Privacy-Enhancing Technologies on Blockchains

Noemi Glaeser

Abstract

Blockchains are inherently public, [but sometimes we want privacy. We need to use crypto to do this. And so on and so forth...] Noemi: actually probably need to expand to also include "security", since the threshold sigs project isn't really about privacy

Contents

1 Introduction

1.1 Model and Preliminaries

1.2 Definitions

2 Privacy in Cryptocurrencies

2.1 Introduction

2.2 Related Work

2.3 Anonymous Atomic Locks for coin mixing and cross-chain payments

2.3.1 Overview

[copied] In this section, we summarize the contributions and constructions of [GMM+22], including...

2.4 Circuit-Succinct Universally Composable NIZKs with Updatable CRS

2.4.1 Overview

[copied] In this section, we summarize the contributions and constructions of [AGRS24], including...

2.5 Cicada: A framework for private non-interactive on-chain auctions and voting

2.5.1 Overview

[copied] In this section, we summarize the contributions and constructions of [GSZB23], including...

3 Proposed Work

3.1 Registration-Based Encryption as a Web3 service

Noemi: Unclear if this can be included

3.2 Threshold cryptocurrency wallets in the hot-cold paradigm

References

[AGRS24] Behzad Abdolmaleki, Noemi Glaeser, Sebastian Ramacher, and Daniel Slamanig. Circuit-succinct universally-composable NIZKs with updatable CRS. 2024.

[GMM$^+$22] Noemi Glaeser, Matteo Maffei, Giulio Malavolta, Pedro Moreno-Sanchez, Erkan Tairi, and Sri Aravinda Krishnan Thyagarajan. Foundations of coin mixing services. In Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi, editors, *ACM CCS 2022*, pages 1259–1273. ACM Press, November 2022.

[GSZB23] Noemi Glaeser, István András Seres, Michael Zhu, and Joseph Bonneau. Cicada: A framework for private non-interactive on-chain auctions and voting. Cryptology ePrint Archive, Paper 2023/1473, 2023. https://eprint.iacr.org/2023/1473.