AIJR Preprints
Section: Working Paper
Article Id: 384, Version: 1, 2022
DOI: https://doi.org/10.21467/preprints.384
URL: https://preprints.aijr.org/index.php/ap/preprint/view/384

{Click on above link or DOI to see the latest available version of this article}

NOT PEER-REVIEWED

Version 1: Received: 29 April 2022 / Approved: 01 May 2022 / Online: 02 May 2022

Polynomial Commitment-Based Zero-Knowledge Proof Schemes: A Brief Review

Becky Mundele[1], Chenchen Han[1, 2, 3*]

[1]Advanced Manufacturing and Materials Center, Laramie County Community College

[2]School of Intelligent Engineering, Taishan Institute of Technology

[3]Advanced Machinery Research Institute, Xinghua Hongwei Fluid Equipment

*Corresponding author

ABSTRACT

Blockchain technology is one of the most popular information technologies at present, and its security features are realized through various cryptographic tools. Zero-knowledge proofs are such a tool that can increase data security and improve users' privacy, and zero-knowledge proof schemes constructed with polynomial commitments have advantages in terms of verification time and proof size. Benefiting from the development of blockchain technology, zero-knowledge proof has also ushered in rapid development. This paper analyzes the research status of zero-knowledge proof schemes based on polynomial commitment construction, and introduces the construction and security of polynomial commitments. Finally, blockchain and some other potential commitment schemes that can be used for zero-knowledge proofs and blockchain construction are introduced as future research directions and engineering applications.

Keywords: Polynomial commitment; Zero-knowledge proof, Blockchain technology

1 Introduction

A cryptographic commitment is a two-stage protocol (**Commit**, **Open**) between two parties. The **Commit** stage consists of one party hiding and binding the secret and sending it to the second party; while the **Open** stage is to prove that the first party did not deceive the second party in the Commit stage [1]. Polynomial commitment scheme (PCS) is a new cryptographic commitment scheme, first proposed by Kate

How to Cite:

Becky Mundele & Chenchen Han, "Polynomial Commitment-Based Zero-Knowledge Proof Schemes: A Brief Review". *AIJR Preprints*, 384, Version 1, 2022.

et al. [2]. They give two concrete constructions of the polynomial commitment based on the discrete logarithm assumption, one referring to the Pedersen commitment and the other a completely new construction. Their scheme has a fixed open overhead, which is also constant when multiple evaluations are opened. In addition to the introduced two applications of verifiable secret sharing and zero-knowledge proofs, polynomial commitments have potential applications in other areas. Zero-knowledge proof is a cryptographic protocol that originated in the 1980s. In short, zero-knowledge proof is a method that can fully prove that one is the legal owner of a data set without leaking the relevant information.

Benefiting from blockchain technology, cryptographic commitment schemes and zero-knowledge proofs are one of the research hotspots in the field of cryptography today. The three commonly used zero-knowledge proof schemes are zk-SNARKs [3], zk-STARKs [4], and Bulletproofs [5]. The comparisons are shown in Table 1. It can be seen from Table 1 that zk-SNARKs is superior to the other two schemes in terms of verification time and proof size, while Bulletproofs has a very long verification time. In addition, its verification time is also longer than the other two schemes. zk-SNARK is a zero-knowledge proof algorithm proposed in 2013. It is used in **Zerocash** to realize the function of anonymous currency. However, the zk-SNARKs scheme usually requires trusted settings, which is one of its shortcomings.

Table 1: *Comparison of polynomial commitment-based zero-knowledge proof schemes.*

Property	zk-SNARKs(Have trusted setting)	zk-STARKs	Bulletproofs
Proof size	288bytes	45~200KB	1.3KB
Prover time	2.3s	1.6s	30s
Verification time	10ms	16s	1100s

Trust Setup problem: Trusted setup is one of the problems that zero-knowledge proof schemes based on polynomial commitments need to solve.Polynomial commitments that do not require a trusted setup are often referred to as transparent polynomial commitment schemes (TPCS). Before the zero-knowledge proof protocol can prove and authenticate, some public parameters need to be set and generated. However, in the process of generating these public parameters, some intermediate data that cannot be disclosed is generated, and this part of the undisclosed data needs to be deleted after the setup is completed. Any party with access to this data can break the protocol. We need to ensure that these data are really deleted. One of the ways to solve this problem is to use multi-party computation to generate these public parameters. As long as one party is honest, the protocol is secure; another method is the Sonic method [6], which allows these parameters to be continuously updated as long as the current updater of is honest, then the current parameters are secure.

This paper first introduces the specific construction of polynomial commitments and the security they need to satisfy. Then it introduces the research status of its use in constructing zero-knowledge proofs, and gives a brief overview. Finally, future research points for zero-knowledge proofs based on polynomial commitments are introduced.

2 The Concept of Polynomial Commitment

This section mainly gives the general definition of polynomial commitment. Of course, with the development of polynomial commitment, its structure has also changed. Here, the scheme proposed by Kate et al. shall prevail.

2.1 System Model

PCS is a two-party protocol. PCS can be simply divided into five algorithms: **Parameter Setting**, **Commit**, **Open**, **Verify** and **Evaluate**. A brief description is as follows:

- **Parameter setting:** The algorithm inputs a security parameter, a polynomial $F(x)$ of degree t, and generates a public-private key pair.
- **Commit**: Generate a polynomial $F(x)$ corresponding to the commitment C.
- **Open**: The algorithm opens the above commitment C.
- **Verify**: The algorithm needs to verify that the generated commitment is valid.
- **Evaluate**: Taking the Kate's scheme as an example, the prover needs to generate a witness related to the index, and then the verifier will evaluate whether the witness is valid.

2.2 Security and Extension

The Kate's scheme introduces that polynomial commitments need to satisfy two characteristics: binding and hiding. The binding is divided into evaluation binding and polynomial binding. When we construct a secure polynomial commitment, we need to prove that these two security characteristics. The specific definition can be seen in their paper [1].

- **Binding**: Simply put, the committed value is bound to the polynomial and is unique. It is very difficult for an adversary to tamper with this value.
- **Hiding**: Hiding means that the committed value will not be seen by others, which is the guarantee of the privacy of the commitment scheme.

Usually, we divide commitment schemes into four categories according to binding and hiding:

- **Class A**: Computationally hidden and computationally bound (both sender and receiver are polynomially computationally bounded).
- **Class B**: Computational hiding and statistical binding (sender's computational power is unbounded, receiver is polynomially computationally bounded).
- **Class C**: Statistical hiding and computational binding (the sender is bounded by polynomial computation, and the computing power of sender and receiver is unbounded).
- **Class D**: Statistical hiding and Statistical binding (sender and receiver computation negligible unbounded).

The above classification also provides us with a direction to improve the polynomial commitment scheme. At the same time, we also classify polynomial commitments according to different characteristics, which will be given in the extended version.

3 Zero-knowledge Proof Based on Polynomial Commitment

This section briefly introduces polynomial commitment and the research status of zero-knowledge proof based on polynomial commitment, as shown in Table 2. The specific comparison will be given in the full version.

Note: Before understanding these programs, you need to understand several concepts including Algebraic Group Model (AGM), Interactive Oracle Proof (IOP) in advance. These concepts are widely used in constructing zero-knowledge proof schemes based on polynomial commitments.

Table 2: *Summary of polynomial commitment-based zero-knowledge proof schemes.*

Year	Schemes	Introducation	Trusted Setup
2010	Kate[1]	The first polynomial commitment scheme and zero-knowledge application.	√
2018	Bulletproofs[5]	Generate a single proof by simple multi-party computation.	×
2019	Sonic[6]	Strings are generic and updatable.	√
2016	Groth[7]	Two pairing-based SNARK schemes.	√
2019	Auroralight[8]	Improved sonic scheme in proof time and SRS size.	√
2019	Marlin[9]	Algebraic holographic proof.	-
2019	REDSHIFT[10]	List polynomial commitment.	√
2020	DARK[11]	Multivariate polynomial commitment.	×
2020	Boneh[12]	Multiple points and polynomials schemes, Algebraic Group Model(AGM).	-
2020	PLONK[13]	Improving the Sonic scheme in terms of proof construction and runtime.	-
2020	Halo[14]	Fiat-Shamir transformation without black box.	-
2021	Dory[15]	A multivariate polynomial commitment scheme based on Fiat-Shamir transform.	×
2022	Info-commit[16]	Information-theoretic protocol for polynomial commitment and verification.	-
2022	Hyperproofs[22]	An updated vector commitment scheme that can be efficiently maintained	×

4 Future Engineering Applications

Obviously, the zero-knowledge proof scheme based on polynomial commitment can be applied to the blockchain. Blockchain is a secure data storage technology and an important technology leading the future data revolution. So far, the blockchain can realize public verification and non-public verification, and its efficiency is gradually improving [17]. In the blockchain, zero-knowledge proof schemes can be used to protect transaction privacy, which is a very important application. In addition, zero-knowledge proofs can also provide un-modifiable proofs for transactions between nodes.

However, one of the biggest advantages of cryptographic commitments is that they can be used as building blocks to improve other cryptographic schemes. As the layered identity-based cryptography

scheme (HIBE) mentioned in our previous work [19], the commitment scheme has the potential to improve HIBE schemes.

Also note that several other variants of polynomial commitments, such as vector commitments and functional commitments [20, 21], also have potential in constructing zero-knowledge proofs and in blockchain applications.

5 Conclusion

This paper mainly introduces the development status of polynomial commitment scheme, gives its classical definition and introduces the security that a secure polynomial commitment needs to satisfy. Then this paper introduces the research status of zero-knowledge proof schemes constructed by polynomial commitments. It also introduces a practical application of zero-knowledge proofs constructed by polynomial commitment: blockchain. Combined with zero-knowledge proof, the privacy and security of the blockchain are further improved. However, more actual scheme comparison and analysis will be given in the full version.

6 Declarations

6.1 Acknowledgements

Thank you for Advanced Machinery Research Institute's support for this paper.

6.2 Competing Interests

The author declared that no conflict of interest exists in this work.

References

[1] I. Damgård, "Commitment Schemes and Zero-Knowledge Protocols," In *School organized by the European Educational Forum*, 1999, pp. 63-86, doi: 10.1007/3-540-48969-x_3.

[2] A. Kate, G. M. Zaverucha, and I. Goldberg, "Constant-size commitments to polynomials and their applications," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2010, vol. 6477 LNCS. doi: 10.1007/978-3-642-17373-8_11.

[3] A. Banerjee, M. Clear and H. Tewari, "Demystifying the Role of zk-SNARKs in Zcash," 2020 *IEEE Conference on Application, Information and Network Security (AINS)*, 2020, pp. 12-19, doi: 10.1109/AINS50155.2020.9315064.

[4] A. Rahimi and M. A. Maddah-Ali, "Multi-Party Proof Generation in QAP-Based zk-SNARKs," in *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 3, pp. 931-941, Sept. 2021, doi: 10.1109/JSAIT.2021.3102267.

[5] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille and G. Maxwell, "Bulletproofs: Short Proofs for Confidential Transactions and More," *2018 IEEE Symposium on Security and Privacy (SP)*, 2018, pp. 315-334, doi: 10.1109/SP.2018.00020.

[6] M. Maller, M. Kohlweiss, S. Bowe, and S. Meiklejohn, "Sonic: Zero-knowledge snarks from linear-size universal and updatable structured reference strings," In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp.2111-2128, doi: 10.1145/3319535.3339817.

[7] J. Groth, "On the size of pairing-based non-interactive arguments," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016, vol. 9666, pp. 305-326, doi: 10.1007/978-3-662-49896-5_11.

[8] A. Gabizon, "AuroraLight: Improved prover efficiency and SRS size in a Sonic-like system," *Cryptol. ePrint Arch.*, 2019.

[9] A. Chiesa, Y. Hu, M. Maller, P. Mishra, N. Vesely, and N. Ward, "Marlin: preprocessing zksnarks with universal and updatable srs," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2020, vol. 12105 LNCS, pp. 738-768, doi: 10.1007/978-3-030-45721-1_26.

[10] A. Kattis, K. Panarin, and A. Vlasov, "RedShift: Transparent SNARKs from List Polynomial Commitment IOPs," *Eprint.Iacr*, 2019.

[11] B. Bünz, B. Fisch, and A. Szepieniec, "Transparent snarks from dark compilers," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2020, vol. 12105 LNCS, pp. 677-706, doi: 10.1007/978-3-030-45721-1_24.

[12] D. Boneh, J. Drake, B. Fisch, and A. Gabizon, "Efficient polynomial commitment schemes for multiple points and polynomials," *IACR Cryptol. ePrint Arch.*, 2020.

[13] A. Gabizon, Z. J. Williamson, and O. Ciobotaru, "PLONK : Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge," *IACR Cryptol. ePrint Arch.*, 2020.

[14] D. Boneh, J. Drake, B. Fisch, and A. Gabizon, "Halo infinite: recursive zk-SNARKS from any additive polynomial commitment scheme," *IACR Cryptol. ePrint Arch.*, 2020.

[15] J. Lee, "Dory: Efficient, Transparent Arguments for Generalised Inner Products and Polynomial Commitments," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2021, vol. 13043 LNCS, pp. 1-34, doi: 10.1007/978-3-030-90453-1_1.

[16] S. Sahraei, S. Avestimehr and R. E. Ali, "Info-Commit: Information-Theoretic Polynomial Commitment," in *IEEE Transactions on Information Forensics and Security*, 2022, doi: 10.1109/TIFS.2022.3163581.

[17] C. Han, G. J. Kim, O. Alfarraj, A. Tolba, and Y Ren, "ZT-BDS: A Secure Blockchain-based Zero-trust Data Storage Scheme in 6G Edge IoT," *Journal of Internet Technology*, 2022, 23(2), 89-95, doi: 10.53106/160792642022032302009.

[18] J. Wang, C. Han, X. Yu, Y. Ren, and R. S. Sherratt, "Distributed Secure Storage Scheme Based on Sharding Blockchain," *Computers, Materials & Continua*, 2022, 70(3), 4485-4502, doi: 10.32604/cmc.2022.020648.

[19] C, Han, "Hierarchical Identity-based Broadcast Cryptography and its Application in Blockchain," *AIJR Preprints*, 2021, doi: https://doi.org/10.21467/preprints.346.

[20] D. Catalano and D. Fiore, "Vector commitments and their applications," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2013, vol. 7778 LNCS, pp. 55-72, doi: 10.1007/978-3-642-36362-7_5.

[21] B. Libert, S. C. Ramanna, and M. Yung, "Functional commitment schemes: From polynomial commitments to pairing-based accumulators from simple assumptions," in *Leibniz International Proceedings in Informatics, LIPIcs*, 2016, vol. 55, doi: 10.4230/LIPIcs.ICALP.2016.30.

[22] S. Srinivasan *et al.*, "Hyperproofs: Aggregating and Maintaining Proofs in Vector Commitments," *Cryptol. ePrint Arch.*, 2021.