




Proceeding Paper

Secure and Efficient Code-Based Cryptography for Multi-Party Computation and Digital Signatures[†]

Abdellatif Kichna *  and Abderrazak Farchane

Laboratory of Innovation in Mathematics Applications & Information Technologies, Department of Mathematics and Informatics, Sultane Moulay Slimane University, Beni Mellal 23000, Morocco; a.farchane@gmail.com

* Correspondence: abdellatif.kichna@usms.ac.ma

† Presented at the 3rd International Day on Computer Science and Applied Mathematics, Errachidia, Morocco, 13 May 2023.

Abstract: Code-based cryptography is a promising candidate for post-quantum cryptography due to its strong security guarantees and efficient implementations. In this paper, we explore the use of code-based cryptography for multi-party computation and digital signatures, two important cryptographic applications. We present several efficient and secure code-based protocols for these applications, based on the McEliece cryptosystem and its variants. Our protocols offer strong security guarantees against both classical and quantum attacks, and have competitive performance compared to other post-quantum cryptographic schemes. We also compare code-based cryptography with other post-quantum schemes, including lattice-based and hash-based cryptography, and discuss the advantages and disadvantages of each approach.

Keywords: code-based cryptography; post-quantum cryptography; multi-party computation; digital signatures; McEliece cryptosystem

1. Introduction

Code-based cryptography is a well-established field of research that aims to design cryptographic schemes based on the properties of error-correcting codes. Code-based cryptography offers strong security guarantees against classical and quantum attacks, making it an attractive alternative to traditional cryptographic schemes that rely on mathematical assumptions that may be broken by future advances in computing [1]. Code-based cryptography has been studied for several decades, and numerous efficient and secure schemes have been proposed for various cryptographic tasks, including encryption, digital signatures, and multi-party computation.

Digital signatures and multi-party computation are two fundamental cryptographic tasks that have numerous applications in modern communication systems. Digital signatures provide a means for users to authenticate their identities and verify the integrity of digital documents. Multi-party computation refers to a cryptographic technique that enables multiple parties to collaborate and compute a function without revealing their individual inputs to each other, enabling secure collaborative computing in various scenarios. However, both tasks are computationally intensive and require the use of sophisticated cryptographic techniques to ensure their security and efficiency.

The motivation for using code-based cryptography in digital signatures and multi-party computation stems from the increasing threat of quantum computing to the security of traditional cryptographic schemes [1]. Quantum computers can efficiently solve several hard problems that form the basis of modern cryptography, including factoring and discrete logarithm problems. As a result, many traditional cryptographic schemes are vulnerable to attacks by quantum computers. Code-based cryptography, on the other hand, relies on different mathematical assumptions that are believed to be secure even against quantum



Citation: Kichna, A.; Farchane, A. Secure and Efficient Code-Based Cryptography for Multi-Party Computation and Digital Signatures. *Comput. Sci. Math. Forum* **2023**, *6*, 1. <https://doi.org/10.3390/cmsf2023006001>

Academic Editors: Abdeslam Jakimi and Mohamed Oualla

Published: 26 May 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

attacks. Therefore, code-based cryptography is a potential solution for post-quantum cryptography that shows promise in providing strong security guarantees against classical and quantum attacks [2], and its potential applications in digital signatures and multi-party computation are currently being actively explored.

This paper is organized as follows. In Section 2, we provide an introduction to code-based cryptography and digital signatures, as well as its security properties. In Section 3, we discuss the motivation and background for using code-based cryptography in multi-party computation. In Section 4, we compare code-based cryptography with other post-quantum cryptographic schemes, including lattice-based and hash-based cryptography. Finally, we discuss the implications of our findings for future research in the field of code-based cryptography.

2. Code-Based Cryptography for Digital Signatures

2.1. Review of Existing Digital Signature Schemes

Digital signature schemes play a crucial role in ensuring the authenticity, integrity, and non-repudiation of digital documents [3]. In this section, we review the existing digital signature schemes that are based on code-based cryptography. These schemes include the McEliece, Niederreiter, and CFS digital signature schemes, which were proposed in the 1990s and early 2000s [4].

2.2. Advantages of Code-Based Cryptography for Digital Signatures

Code-based cryptography offers several advantages for digital signatures [5]. Firstly, it offers strong security guarantees against both classical and quantum attacks. Secondly, it provides a high level of flexibility in terms of key size and algorithmic design. Thirdly, it is based on well-understood mathematical problems that are believed to be secure even in the post-quantum era.

2.3. Construction and Implementation of Code-Based Digital Signature Schemes

Code-based digital signature schemes are constructed using error-correcting codes and other algebraic structures. These schemes typically involve the use of hash functions, secret keys, and public keys, which are generated using specific algorithms. Implementation of these schemes requires careful consideration of the underlying algorithms and their security properties, as well as efficient techniques for key generation, signing, and verification [6].

2.4. Evaluation of Security and Efficiency of Code-Based Digital Signatures

The security and efficiency of code-based digital signature schemes have been extensively studied in the literature. These schemes are generally considered to offer high levels of security against both classical and quantum attacks. However, they also have some drawbacks in terms of key size and computational complexity, which may limit their practical applications in certain scenarios [7]. Therefore, the evaluation of code-based digital signature schemes requires a careful analysis of their security and efficiency properties, as well as their suitability for different applications.

3. Code-Based Cryptography for Multi-Party Computation

3.1. Overview of Multi-Party Computation

Multi-party computation, commonly referred to as MPC, is a cryptographic approach that enables a group of participants to collaboratively perform a computation on their respective private inputs without disclosing them to one another. MPC is a powerful tool for secure collaborative computing in various scenarios, such as electronic voting, auctions, and privacy-preserving data analysis [8]. MPC protocols typically involve a set of n parties, each holding a private input x_i , and aim to compute a function $f(x_1, x_2, \dots, x_n)$ in a way that preserves the privacy of the inputs.

3.2. Review of Existing Multi-Party Computation Schemes

There are several MPC schemes that have been proposed in the literature, including secret sharing-based schemes [9], garbled circuit-based schemes [10], and homomorphic encryption-based schemes [11]. Each scheme has its own strengths and weaknesses in terms of security, efficiency, and applicability; however, all existing MPC schemes are vulnerable to attacks by quantum computers, which can break the underlying mathematical assumptions and compromise the security of the protocols.

3.3. Advantages of Code-Based Cryptography for Multi-Party Computation

Code-based cryptography offers several advantages for MPC over traditional cryptographic schemes. First, code-based MPC schemes are based on different mathematical assumptions than traditional schemes, which are believed to be secure even against quantum attacks. Second, code-based MPC schemes are typically simpler and more efficient than traditional schemes, which can reduce the computational overhead and improve the scalability of MPC. Third, code-based MPC schemes can be implemented using existing error-correcting codes, which have been extensively studied and optimized over several decades.

3.4. Construction and Implementation of Code-Based Multi-Party Computation Schemes

Several code-based MPC schemes have been proposed in the literature, including variants of the McEliece and Niederreiter cryptosystems. Code-based MPC schemes typically involve encoding the private inputs of the parties using error-correcting codes, computing the function over the encoded inputs, and decoding the output using error-correcting codes. The encoding and decoding operations are typically performed using efficient algorithms that exploit the structure of the codes.

3.5. Evaluation of Security and Efficiency of Code-Based Multi-Party Computation

The security and efficiency of code-based MPC schemes depend on several factors, such as the choice of error-correcting codes, the complexity of the function being computed, and the number of parties involved. Code-based MPC schemes can achieve comparable or even better security and efficiency than traditional MPC schemes, while being more resilient to attacks by quantum computers. However, there are also some challenges associated with code-based MPC, such as the vulnerability of the codes to side-channel attacks and the difficulty of achieving information-theoretic security.

4. Comparison with Other Post-Quantum Cryptographic Schemes

Code-based cryptography is one of the leading candidates for post-quantum cryptography due to its strong security guarantees and efficient implementations. However, it is important to compare code-based cryptography with other post-quantum cryptographic schemes to evaluate its strengths and weaknesses. In this section, we will compare code-based cryptography with lattice-based schemes, hash-based schemes, and other code-based schemes.

4.1. Comparison with Lattice-Based Schemes

Lattice-based cryptography is another promising candidate for post-quantum cryptography. Lattice-based schemes are based on the hardness of certain problems in lattice theory, such as the shortest vector problem (SVP) and the closest vector problem (CVP) [12]. Like code-based cryptography, lattice-based cryptography offers strong security guarantees against both classical and quantum attacks. However, lattice-based cryptography has some disadvantages compared to code-based cryptography.

First, lattice-based cryptography requires larger key sizes than code-based cryptography to achieve the same level of security. This is because the security of lattice-based schemes depends on the size of the underlying lattice, which needs to be sufficiently large to resist attacks. Second, lattice-based cryptography is more computationally intensive

than code-based cryptography, which can lead to slower implementations. Finally, lattice-based cryptography is still a relatively new field of research compared to code-based cryptography, which has been studied for several decades.

4.2. Comparison with Hash-Based Schemes

Hash-based cryptography is another approach to post-quantum cryptography that is based on the properties of cryptographic hash functions. Hash-based schemes are typically faster and more efficient than both lattice-based and code-based schemes [13]. However, hash-based cryptography has some limitations that make it less attractive than code-based cryptography.

One limitation of hash-based cryptography is that it is vulnerable to collision attacks, where an attacker can find two messages that hash to the same value. This can lead to security vulnerabilities in certain scenarios. Another limitation of hash-based cryptography is that it requires trusted setup, which can be difficult to implement in practice.

4.3. Comparison with Other Code-Based Schemes

Code-based cryptography includes several different families of schemes, each with its own strengths and weaknesses. One example is the McEliece cryptosystem, which is based on the hardness of decoding random linear codes. The McEliece cryptosystem has been studied extensively and is known to be secure against both classical and quantum attacks. However, it has some disadvantages compared to other code-based schemes, such as larger key sizes and slower encryption and decryption times.

Another example of code-based cryptography is the Niederreiter cryptosystem [14], which is based on the hardness of computing discrete logarithms in certain finite fields. The Niederreiter cryptosystem has some advantages over the McEliece cryptosystem, such as smaller key sizes and faster encryption and decryption times. However, it is vulnerable to a specific type of attack known as the syndrome decoding attack, which limits its security in certain scenarios.

5. Conclusions

In conclusion, this paper presented an overview of code-based cryptography and its applications in multi-party computation and digital signatures. We discussed the security properties of code-based cryptography, including its resistance to both classical and quantum attacks, as well as its efficiency in terms of key size and computation time. We also reviewed several code-based schemes, including the McEliece cryptosystem, the Niederreiter cryptosystem, and the RQC scheme, and their suitability for multi-party computation and digital signatures.

Future work in this area could include further optimizations of our proposed scheme, as well as exploring the potential of code-based cryptography in other applications, such as homomorphic encryption and secure multiparty computation. Additionally, the security of code-based cryptography against attacks that exploit structural properties of codes, such as the rank metric attack, needs to be further investigated.

Author Contributions: Conceptualization, A.K.; methodology, A.K.; software, A.K.; validation, A.K. and A.F.; formal analysis, A.K.; investigation, A.K.; resources, A.K.; data curation, A.K.; writing—original draft preparation, A.K.; writing—review and editing, A.K.; visualization, A.K.; supervision, A.K. and A.F.; project administration, A.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data have been presented in the main text.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134. [[CrossRef](#)]
2. McEliece, R.J. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *Deep. Space Netw. Prog. Rep.* **1978**, *44*, 114–116.
3. Fang, W.; Chen, W.; Zhang, W.; Pei, J.; Gao, W.; Wang, G. Digital signature scheme for information non-repudiation in blockchain: A state of the art review. *EURASIP J. Wirel. Commun. Netw.* **2020**, *1*, 56. [[CrossRef](#)]
4. Haidary Makoui, F.; Gulliver, T.A.; Dakhilalian, M. A new code-based digital signature based on the McEliece cryptosystem. *IET Commun.* **2023**. [[CrossRef](#)]
5. Kuznetsov, A.; Pushkar'ov, A.; Kiyan, N.; Kuznetsova, T. Code-based electronic digital signature. In Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 24–27 May 2018; pp. 331–336. [[CrossRef](#)]
6. Kuznetsov, A.; Kiian, A.; Babenko, V.; Perevozova, I.; Chepurko, I.; Smirnov, O. New approach to the implementation of post-quantum digital signature scheme. In Proceedings of the 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 14–18 May 2020; pp. 166–171. [[CrossRef](#)]
7. D'Alconzo, G.; Meneghetti, A.; Piasenti, P. Security issues of CFS-like digital signature algorithms. *arXiv* **2021**. [[CrossRef](#)]
8. Raeini, M.G. Selected Applications of MPC. Ph.D. Thesis, Florida Atlantic University, Boca Raton, FL, USA, 2022.
9. Escudero, D. An Introduction to Secret-Sharing-Based Secure Multiparty Computation. *Cryptology ePrint Archive*, **2022**. Paper 2022/062.
10. Heath, D.A. New Directions in Garbled Circuits. Ph.D. Thesis, Georgia Institute of Technology, Atlanta, GA, USA, 2022.
11. Peng, K. Efficient Homomorphic E-Voting Based On Batch Proof Techniques—An Improvement to Secure MPC Application. In Proceedings of the 2022 19th Annual International Conference on Privacy, Security Trust (PST), Fredericton, NB, Canada, 22–24 August 2022; pp. 1–8. [[CrossRef](#)]
12. Micciancio, D.; Regev, O. Lattice-based cryptography. In *Post-Quantum Cryptography*; Bernstein, D.J., Buchmann, J., Dahmen, E., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 147–191. [[CrossRef](#)]
13. Rohde, S.; Eisenbarth, T.; Dahmen, E.; Buchmann, J.; Paar, C. Fast hash-based signatures on constrained devices. In Proceedings of the Smart Card Research and Advanced Applications: 8th IFIP WG 8.8/11.2 International Conference, CARDIS 2008, London, UK, 8–11 September 2008; Proceedings 104–117; Springer: Berlin/Heidelberg, Germany. [[CrossRef](#)]
14. Niederreiter, H. Knapsack-type cryptosystems and algebraic coding theory. *Prob. Contr. Inform. Theory* **1986**, *15*, 157–166.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.