Threshold Signatures and Applications in Blockchains

Zhuo Cai

Hong Kong University of Science and Technology

Abstract. The abstract should briefly summarize the contents of the paper in 150–250 words.

1 Introduction

[1]

2 Background and Toolbox

2.1 Cryptographic Assumptions

2.2 Pairing

2.3 Digital Signatures

Definition 1. *(Digital Signature) A digital signature scheme,* $SGN(KeyGen, Sign, Verify)$*, consists of four algorithms defined as follows:*

- $(pk, sk) \leftarrow SGN.Setup(\kappa, pp)$: Given the security parameter κ and public parameters pp, it generate a pair of public/secret keys (pk, sk).
-

2.4 Threshold Signatures

2.5 Multi Signatures

2.6 Aggregators

2.7 Weighted Threshold Signatures

2.8 Adaptive Security

3 Topic 1

4 Topic 2

5 Conclusion

References

1. Das, S., Camacho, P., Xiang, Z., Nieto, J., Bünz, B., Ren, L.: Threshold signatures from inner product argument: Succinct, weighted, and multi-threshold. In: CCS. pp. 356–370. ACM (2023)