

Post-Quantum Verifiable Delay Functions

Péter Burcsi¹, István András Seres¹, and Dániel A. Nagy¹

¹Department of Computer Algebra, Eötvös Loránd University

December 18, 2018

Abstract

Keywords: Cryptography, Verifiable delay function, Post-Quantum Cryptography, Cryptocurrency, Ethereum

- 1 Introduction
- 2 Background
- 3 Construction
- 4 Security arguments
- 5 Conclusion
- 6 Acknowledgements