# MPC for Group Reconstruction Circuits

Lúcás Críostóir Meier

June 6, 2022

**Abstract**

In this paper, we present a thing.

1 Introduction

2 Background

2.1 Pedersen Commitments

2.2 Sigma Protocols

2.3 Maurer's $\varphi$-Proof

2.4 UC Security and the Hybrid Model

2.5 Ideal Functionalities for Sigma Protocols

2.6 Broadcast Functionalities

3 Group Reconstruction Circuits

3.1 Formal Definition

3.2 Normalized Form

4 MPC Protocol for GRCs

5 Security Analysis

6 Applications

7 Limitations and Further Work

8 Conclusion

References