c .

Once Alice receives the state $|\psi\rangle H_\Omega$, she executes the *zero-knowledge modifications* using the same principle as Bob's modifications. She generates a random string of bits $d \in \{0, 1\}^n$ and applies the Hadamard gate to obtain the state $|\psi\rangle H_\Omega H_\Gamma$, where $\Gamma = \{i \mid d_i = 1\}$.

These random modifications ensure the zero-knowledge property of the protocol by randomizing Alice's estimation c' if the state $|\psi\rangle$ is not prepared honestly, thereby preventing dishonest verifiers or eavesdroppers from learning nothing from the secret keys. After the *zero-knowledge modifications*, Alice collapses the resulting state using the secret basis b and obtains a string of bits a' . She then cleverly generates the *estimation string* c' using information from Γ , a , and a' , and sends c' to the verifier, Bob.

Upon receiving c' , Bob counts the number of coincidences between c and c' . If both parties are honest, Alice is expected to recover approximately 75% of the bits of c correctly, while if Alice is dishonest, she is expected to recover only 50% of c . A honest prover's accuracy follows a binomial distribution $B(n, \frac{3}{4})$, whereas a dishonest prover follows a binomial distribution $B(n, \frac{1}{2})$. This makes the security of the protocol increase by increasing n . Additionally, there is no probabilistic distinction between executing a single iteration for key size n or performing k iterations over a $\frac{k}{n}$ and taking the mean accuracy of all iterations, making both options equally safe except for the evident brute-force attack for smaller secret key sizes.

This work provides a mathematical analysis of the protocol's security by examining the probability distributions of both honest and dishonest provers. This analysis allows us to formally assess the completeness and soundness properties of the protocol by giving the probabilities associated to the wanted threshold for the number of coincidences, modifying the threshold in terms of the wanted probabilities for the soundness and completeness probabilities of this protocol. Furthermore, our theoretical framework is substantiated through a simulation-based implementation utilizing IBM's quantum simulator, Qiskit [9]. The simulations are conducted not only under ideal conditions but also in a more realistic setting that accounts for prevalent quantum errors, such as phase damping and amplitude damping [10], which could occur during transmission through a quantum channel [11].

As evidenced by this work's results, the protocol not only upholds its security guarantees but also remains practical and feasible under real-world conditions. Additionally, the protocol offers significant flexibility in the implementation of each iteration thanks to the independent execution of this protocol over each one of the qubits, allowing for adaptable execution strategies. This adaptability proves particularly advantageous in scenarios where quantum resources are constrained, such as limited quantum channels and hardware, thereby enhancing its applicability across diverse quantum communication environments.

Acknowledgments.

This work was possible thanks to the projects: 2023DIG28 IACTA, PID2022-138933OB-I00 ATQUE, and SCITALA C064/23 ULL-INCIBE, and to the C065/23 Cybersecurity Chair of the University of La Laguna and INCIBE, funded by Cajacanarias la Caixa Foundations, MCIN/AEI/10.13039/501100011033, and the Recovery, Transformation, and Resilience Plan (Next Generation) financed by the European Union.

References

1. Grover, L.K.: A fast quantum mechanical algorithm for database search (1996), <https://arxiv.org/abs/quant-ph/9605043>
2. Shor, P.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science. pp. 124–134 (1994)
3. Broadbent, A., Ji, Z., Song, F., Watrous, J.: Zero-knowledge proof systems for qma. In: 2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS). p. 31–40. IEEE (Oct 2016), <http://dx.doi.org/10.1109/FOCS.2016.13>
4. Vidick, T., Watrous, J.: Quantum proofs. Foundations and Trends in Theoretical Computer Science 11(1–2), 1–215 (2016), <http://dx.doi.org/10.1561/04000000068>
5. García Cid, M.I., Bodanapu, D., Sánchez-Ledesma, R.M., Ortiz Martín, L., Martín Ayuso, V., Brunero, M., Gatto, A., Martelli, P.: Quantum zero-knowledge protocol for identity authentication. In: Quantum Engineering and Technology Conference (QET 2023). vol. 2023, pp. 15–18 (2023)
6. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science 560, 7–11 (2014), <https://www.sciencedirect.com/science/article/pii/S0304397514004241>, theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84
7. Wiesner, S.: Conjugate coding. SIGACT News 15(1), 78–88 (Jan 1983), <https://doi.org/10.1145/1008908.1008920>
8. Escanez-Exposito, D., Caballero-Gil, P., Rodriguez-Vega, M., Costa-Cano, F., Sáenz-de Cabezón, E.: Algebraic language for the efficient representation and optimization of quantum circuits. Physica Scripta 100(2), 025107 (jan 2025), <https://dx.doi.org/10.1088/1402-4896/ad9fb6>
9. Javadi-Abhari, A., Treinish, M., Krsulich, K., Wood, C.J., Lishman, J., Gacon, J., Martiel, S., Nation, P.D., Bishop, L.S., Cross, A.W., Johnson, B.R., Gambetta, J.M.: Quantum computing with Qiskit (2024)
10. Giovannetti, V., Fazio, R.: Information-capacity description of spin-chain correlations. Physical Review A 71(3) (Mar 2005), <http://dx.doi.org/10.1103/PhysRevA.71.032314>
11. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press (2010)

The Butterfly Protocol: QKD as a Service Without the "Weakest Link" Vulnerability

Sergejs Kozlovičs, Elīna Kalniņa, Juris Viksna, Krišjānis Petručeņa, and
Edgars Rencis

Institute of Mathematics and Computer Science, University of Latvia, Riga, Latvia
Sergejs.Kozlovics@lumii.lv Elina.Kalnina@lumii.lv Juris.Viksna@lumii.lv
Krisjanis.Petrucena@lumii.lv Edgars.Rencis@lumii.lv

1 Introduction

Quantum Key Distribution (QKD) is a process of generating a secret key shared by two parties (Alice and Bob) that relies on the laws of Physics and ensures that the keys have not been eavesdropped on or modified by a third party. QKD provides perfect forward secrecy in the face of the quantum computing era and is resistant to "Harvest now, decrypt later" attacks.

While commercial QKD devices are available on the market, they are expensive, require specific infrastructure, and have high operational expenses. Thus, they are not affordable to everyone. Furthermore, it is impossible to integrate QKD-specific hardware components (such as single photon detectors and cooling systems) into physically small or low-resource devices such as smartphones and IoT devices.

We propose an architecture and the extended version of the Butterfly Protocol, which we used to implement QKD as a service (QaaS) [1, 2].

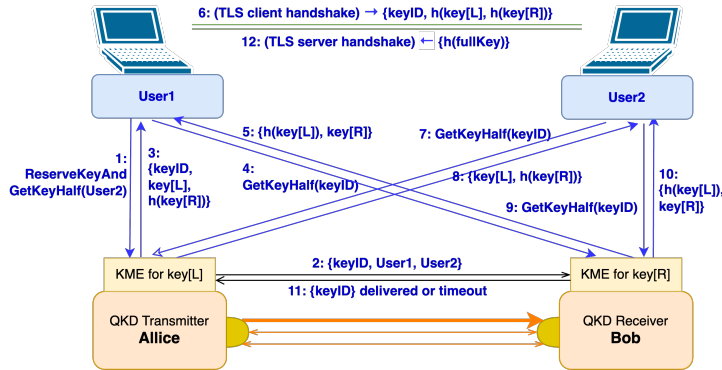


Fig. 1. The seven segments of the Butterfly Protocol: the data link (top-most, TLS with QaaS), the four butterfly links (PQC), the KME link, and the quantum link (two "black boxes" with 2-4 optical fibers for quantum and service channels).

2 The Essence of the Butterfly Protocol

Figure 1 depicts the 12-step Butterfly protocol, where User1 and User2 (e.g., an application client and a server) access QaaS Key Management Entities (KME) via 4 "butterfly" links secured by TLSv1.3 connections with PQC. We currently use FrodoKEM and SPHINCS+ but can easily swap to other PQC algorithms (such as implemented in LibOQS or BouncyCastle). Each KME returns only half of the key ($\text{key}[L]$ or $\text{key}[R]$) and the hash h of the other half. When both users receive both halves of the key, they use the received hashes to verify each half and, hence, the whole key.

The data link is secured by a modified TLSv1.3, where the key encapsulation algorithm is replaced by steps 6 and 12 in Figure 1. Notice that User1 sends $h(\text{key}[L])$ and $h(\text{key}[R])$ to User2, while User2 replies with $h(\text{fullKey})$. That ensures independent verification of the other user's possession of the full key.

The KME link is needed to ensure that only User1 and User2 (and not Eve listening to step 6) are allowed to obtain $\text{key}[R]$ from Bob's KME.

We axiomatize the security of the QKD link, where an attacker can be detected using Quantum Mechanics and QKD protocols. This implies the security of the KME link since it has direct access to QKD keys. Since the full key is never transmitted via any single classical link, an active attacker (with unlimited computational power) must eavesdrop and decrypt at least two butterfly connections to obtain the QKD-generated key. If an eavesdropper attacks the data link, the probability of obtaining the key (even if preimage resistance for the hash function h is broken) can be made negligible if we use, e.g., a 128-bit hash with 512-bit QKD keys: for any half of the key (256 bits), we would have $\approx 2^{128}$ preimages.

The authentication of QKD devices and KME nodes is a black box from our perspective.¹ We rely on PQC certificates (currently, SPHINCS+) for authenticating the butterfly links. While the data link can also be authenticated in the same way, we can also utilize the full QKD key (verified via hashes) for that. Furthermore, it is possible to introduce a Butterfly Protocol extension for implicit mutual authentication, which aborts the TLS session in case of forgery.

3 Current Results and Work-in-Progress

Our QaaS solution is novel in that we sacrifice the idea of relying on the geographically closest QKD node² in favor of the tolerance to breaking *any* 1 out of 7 links from Figure 1.

Our QaaS implementation is available at qkd.lumii.lv. We are working on proxy software to integrate ETSI GS QKD 014 and CISCO SKIP API into our QaaS [3, 4]. As a result, our QaaS solution could replace missing point-to-point QKD links while gradually building QKD networks.

¹ This is usually a commercial know-how. The QKD link is presumably authenticated by hash-signing challenge requests with a pre-shared key (PSK).

² which might be challenging to implement due to per-packet routing in the global Internet

Acknowledgments. Research supported by the project No. 2.3.1.1.i.0/1/22/I/CFLA/001 "Latvian Quantum Technologies Initiative".

References

1. Kozlovičs, S., Petručeņa, K., Lāriņš, D., Viksna, J.: Quantum Key Distribution as a Service and Its Injection into TLS. In: Information Security Practice and Experience (ISPEC 2023), LNCS, vol. 14341, pp. 527–545. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-7032-2_31
2. Viksna, J., Kozlovics, S., Rencis, E.: POSTER: Integrating Quantum Key Distribution into Hybrid Quantum-Classical Networks. In: Zhou, J., et al. Applied Cryptography and Network Security Workshops. ACNS 2023. LNCS, vol. 13907 pp. 695–699. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-41181-6_42
3. European Telecommunications Standards Institute (ETSI): Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API. ETSI GS QKD 014 V1.1.1, February 2019.
4. Cisco Systems. Secure Key Integration Protocol (SKIP). Internet Draft, draft-cisco-skip-00, v2024-08-30, 2024.

Entanglement-Based QKD Proposal Without Sharing Measurement Bases

Daniel Escanez-Exposito^[0000–0003–4215–0501] and
Pino Caballero-Gil^[0000–0002–0859–5876]

University of La Laguna, Tenerife, Spain
{jescanez, pcaballe}@ull.edu.es

Extended Abstract

Bennett, Brassard and Mermin [1] proposed a protocol in 1992 (called BBM92) to refine the ideas contained in the first entanglement-based Quantum Key Distribution (QKD) proposal, E91 [2]. Their work justifies that it is not necessary to rely on Bell's inequalities to certify security in an EPR peer-based key distribution. It also shows the security equivalence with the BB84 protocol [3], not based on quantum entanglement. BBM92 uses two measurement bases, which the legitimate participants in the communication (Alice and Bob) will randomly use on their corresponding qubits of the EPR pairs [4]. After the measurements, Alice and Bob publish the used bases and discard the incorrectly measured pairs. The remaining ones must be perfectly correlated. To check this, they compare at least half of the measurements they have made, and if the results match, then they can be sure that the remaining pairs are perfectly correlated so they can use them to determine a common secret key. In a sense, this is like recovering the BB84 scheme, but applied on entanglement pairs.

The Photon-Number Splitting (PNS) vulnerability [5] is a threat to certain implementations of the BB84 protocol, which use light pulses containing multiple photons. Eve can measure one photon from each pulse and let the rest pass without Alice and Bob being aware of the eavesdropping. To do this, Eve could use a device for measuring the number of photons in the pulses or Quantum Non-Demolition (QND) measurement of the photon number [6]. This blocks the pulses with a single photon and extracts one of the particles when it has more, to store it in quantum memory and send the rest. When the time comes for Alice and Bob to publish the used bases, Eve can benefit from this information to measure the state of the stored photons. If Eve does not introduce a loss rate higher than the quantum channel threshold, taking into account the photons it blocks and those it stores, then its presence will go unnoticed. In 2004, Scarani, Acín, Ribordy and Gisin proposed a QKD protocol (called SARG04) to prevent this type of attack [7]. These authors establish as a starting point for their proposal that the vulnerability of BB84 is due to the use of orthogonal states, since after the basis reconciliation, Eve only has to discriminate between two states that are mutually exclusive. To avoid this, they suggest the use of non-orthogonal states, so that the used basis cannot be determined deterministically.

The following describes a QKD protocol inspired by the two previous proposals. As in the BBM92 protocol, a source of entangled pairs is needed, which distributes each pair between both participants, and assigns half of entangled pairs to each participant randomly. Then, assuming that the emitted entangled pairs are in the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) = \frac{1}{\sqrt{2}}(|+_A +_B\rangle + |-_A -_B\rangle)$, Alice and Bob each measure their qubit using a randomly chosen basis between: computational $C = \{|0\rangle, |1\rangle\}$ or Hadamard $H = \{|+\rangle, |-\rangle\}$. For each of its assigned qubits, each participant publicly announces a non-orthogonal two-state basis belonging to the set of the 4 possible bases: $C \times H = \{|0\rangle, |+\rangle\}, \{|0\rangle, |-\rangle\}, \{|1\rangle, |+\rangle\}, \{|1\rangle, |-\rangle\}$, such that the basis chosen for each qubit is consistent with the corresponding measurement. In this way, the bases chosen for the projections are not announced. For those qubits that a participant has measured obtaining values not contained in the basis announced by the other participant, the qubit of the announcing entity can be deduced. For example, if Alice uses the C basis, measures the state $|0\rangle$ and announces the basis $\{|0\rangle, |+\rangle\}$, then in the event that Bob measures using the H basis and gets a $|-\rangle$ state, he can be sure that Alice measured the $|0\rangle$. Thus, 25% of the values obtained from each participant's measurements will be known to the other participant, so these values are candidates for forming part of the final shared secret key. To detect possible interceptions, both participants publicly share the values obtained from the rest of the measurements and the bases with which they were measured. In this way, they will be able to verify that when the bases coincide (50% of the total qubits), the values must also match. If this check is successful, the participants use privacy amplification and information reconciliation techniques to eliminate possible erroneous bits and reduce adequately Eve's possible knowledge of the key [8]. Otherwise, the protocol must be restarted.

Although a version of SARG04 using entanglement was proposed in [9], that protocol contains some asymmetry and follows a structure similar to the typical prepare-and-measure scheme. In that proposal, Alice prepares the entangled pairs and then sends one of the qubits for Bob to measure, with her measuring the remaining qubit. The use of entanglement certainly seems forced, since Alice could arbitrarily and randomly choose the state of her bit and send the corresponding qubit to Bob, without using entanglement. This would allow the protocol to be simplified considerably, obtaining the same results and resembling its form without entanglement. Instead, the protocol proposed in the present work tries to achieve greater symmetry, so that if an interception occurs in any of the parties, it can be detected in the same way as in the BBM92 protocol. To do so, all the measurements already made on the qubits are used, including those that will never form part of the key and that are discarded in the SARG04 protocol, so that the information that verifies the absence of interception can be shared securely and publicly. In addition, the entanglement-based version of SARG04 required Alice to participate as the generator of the entangled pairs, which does not occur in the present proposal.





Acknowledgments.

This work has been possible thanks to the PID2022-138933OB-I00 and 2023DIG28 IACTA research projects funded by MCIN/AEI/10.13039/501100011033/FEDER EU, and the CajaCanarias la Caixa Foundation. It is also part of the Cybersecurity Chairs sponsored by Binter, and by INCIBE through an initiative carried out within the framework of the funds of the Recovery, Transformation and Resilience Plan, financed by the European Union (Next Generation).

References

1. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without bell's theorem. *Phys. Rev. Lett.* 68, 557–559 (1992)
2. Ekert, A.K.: Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* 67, 661–663 (1991)
3. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* 560, 7–11 (1984)
4. Einstein, A., Podolsky, B., Rosen, N.: Can quantum-mechanical description of physical reality be considered complete? *Physical review* 47(10), 777 (1935)
5. Acín, A., Gisin, N., Scarani, V.: Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks. *Physical Review A* 69(1), 012309 (2004)
6. Grangier, P., Levenson, J.A., Poizat, J.P.: Quantum non-demolition measurements in optics. *Nature* 396(6711), 537–542 (1998)
7. Scarani, V., Acín, A., Ribordy, G., Gisin, N.: Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* 92, 057901 (2004)
8. Chau, H.F.: Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate. *Physical Review A* 66(6), 060302 (2002)
9. Branciard, C., Gisin, N., Kraus, B., Scarani, V.: Security of two quantum cryptography protocols using the same four qubit states. *Physical Review A—Atomic, Molecular, and Optical Physics* 72(3), 032301 (2005)

Confidential QUBO solver

Mariano Caruso^{1,2,3,4} , Daniel Escanez-Exposito⁵ , Pino Caballero-Gil⁵ ,
and Carlos Kuchkovsky⁴ 

¹ UGR, Granada, Spain.

`mcaruso@ugr.es`

² FIDESOL, Granada, Spain.

³ UNIR, Logroño, Spain.

⁴ QCentroid, Bilbao, Spain.

⁵ CryptULL–ULL, Tenerife, Spain.

Abstract. Quadratic Unconstrained Binary Optimization (QUBO) is widespread and solvable via classical or quantum computing. However, outsourcing these computations online exposes sensitive data to potential breaches. We introduce a novel encryption scheme that seamlessly integrates with any solver or hardware platform, ensuring data security without compromising performance. A robust `python` implementation delivers promising results, marking a significant step forward in secure optimization for both classical and quantum environments.

Keywords: QUBO problems, secure optimization, cryptographic solution, transfer principle, quantum computing, hardware agnostic.

1 Introduction

Quadratic Unconstrained Binary Optimization (QUBO) is crucial in combinatorial optimization across disciplines like cryptography, economics, physics, and machine learning [1–8]. It models problems such as max-cut, graph coloring, and clustering [9–11, 13], with applications in quantum computing via Ising models and quantum annealing [14–16]. As NP-hard [17], QUBO demands efficient and secure solving methods.

Online solvers risk exposing sensitive data. This work proposes an encryption scheme enabling secure external solving without revealing original data. Unlike standard homomorphic encryption [18–20], our approach meets the specific needs of QUBO.

We define the set of natural indices $I_n := \{1, \dots, n\}$ and the binary space $\{0, 1\}^n$. A function $f(\mathbf{x}) = \sum_{(i,j) \in I_n^2} \mathbf{Q}_{ij} x_i x_j$ is defined using a matrix $\mathbf{Q} \in \mathbb{R}^{n \times n}$. Since adding a constant does not change the optimal solution, the typical QUBO problem is to find

$$\underset{\mathbf{x} \in \{0,1\}^n}{\operatorname{argmin}} f(\mathbf{x}),$$

where the objective function f can be expressed compactly as $f(\mathbf{x}) = \mathbf{x} \cdot \mathbf{Q} \mathbf{x}$. When solving such problems with cloud solvers, transmitting the matrix \mathbf{Q} in clear text risks exposing sensitive information.

2 Transfer principle

The encrypted objects are denoted with a prime, so the encrypted objective function is $f'(\mathbf{x}') = \mathbf{x}' \cdot \mathbf{Q}' \mathbf{x}'$. Define a mapping T from the original optimization problem to an encrypted version $f'(\mathbf{x}') := f(T(\mathbf{x}'))$. This allows a user to send an encrypted QUBO problem to an external solver without exposing sensitive data (the matrix \mathbf{Q}). The transformation T defines a new optimization problem in such a way that its resolution in the encrypted domain can be carried out without revealing information about the original optimization problem and without requiring key exchange. In this context, we could mention some similarities with homomorphic encryption. Note that T will not be a homomorphism in all cases, as it will not preserve the operations of addition \oplus or product \odot in $\{0,1\}^n$. With a transformation T satisfying $\mathbf{x} = T(\mathbf{x}')$, we establish a relation between the original matrix \mathbf{Q} and its encrypted counterpart \mathbf{Q}' . Matching the quadratic forms in the expressions for f and f' yields a closed-form relation through an encryption function: $\mathbf{Q}' = \mathcal{E}(\mathbf{k}_T, \mathbf{Q})$ or $\mathbf{Q}' = \mathcal{E}_{\mathbf{k}_T}(\mathbf{Q})$ [21]. The matrix of the original QUBO problem is encrypted and sent to the `QUBO – solver`. The solution returned, \mathbf{x}'_* , is then decrypted locally, and the solution to the original problem is obtained via $\mathbf{x}_* = T(\mathbf{x}'_*)$. In order to construct T there are two ingredients: diffusion via permutations and confusion via substitutions, and the encrypted matrix \mathbf{Q}' is obtained from $\mathcal{E}_{\mathbf{P}}$ and $\mathcal{E}_{\mathbf{k}}$, respectively.

3 Conclusions

This work addresses the security challenges in the online resolution of unconstrained binary quadratic optimization problems. By employing cryptographic methods, we establish a framework for securely solving these problems using both classical and quantum computing. This approach protects the problem’s sensitive information during resolution and encourages the adoption of advanced techniques in online environments, promoting further development in quantum computing and data security.

A complete implementation of these proposals has been developed in `python`. The proposed cryptographic solution is independent of the optimization method, so it does not depend on how the QUBO problem is solved. It supports exact methods, classical or quantum annealing, as well as heuristic approaches such as simulated annealing and genetic algorithms, making it hardware agnostic.

Acknowledgments. We thank FIDESOL, UGR, and QCentroid for the support and recall also the anonymous readers for their constructive criticism of this work. This research has been partially supported by the project ECO-20241014: QUORUM funded by Ministerio de Ciencia, Innovación y Universidades, through CDTI and PID2022-138933OB-I00: ATQUE funded by MCIN/AEI/10.13039/501100011033/FEDER, EU.

References

1. Burek, Elzbieta, et al. “Algebraic attacks on block ciphers using quantum annealing.” *IEEE Transactions on Emerging Topics in Computing* vol. 10, 2 pp. 678-689 (2022).
2. Phab, Luca, Stéphane Louise, and Renaud Sirdey. “First attempts at cryptanalyzing a (toy) block cipher by means of quantum optimization approaches” *Journal of Computational Science* 69 (2023): 102004.
3. Orús, R., Muga, S., Lizaso, E.: “Quantum computing for finance: Overview and prospects”, *Reviews in Physics*, vol. 4, pp. 100028, 2019.
4. Hong, S. W., et al.: “Market graph clustering via qubo and digital annealing”, *Journal of Risk and Financial Management*, vol. 14, n. 1, pp. 34, 2021.
5. Neukart, F., et al.: “Traffic flow optimization using a quantum annealer”, *Frontiers in ICT*, vol. 4, pp. 29 (2017).
6. Li, R. Y., et al.: “Quantum annealing versus classical machine learning applied to a simplified computational biology problem”, *NPJ quantum information*, vol. 4, n. 1, pp. 14 (2018).
7. R. Novak, “Quantum Algorithms in Electromagnetic Propagation Modelling for Telecommunications”, *IEEE Access* (2023).
8. Streif, M., Neukart, F., Leib, M.: “Solving quantum chemistry problems with a d-wave quantum annealer”, *Quantum Technology and Optimization Problems: First International Workshop, Springer International Publishing*, vol. 11413, pp. 111-122 (2019).
9. Rehfeldt, D., Koch, T., Shinano, Y.: “Faster exact solution of sparse MaxCut and QUBO problems”, *Mathematical Programming Computation*, vol. 15, n. 3, pp. 445-470 (2023).
10. Tabi, Z., et al.: “Quantum optimization for the graph coloring problem with space-efficient embedding”, *2020 IEEE international conference on quantum computing and engineering (QCE)*, pp. 56-62 (2020).
11. Mniszewski, S. M.: “Graph partitioning as quadratic unconstrained binary optimization (QUBO) on spiking neuromorphic hardware”, *Proceedings of the International Conference on Neuromorphic Systems*, pp. 1-5 (2019).
12. Date, P., Potok, T.: “Adiabatic quantum linear regression”, *Scientific reports*, vol. 11, n. 1, pp. 21905 (2021).
13. Date, P., Arthur, D., Pusey-Nazzaro, L.: “QUBO formulations for training machine learning models”, *Scientific reports*, vol. 11, n. 1, pp. 10029 (2021).
14. Brush, S. G.: “History of the Lenz-Ising model”, *Reviews of modern physics*, vol. 39, n. 4, pp. 883 (1967).
15. Albash, T., Lidar, D. A.: “Adiabatic quantum computation”, *Reviews of Modern Physics*, vol. 90, n. 1, pp. 015002 (2018).
16. P. Hauke, et al: “Perspectives of quantum annealing: Methods and implementations”, *Reports on Progress in Physics*, vol. 83, n. 5, pp. 054401 (2020).
17. F. Barahona, *On the computational complexity of Ising spin glass models*, J. Phys. A: Math. Gen. 15 3241 (1982).
18. Paillier, P. “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes”. *Advances in Cryptology — EUROCRYPT '99. Lecture Notes in Computer Science*. Vol. 1592. Springer. pp. 223–238 (1999).
19. ElGamal, T. “A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”. *IEEE Transactions on Information Theory*. 31 (4): 469–472 (1985).

20. Goldwasser, S, Micali, S. “Probabilistic encryption & how to play mental poker keeping secret all partial information”. Proceedings of the fourteenth annual ACM symposium on Theory of computing - STOC '82. pp. 365–377 (1982).
21. Boneh, D. and Shoup, V., “A Graduate Course in Applied Cryptography”, Applied Cryptography Group - University Stanford (2020).

On a Quantum Search for Short Vectors in Lattices using QRISP

Julen Bernabé-Rodríguez^[0000–0002–2130–3591], Iñaki Seco-Aguirre^[0000–0001–9264–2286], Cristina Regueiro^[0000–0002–6031–9449], and Oscar Lage^[0000–0003–1168–1932]

TECNALIA, Basque Research and Technology Alliance (BRTA), Bizkaia Science and Technology Park, Building 700, E-48160 Derio, Bizkaia, Spain {julen.bernabe, iñaki.seco, cristina.regueiro, oscar.lage}@tecnalia.com

Abstract. Learning With Errors is a fundamental problem in modern cryptography. In addition to allowing to build very efficient post-quantum secure schemes (*e.g.* ML-KEM or ML-DSA), it has also enabled the construction of other interesting primitives, such as Fully Homomorphic Encryption.

The security of this problem comes from the fact that the currently most efficient algorithms to solve it rely on classical lattice problems such as the Shortest Vector Problem (SVP) or the Short Integer Solution (SIS) Problem. These problems are thought to be very hard to solve, both in theory and in practice. A concrete family of algorithms trying to break SVP and SIS, sieving methods, can theoretically benefit from Grover’s search algorithm, but no improved acceleration has been shown in practice yet.

This ongoing work intends to instantiate the first practical quantum acceleration based on Grover’s search for solving SVP and SIS. This implementation will use QRISP, a Python module enabling the implementation of high-level quantum circuits. The resulting implementation will show to what extent quantum acceleration might work in practice, giving concrete results for low-dimensional lattices.

Keywords: Learning With Errors · Sieving · Quantum Acceleration.

1 Introduction

Learning With Errors (LWE) is a crucial problem in modern cryptography. Besides having allowed for the creation of cryptographic primitives not previously resolved, such as Fully Homomorphic Encryption, it is considered hard to solve by both classical and quantum computers. In fact, currently, the only standardized scheme by NIST in their Post-Quantum Cryptography Standardization process is ML-KEM [12], which is based on a variant of LWE. Given a random matrix \mathbf{A} and a vector \mathbf{t} , the LWE problem can be stated in two different ways: the Decision-LWE problem asks for distinguishing if \mathbf{t} is also randomly generated or if there exist small \mathbf{s} and \mathbf{e} such that $\mathbf{t} = \mathbf{A}\mathbf{s} + \mathbf{e}$, and the equivalent Search-LWE problem involves recovering the secret vector \mathbf{s} from $(\mathbf{A}, \mathbf{t} = \mathbf{A}\mathbf{s} + \mathbf{e})$.

The LWE problem can also be restated from a lattice perspective. Interestingly, solving the LWE problem can be reduced to solving some of the mostly known lattice problems: the Shortest Vector Problem (primal attacks) and the Short Integer Solution problem (dual attacks) [3]. In both cases, the problem to be solved is equivalent: finding short vectors in a lattice. The shortness of vectors can be defined with respect to any norm, but usually the Euclidean norm is used [11]. The aforementioned lattice problems have been proven to be very hard to solve [13], even for quantum computers.

2 Lattice Attacks

In this context, the best known approach to break LWE cryptography is to use algorithms for finding short vectors in the underlying lattice. There are two main families of such algorithms:

- Algorithms for finding *exact* short vectors in the lattice, *i.e.*, vectors that are actually short in the lattice.
- Algorithms for finding *approximate* short vectors in the lattice, *i.e.*, vectors whose norm is at most γ times the norm of the shortest vector.

In practice, approximate algorithms are mostly used because they are much more efficient than the former (polynomial vs. exponential time). Modern algorithms of this family [4] use lattice basis reduction in order to find short vectors in lower-dimensional lattices afterwards. Thus, after reducing the basis, they make use of algorithms of the first family. The approximate algorithms run in polynomial time, but the short vector they guarantee to find is exponentially larger than the shortest one, even if in practice this exponent is not too large [10].

The Lenstra-Lenstra-Lovász (LLL) [9] and Blockwise Korkine-Zolotarev (BKZ) [7] algorithms are the most widely used methods for finding approximate short vectors. Given a basis defining a lattice, both algorithms make use of the Gram-Schmidt orthogonalization [14] process in order to reduce the basis. In fact, BKZ is an

extension of LLL that has been evolved with several improvements [5], being considered the most efficient lattice reduction algorithm nowadays [4]. At its very core, the BKZ algorithm defines a so-called block β , and tries to find the shortest possible vector for the different blocks that can be taken from the lattice's basis. In other words, given a basis $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$, the BKZ algorithm iteratively uses exact algorithms to find the shortest vector in the lattice generated by every block $\{\mathbf{b}_i, \dots, \mathbf{b}_{i+\beta-1}\}$, then adds this shortest vector to \mathbf{B} and removes the linear dependence of the new basis using Gram-Schmidt.

3 Exact Algorithms and Quantum Acceleration

As explained in Section 2, any modern attack to LWE instances, such as those based on BKZ, always requires algorithms for finding the exact shortest vector in a lattice, even if reduced to lower dimensions. There are two major techniques for this:

- *Enumeration*: Consists of defining a bounded region of space and then enumerating all the lattice points inside it. Having all possible lattice points of a bounded region makes it possible to find the shortest one. This technique is the most efficient one in practice nowadays, even if it has super-exponential worst-case time complexity.
- *Sieving*: In contrast to enumeration, sieving is performed by building an extremely large list of lattice vectors and finding the shortest vector by computing linear combinations of them. Theoretically, the time complexity of sieving algorithms is only exponential, so better than for enumeration. However, their current implementation is still very immature and also requires exponential memory to build the list of lattice vectors.

Even if enumeration is more efficient in practice nowadays, this can change in the future years as sieving could benefit from quantum acceleration and improve its current implementation approaching the better theoretical time complexity. Indeed, let us observe that, given a list \mathcal{L} of lattice vectors, finding short vectors in it involves searching in \mathcal{L} . This process, required in sieving methods, could somehow benefit from Grover's search algorithm [6]. Note that Grover's quantum search algorithm provides at most quadratic speed-up, thus the practical performance gain must be experimentally assessed. This is an already known issue [8, 2], and thus it is usual to consider that BKZ could benefit from quantum acceleration as well [1].

4 Contribution and Future work

Even if previous theoretical works [8] have suggested significant asymptotic improvements using quantum search for sieving-based lattice algorithms, it is still difficult to know if it actually improves it, or even at what extent does it accelerate in practice. Although there has been a huge development on quantum computation in the recent years, there are no results in the literature which show implementations on quantum accelerated sieving primitives yet.

This is the gap we aim to cover in this work. Even if it still a work in progress, we seek for implementing a quantum search algorithm that allows to find short lattice vectors in a given list. The implementation will be performed using QRISP [15], a state-of-the-art Python module that allows to abstract from the low-level quantum executions, facilitating quantum algorithm implementation. As a result, we expect to prove that this quantum search is feasible nowadays, starting with very low-dimensional lattices.

To the best of our knowledge, our research represents one of the first attempts to experimentally demonstrate quantum speed-ups in lattice sieving algorithms using a contemporary quantum computing framework. Understanding the real-world quantum acceleration achievable for lattice algorithms is crucial for accurately assessing the security parameters in post-quantum cryptographic schemes.

5 Acknowledgments

This research was funded by the Commission of the European Communities HORIZON under QUIET project, awarded from a first open call of PQ-REACT project (Grant Agreement No. 101119547).

References

1. Albrecht, M., Chase, M., Chen, H., Ding, J., Goldwasser, S., Gorbunov, S., Halevi, S., Hoffstein, J., Laine, K., Lauter, K., Lokam, S., Micciancio, D., Moody, D., Morrison, T., Sahai, A., Vaikuntanathan, V.: Homomorphic encryption security standard. Tech. rep., HomomorphicEncryption.org, Toronto, Canada (November 2018)

2. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key {Exchange—A} new hope. In: 25th USENIX Security Symposium (USENIX Security 16). pp. 327–343 (2016)
3. Bi, L., Lu, X., Luo, J., Wang, K., Zhang, Z.: Hybrid dual attack on lwe with arbitrary secrets. *Cybersecurity* **5**(1), 15 (2022)
4. Chen, Y., Nguyen, P.Q.: Bkz 2.0: Better lattice security estimates. In: Lee, D.H., Wang, X. (eds.) *Advances in Cryptology – ASIACRYPT 2011*. pp. 1–20. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
5. Gama, N., Nguyen, P.Q.: Finding short lattice vectors within mordell’s inequality. In: *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*. p. 207–216. STOC ’08, Association for Computing Machinery, New York, NY, USA (2008). <https://doi.org/10.1145/1374376.1374408>, <https://doi.org/10.1145/1374376.1374408>
6. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC ’96*. pp. 212–219. ACM Press, New York, New York, USA (1996). <https://doi.org/10.1145/237814.237866>
7. Korkine, A., Zolotareff, G.: Sur les formes quadratiques. *Mathematische Annalen* **6**(3), 366–389 (1873)
8. Laarhoven, T., Mosca, M., Van De Pol, J.: Finding shortest lattice vectors faster using quantum search. *Designs, Codes and Cryptography* **77**, 375–400 (2015)
9. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. *Mathematische Annalen* **261**(4), 515–534 (Dec 1982). <https://doi.org/10.1007/BF01457454>, <http://link.springer.com/10.1007/BF01457454>
10. Lyubashevsky, V.: Basic lattice cryptography: The concepts behind kyber (ML-KEM) and dilithium (ML-DSA). *Cryptology ePrint Archive*, Paper 2024/1287 (2024), <https://eprint.iacr.org/2024/1287>
11. Micciancio, D., Goldwasser, S.: Shortest vector problem. In: *Complexity of Lattice Problems: A Cryptographic Perspective*, pp. 69–90. Springer (2002)
12. NIST: NIST Releases First 3 Finalized Post-Quantum Encryption Standards (8 2024)
13. Peikert, C.: A decade of lattice cryptography. *Cryptology ePrint Archive*, Paper 2015/939 (2015), <https://eprint.iacr.org/2015/939>
14. Schmidt, E.: Zur Theorie der linearen und nichtlinearen Integralgleichungen I. Teil: Entwicklung willkürlicher Funktionen nach Systemen vorgeschriebener. *Mathematische Annalen* pp. 433–476 (1907)
15. Seidel, R., Bock, S., Zander, R., Petrič, M., Steinmann, N., Tcholtchev, N., Hauswirth, M.: Qrisp: A Framework for Compilable High-Level Programming of Gate-Based Quantum Computers (Jun 2024). <https://doi.org/10.48550/arXiv.2406.14792>, <http://arxiv.org/abs/2406.14792>, arXiv:2406.14792 [quant-ph]