MPC for Group Reconstruction Circuits

Lúcás Críostóir Meier

June 7, 2022

Abstract

In this paper, we present a thing.

1 Introduction

2 Background

Throughout this paper, we let $\mathbb{G}$ denote a group of prime order q, with generators G and H. Let $\mathbb{F}_q$ denote the scalar field associated with this group, and let $\mathbb{Z}/(q)$ denote the additive group of elements in this field.

We make heavy use of group homomorphisms throughout this paper. We let

$$\varphi(P_1, \ldots, P_m) : \mathbb{A} \to \mathbb{B}$$

denote a homomorphism from $\mathbb{A}$ to $\mathbb{B}$, parameterized by some public values $P_1, \ldots, P_m$. Commonly $\mathbb{A}$ will be a product of several groups $\mathbb{G}_1, \ldots, \mathbb{G}_n$, in which case we'd write:

$$\varphi(P_1, \ldots, P_m)(x_1, \ldots, x_n)$$

to denote the application of φ to an element $(x_1, \ldots, x_n)$ of the product group. We also often leave the public values P_i implicit.

2.1 Pedersen Commitments
2.2 Sigma Protocols
2.3 Maurer's φ-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