© INNOVATIVE RESEARCH THOUGHTS
Refereed | Peer Reviewed | Indexed
ISSN : 2454 – 308X | Volume : 09 , Issue : 04 | July - September 2023

DOI : https://doi.org/10.36676/irt.2023-v9i4-024

Key exchange protocol under Ding reconciliation scheme in Lattice-based cryptography

Sonam Yadav
Department of Mathematics,
Shree Guru Gobind Singh Tricentenary University, Gurugram, Haryana
Gmail: sonamyadav20jan@gmail.com

Abstract

The Ding Reconciliation Scheme is dissected in detail in this study. A recently proposed method within the lattice-based cryptography framework. The study delves into the mathematical foundations and principles of the scheme, its role in secure key exchange, and its in-depth examination of the key exchange protocol that leverages it. It discusses theoretical security guarantees, vulnerabilities, and mitigation strategies. The paper also provides insights into the practical implementation of the scheme, highlighting its computational efficiency and performance evaluations. It also conducts a comparative analysis with other prominent lattice-based key exchange protocols to assess its strengths and weaknesses, highlighting potential advantages and areas for further research. The paper serves as a reference for researchers, cryptographers, and practitioners interested in the Ding Reconciliation Scheme and its applications in lattice-based cryptography, contributing to the ongoing dialogue in the field and promoting advancements in secure communication solutions.

Keywords: Lattice-Based Cryptography, Ding Reconciliation Scheme, Key Exchange Protocol, Cryptographic Reconciliation, Secure Communication, Security Guarantees

Introduction

Lattice-based cryptography is a game-changing paradigm in contemporary cryptography, especially in light of the challenges posed by quantum computers. The Ding Reconciliation Scheme is an innovative method of implementing safe key exchange within the context of communication security protocols. The approach uses lattices to make exchanging keys more efficient and give cryptographic resistance against quantum attackers. It is the assumption hardness of foundational problems in this area, such as the Learning With Errors (LWE) problem, that gives lattice-based cryptography its strength. The Ding Reconciliation Scheme is a flexible and secure key exchange protocol that makes use of LWE and related lattice problems. The mathematical complexities of lattice theory are the backbone of security in lattice-based systems and must be grasped in order to understand their basis. In this in-depth review, we look at the inner workings, security assurances, and real-world ramifications of the Ding Reconciliation Scheme. It zeroes in on the key exchange protocol, explaining how two people can securely exchange secret information without giving away their identities to prying eyes. The resilience of the scheme against various attack vectors is tested, and security is an overarching theme throughout the investigation. In this in-depth look into the Ding Reconciliation Scheme, we focus on its auctionability and efficiency, two of the most pressing issues in contemporary cryptography. To better understand the benefits and drawbacks of the scheme, it can be compared to other prominent lattice-based key exchange protocols. The Ding Reconciliation Scheme is a prime example of the ever-changing landscape of cryptographic research, which is where theoretical underpinnings and real-world security needs meet and mingle. It's proof that lattice-based encryption can keep up with changing threats and new technologies. This research not only deepens our familiarity with cryptographic

DOI : https://doi.org/10.36676/irt.2023-v9i4-024

protocols, but also adds to the ongoing discussion about how best to ensure confidential digital exchanges.

Ding Reconciliation Scheme

The Ding Reconciliation Scheme represents a pivotal advancement within the landscape of lattice-based cryptography, offering innovative solutions to the increasingly pressing challenges of secure key exchange in an era marked by evolving threats, including the potential advent of quantum computing. At its core, this scheme capitalizes on the deep mathematical foundations of lattice theory, particularly the LWE issue, which is fundamental to the concept of security in lattice-based systems. By harnessing the inherent computational complexity of lattice problems, the Ding Reconciliation Scheme provides a robust foundation for cryptographic resilience against quantum adversaries. Key to its functionality is its role in facilitating secure key exchange, a fundamental pillar of cryptographic communication. In practical terms, the scheme enables two parties to establish a shared secret key over potentially insecure channels while thwarting eavesdroppers and malicious actors. Understanding the inner workings of this scheme necessitates an exploration of its key exchange protocol, wherein we unravel the intricacies of key generation, exchange, and cryptographic operations. Security, a paramount concern in cryptographic research, permeates our analysis, where we scrutinize the security assumptions, the scheme's theoretical resilience against various attack vectors, and potential vulnerabilities, all while offering strategies for mitigation. Moreover, the Ding Reconciliation Scheme does not reside solely in the realm of theory; it extends into the practical domain, where efficiency and implement ability become critical factors. Therefore, our examination delves into the computational costs and performance considerations associated with its deployment, offering insights into its viability in real-world cryptographic applications. The landscape of cryptography is ever-evolving, and no cryptographic scheme exists in isolation. To place the Ding Reconciliation Scheme within its broader context, we embark on a comparative analysis, juxtaposing it against other prominent lattice-based key exchange protocols. This comparative lens unveils the scheme's unique strengths and potential weaknesses, facilitating a nuanced understanding of its significance within the realm of lattice-based cryptographic solutions. In sum, the Ding Reconciliation Scheme emerges as a dynamic and adaptable cryptographic paradigm that bridges the gap between mathematical theory and practical security concerns, ultimately contributing to the ongoing discourse on secure communication solutions in a rapidly evolving digital landscape.

Key Exchange Protocol

To ensure confidential communications via unsecured channels, current cryptography relies on a key exchange system. The fundamental goal of this system is to enable two people, Alice and Bob, to create a secret key that can be used to encrypt and decode communications between them. Confidentiality and integrity. This process typically unfolds in several well-defined steps, commencing with key generation. During this phase, Alice and Bob independently generate their respective cryptographic keys, which may include public and private key pairs, depending on the protocol. These keys are derived using complex mathematical algorithms and are chosen to be computationally challenging to reverse-engineer. Once generated, the keys are exchanged between the parties, often accompanied by additional information, which may include random values, nonces, or ephemeral keys. The exchange itself can occur through various methods, such as direct communication, public key infrastructure (PKI), or secure channels like TLS/SSL. Subsequently, the received information is used to derive a shared secret key that is known only to Alice and Bob, typically through a mathematical process that combines their

DOI : https://doi.org/10.36676/irt.2023-v9i4-024

private keys and exchanged data. It is essential to emphasize that an eavesdropper, often referred to as Eve, may attempt to intercept or manipulate the exchanged data during this process. Therefore, the security of the key exchange protocol hinges on its ability to resist various attacks and ensure that Eve cannot deduce the shared secret key, even if she has access to all the exchanged information. To this end, protocols employ various cryptographic techniques, such as the Diffie-Hellman key exchange, elliptic curve cryptography, or lattice-based cryptography, each with its unique set of security assumptions and computational complexity. Moreover, key exchange protocols often integrate additional security features, such as forward secrecy, which ensures that compromising one session's key does not compromise past or future sessions, and post-quantum resistance, which safeguards against attacks by quantum computers. In conclusion, a key exchange protocol represents a critical component of secure communications, bridging the gap between theoretical cryptography and practical security, while navigating the intricate balance between complexity, efficiency, and resilience to attacks in an ever-evolving threat landscape.

Secure Communication

Information privacy is of utmost importance in today's highly linked society, thus secure communication is crucial. Digital information security is the multifaceted effort to keep data private, legitimate, and unaltered while it travels from one location to another online. The primary goal of secure communication is to prevent unauthorised parties from gaining access to sensitive information online by thwarting eavesdroppers, malicious actors, and other online risks. Cryptographic methods provide the foundation for this endeavour, as they provide the mathematical instruments and algorithms necessary to encode and decode information in a manner that makes it unintelligible to third parties. While encryption techniques turn plaintext into unreadable ciphertext, key exchange protocols allow for the safe transfer of cryptographic keys, allowing parties to set up secret communication channels. Digital signatures allow for the confirmation of a message's and its sender's identities. Bolstering trust in digital interactions. Secure communication extends beyond cryptographic mechanisms, encompassing secure network protocols, secure software development practices, access controls, and secure hardware implementations. Moreover, it responds dynamically to emerging threats, adapting to technological advancements, from quantum-resistant cryptography to advanced threat detection mechanisms. In a world where digital data is the lifeblood of our societies, economies, and personal lives, secure communication is not just a technological imperative but a fundamental human right. It underpins online banking, e-commerce, healthcare, government services, and the broader digital infrastructure that powers our modern existence. As we navigate an ever-evolving threat landscape, secure communication continues to evolve, offering a resilient shield against cyberattacks, data breaches, and privacy infringements. In this pursuit of security, it embodies not just the realm of technology but also legal and ethical considerations, striving to strike the delicate balance between privacy, national security, and individual freedoms. Secure communication, in all its complexity and importance, remains the guardian of the digital realm, ensuring that the benefits of the interconnected world are enjoyed without compromising the safety and privacy of individuals and organizations alike.

Security Guarantees

Cryptography security guarantees are the foundation of trust, privacy, and integrity in digital communication. They are based on mathematical and computational complexity and serve as the cornerstone of secure systems in an ever-evolving threat landscape. These guarantees ensure that cryptographic protocols and primitives are resilient to various forms of attacks, ensuring that sensitive information remains confidential, unaltered, and accessible only to authorized parties. Theoretical foundations of these guarantees often hinge on the presumed intractability of certain challenges in mathematics, such as calculating discrete logarithms in finite fields or factoring huge semiprime integers. These issues are purposefully made to be computationally challenging, so that they might test your patience and resources. The idea that attackers, even with substantial computer capacity, cannot possibly crack the cryptographic system within a reasonable timescale is the basis for security assurances. Public-key encryption, digital signatures, key exchange, and other cryptographic primitives and protocols are all covered by the security guarantees. Cryptographic researchers have established rigorous security definitions for each of these primitives, outlining the properties and protections they afford. However, security guarantees are not uniform across all cryptographic systems, as they vary depending on the specific cryptographic primitive, the mathematical foundation it relies upon, and the assumptions about the computational capabilities of potential adversaries. The practicality and effectiveness of security guarantees are inherently tied to real-world implementation, including factors like key management, secure random number generation, side-channel attacks, and secure software and hardware implementation. Additionally, the human element, encompassing user behavior and adherence to security best practices, plays a critical role in the overall security posture. security guarantees in cryptography serve as the linchpin of trust and privacy in our digital age. They are the result of meticulous mathematical and computational analysis, providing assurances that sensitive information remains confidential, unaltered, and accessible only to authorized parties. As we navigate the complex terrain of cybersecurity, these guarantees remind us that, even in an era of advanced technology and sophisticated adversaries, the principles of cryptography continue to safeguard the digital world.

Lattice-Based Cryptography

As a breakthrough paradigm in the world of contemporary cryptography, lattice-based encryption has received widespread attention and recognition for its exceptional resistance to quantum assaults. The foundation of this cryptographic method is the notion of lattices in mathematics, which broadly accepts complicated mathematical structures constructed by linear equations. Lattice-based cryptography relies on a solution to the Learning With Errors (LWE) issue, which serves as the framework's primary source of security. Lattice-based techniques provide a secure and tried alternative to other encryption systems that are sensitive to quantum algorithms like Shor's algorithm. Public-key encryption, digital signatures, and key exchange protocols are only some of the cryptographic primitives that may be provided by lattice-based cryptography. These primitives are designed to operate in the presence of adversaries equipped with powerful quantum computers, thereby ensuring long-term security for digital communication in the post-quantum era. In practice, lattice-based cryptographic schemes have demonstrated both theoretical strength and practical viability, gaining recognition as promising candidates for securing sensitive data in a world where quantum computing capabilities are on the horizon. The ongoing development and standardization efforts within the cryptographic community further underscore the significance of lattice-based cryptography in safeguarding the confidentiality and integrity of digital communications against the ever-evolving landscape of advanced threats. As we delve deeper into this multifaceted cryptographic paradigm, we unveil its mathematical intricacies, cryptographic primitives, security guarantees, and the promise it holds for a secure digital future. In a time when security is paramount in the digital age, lattice-based cryptography emerges as a beacon of resilience, offering mathematical elegance and practicality in equal measure, setting the stage for a new era of cryptographic innovation and protection.

DOI : https://doi.org/10.36676/irt.2023-v9i4-024

Post-Quantum Cryptography

Post-quantum cryptography is a rapidly growing field in cryptographic research that aims to protect the digital world from the potential of quantum computing. It aims to redefine cryptographic primitives and algorithms that have been the foundation of secure digital communication, embracing mathematical constructs and problems that have demonstrated resilience against quantum attacks. The field encompasses various cryptographic primitives, such as lattice-based, code-based, hash-based, and multivariate polynomial cryptography, each with unique strengths and weaknesses. The goal is to develop new public-key encryption schemes, digital signature algorithms, and key exchange protocols that can withstand the computational might of quantum adversaries. The practicality and efficiency of these post-quantum cryptographic schemes must be paramount, as they must seamlessly integrate into existing digital infrastructures without burdening computational resources. Standardization efforts by organizations like NIST emphasize the urgency of developing post-quantum cryptographic solutions that can be easily adopted in various applications, such as securing online communications, financial transactions, and safeguarding critical infrastructure and sensitive data. As quantum computers approach practicality, the transition from classical to quantum-resistant cryptographic systems becomes increasingly urgent. Advancements in post-quantum cryptography are not just a scientific endeavor but a moral and strategic imperative, ensuring the digital future remains secure and resilient in the face of the quantum threat. Collaboration among cryptographers, mathematicians, engineers, policymakers, and industry stakeholders is crucial for the transition to post-quantum cryptography.

Review of literature

(Alkim et al., n.d.) studied "New Hope without reconciliation" and said that We provide a simple way to convert Ring-LWE encryption into a Key Exchange Module (KEM) that may be utilised in a passively secure environment using New Hope-Simple, a variation of the New Hope Riegle-based key exchange system (or key-exchange scheme). The primary benefit of NewHopeSimple over New Hope is its ease of usage. In particular, it does away with Ding's recommended approach to conflict resolution. His approach, along with some other tactics like unbiasing the key after Peikert's adjustment and utilising the quantizer D4 to extract one key bit from several coefficients, is described in depth throughout more than three pages of the New Hope article.

(Choi et al., n.d.) studied "Constant-round Dynamic Group Key Exchange from RLWE Assumption" and said that This study introduces a novel group key exchange method that makes use of a dynamic membership lattice. We construct our protocol by generalising the Dutta-Barua protocol to the RLWE case, based on the work of Apon et al. from the most current issue of PQCrypto 2019, published in March 2019. We provide an improvement to third round and calculation phase of the group key exchange protocol described in the publication by Apon et al. We then provide an authenticated and secure protocol for dynamic group key exchange, complete with Join and Leave algorithms. An authorised group key exchange takes the same number of rounds as an unauthenticated one. The total number of rounds will remain constant regardless of the size of the group since our technique is scalable. For unauthenticated dynamic group key exchange protocols, we provide a comprehensive demonstration of security under the assumptions of the hardness of the RLWE assumption and the verifiability of digital signatures.

(Nejatollahi et al., n.d.) studied "Software and Hardware Implementation of Lattice-based Cryptography Schemes" and said that The threat presented by Public key cryptography has developed post-quantum encryption primitives and protocols in response to the threat posed by quantum computers. Lattice-based encryption is a subset of post-quantum cryptography. Has a lot of potential

DOI : https://doi.org/10.36676/irt.2023-v9i4-024

for addressing both long-standing and cutting-edge security concerns. However, it requires careful design considerations and trade-offs to be implemented on today's computer platforms, since there is a large range of hardware configurations and the market demands change quickly. This research takes a look at where lattice-based cryptographic algorithms are at the moment, what they may be used for, what's new, and how difficult they are to implement in software and hardware. This study's overarching goal is to provide some mathematical insight on the processes involved in mapping systems onto general-purpose hardware and synthesising techniques for specialised hardware.

(Yang & Ma, n.d.) studied “Two-party authenticated key exchange protocol using lattice-based cryptography” and said that For the aim of ensuring future communication between communicative entities operating over an unsecured network, the A fundamental building block of cryptography is the Authenticated Key Exchange (AKE) protocol. Primitives of lattice-based encryption are believed to be robust against quantum computer assaults. Using a reduced module over ideal lattices, we build a high-performance AKE protocol that outperforms the original Diffie-Hellman protocol. In the Bellare-Rog away model, we prove the proposed protocol safe under the strong assumption of ring learning with errors, and we also establish wPFS (RLWE).

(Bos et al., 2015) studied “Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem” and said that Protected against quantum-computer-based assaults are cryptographic primitives based on lattices. To demonstrate how post-quantum key exchange might be included into the design of ciphersuites for the Transport Layer Security (TLS) standard, we utilise the ring learning with errors (R-LWE) issue as an example. Combining the tried-and-true authentication methods of RSA or elliptic curve digital signatures with lattice-based key exchange, this technique ensures forward secrecy against possible quantum attackers. In light of the low cost of the 128-bit security-focused cryptographic solution, it seems reasonable to abandon unsecure key exchange in light of the threat posed by quantum computers. The speed of a 2-core desktop workstation can be improved by 21% with the addition of R-LWE ciphersuites to the OpenSSL library and the Apache web server, and the size of the handshake can be decreased by 8 KiB for a 10 KiB payload.

(Ravi et al., 2020) studied “Generic Side-channel attacks on CCA-secure lattice-based PKE and KEMs” and said that This study demonstrates the feasibility and generality of EM side-channel assisted selected ciphertext assaults in the chosen ciphertext paradigm, which may be used to break many different types of Key encapsulation mechanisms (KEM) and Public Key Encryption (PKE) using LWE/LWR (IND-CCA security). Insight into the binary decryption result may be gained by using the EM side-channel data to construct a plaintext checking oracle. The researchers found flaws in error-correcting codes (ECC) and the Fujisaki-Okamoto transform, which allowed previously encrypted information to be deciphered. During the second phase of NIST standardisation, they take use of these flaws to launch attacks against six CCA-secure lattice-based PKE/KEMs. Key recovery for all targeted schemes was shown to be possible in a few of minutes using implementations extracted from the open-source pqm4 library on the ARM Cortex-M4 microcontroller.

(Abla, 2021) studied “Lattice Based Group Key Exchange Protocol in the Standard Model” and said that Members of a group may reach consensus on a session key via a group key exchange technique. Despite the extensive literature on the topic, most group key exchange systems rely on algebraic problems that can be solved by quantum algorithms in polynomial time. Few articles have explored lattice-based group key exchange techniques despite its post-quantum security (at least in the random oracle paradigm).

(Seyhan et al., 2021) studied “Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security” and said that Using bilateral generalisation inhomogeneous short integer solution (Bi-

DOI : https://doi.org/10.36676/irt.2023-v9i4-024

GISIS), we provide a novel key exchange protocol for post-quantum Internet of Things security that makes use of a reusable key feature. The goal is to hasten the process of producing keys for use in IoT device key exchange protocols. We develop modified bilateral pasteurisation within the context of the random oracle model to get a reusable key. It is more probable that the same key may be used in multiple implementations of the proposed protocol if the key can be used more than once. With this enhancement, IoT systems that operate on limited means will be able to effectively recycle keys. The suggested approach is well suited for quantum-safe key exchange in a fog computing setting with D2D communication. We design a safe method of key management and implement it into a D2D key exchange protocol.

(Akleylek & Seyhan, 2022) studied "Module learning with rounding based key agreement scheme with modified reconciliation" and said that By adapting the reconciliation technique to get a shared key, we offer a presumably secure key agreement approach based on the MLWR issue. The error probability is also low when compared to other methods with the same attributes. Against a passive opponent, a thorough security analysis is offered. Then, a programme is tweaked such that it can provide a set of parameters suitable for any degree of protection. The prices of both primary and secondary attacks are determined. In order to reduce the mistake probability and bandwidth required to reach an agreement, this research modifies an existing reconciliation procedure to reach a consensus.

(Choudhary & Gupta, 2022) studied "Hybrid KE: A forward-secure non-interactive quantum-safe hybrid key exchange scheme" and said that In this paper, we present a novel method of key exchange and encryption called Hybrid KE that is both quantum-safe and conventionally secure. Key establishment may occur in parallel without the requirement for reconciliation; this is made possible by the non-interactive nature of the protocol, which is based on the symmetric-key approach used in the Advanced Encryption Standard. Hybrid KE additionally includes forward secrecy and authenticated quantum-safe communication without decryption failure. Unlike previous research, this one use both classical and quantum methods to create a safe kind of key exchange known as a hybrid key. In this paper, the authors provide a practical implementation of the Hybrid KE and the sets of parameters that it accepts, after rigorously testing and investigating the scheme's security against different attacks.

Public-Key Cryptography

The development of public-key cryptography was a major step forward in the security of digital communications and private data. A public key is available to the public and may be verified by anybody, whereas a private key is solely known to its owner. By allowing covert communication between persons that have never shared a secret before, this method delivers an unparalleled degree of security. Factoring big semiprime integers and calculating discrete logarithms in finite fields are two examples of the kinds of mathematically challenging issues that form the basis of this cryptographic miracle. These mathematical hurdles are the backbone of public-key cryptography's security. Secure electronic communication and cryptographic applications like digital signatures for document verification, online banking, and online purchases are all possible now thanks to public-key cryptography (VPNs). Public-key encryption techniques, digital signature algorithms, and key exchange protocols are only some of the cryptographic primitives that have arisen as a result of the development of this cryptographic paradigm. Since different applications have different security needs, many primitives are available to meet those demands. The security of public-key cryptography, however, is threatened by the intractable nature of certain mathematical problems. Cryptographic systems that depend on the computational challenge of factoring big numbers or solving discrete logarithm issues face an imminent threat from quantum computers. Because of this, post-quantum

DOI : https://doi.org/10.36676/irt.2023-v9i4-024

cryptography has emerged as a field of study, with the goal of creating cryptographic algorithms and protocols that can withstand the effects of quantum computing.

Conclusion

The Ding Reconciliation Scheme is a key exchange protocol that attempts to link the worlds of mathematics with computer security. It uses the computational complexity of lattice issues to give a solid basis for cryptographic resistance against quantum adversaries, and it is based on lattice theory, in particular the Learning with Errors (LWE) problem. To create a shared secret key between two parties, the system permits safe key exchange, a crucial component of cryptographic communication. While thwarting eavesdroppers and malicious actors. The scheme's security assumptions, theoretical resilience against attack vectors, and potential vulnerabilities were scrutinized, along with mitigation strategies. The scheme's practicality was also examined, providing insights into computational costs and performance considerations, offering guidance on its viability in real-world cryptographic applications. The scheme's significance lies in its dynamic and adaptable nature, serving as a dynamic and adaptable cryptographic paradigm that bridges the gap between mathematical theory and practical security concerns. It contributes to the ongoing discourse on secure communication solutions in a rapidly evolving digital landscape, underscoring the importance of cryptographic research in safeguarding the confidentiality and integrity of digital communications.

Reference

1. Abla, P. (2021). Lattice Based Group Key Exchange Protocol in the Standard Model. *Computer Science & Information Technology (CS & IT)*, 157–174. https://doi.org/10.5121/csit.2021.111113
2. Akleylek, S., & Seyhan, K. (2022). Module learning with rounding based key agreement scheme with modified reconciliation. *Computer Standards & Interfaces*, *79*, 103549. https://doi.org/10.1016/j.csi.2021.103549
3. Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (n.d.). *NewHope without reconciliation*.
4. Bos, J. W., Costello, C., Naehrig, M., & Stebila, D. (2015). Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem. *2015 IEEE Symposium on Security and Privacy*, 553–570. https://doi.org/10.1109/SP.2015.40
5. Choi, R., Hong, D., & Kim, K. (n.d.). *Constant-round Dynamic Group Key Exchange from RLWE Assumption*.
6. Choudhary, S., & Gupta, A. (2022). HybridPKE: A forward-secure non-interactive quantum-safe hybrid key exchange scheme. *Engineering Science and Technology, an International Journal*, *34*, 101094. https://doi.org/10.1016/j.jestch.2022.101094
7. Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (n.d.). *Software and Hardware Implementation of Lattice-based Cryptography Schemes*.
8. Ravi, P., Sinha Roy, S., Chattopadhyay, A., & Bhasin, S. (2020). Generic Side-channel attacks on CCA-secure lattice-based PKE and KEMs. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 307–335. https://doi.org/10.46586/tches.v2020.i3.307-335
9. Seyhan, K., Nguyen, T. N., Akleylek, S., Cengiz, K., & Islam, S. K. H. (2021). Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security. *Journal of Information Security and Applications*, *58*, 102788. https://doi.org/10.1016/j.jisa.2021.102788
10. Yang, X., & Ma, W. (n.d.). *Two-party authenticated key exchange protocol using lattice-based cryptography*.