

MPC for Group Reconstruction Circuits

Lúcas Críostóir Meier

June 7, 2022

Abstract

In this paper, we present a thing.

1 Introduction

Write the 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

$$\varphi(P_1, \dots, P_m) : \mathbb{A} \rightarrow \mathbb{B}$$

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

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

to denote the application of φ to an element (x_1, \dots, 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

In [Mau09], Maurer generalized Schnorr's sigma protocol for knowledge of the discrete logarithm [Sch90] to a much larger class of relations. In particular, Maurer provided a sigma protocol for proving knowledge of the pre-image of a group homomorphism φ . We denote this protocol as a “ φ -proof”, and recapitulate the scheme here.

Given a homomorphism $\varphi : \mathbb{A} \rightarrow \mathbb{B}$, and a public value $X \in \mathbb{B}$, the prover wants to demonstrate knowledge of a private value $x \in \mathbb{A}$ such that $\varphi(x) = X$.

Figure 2.1: φ -Proof

$$\begin{array}{c} x + 2 \\ x + 2 \end{array}$$

In Figure 2.1

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

- [Mau09] Ueli Maurer. Unifying Zero-Knowledge Proofs of Knowledge. In *AFRICACRYPT 2009*, volume 5580 of *LNCS*, pages 272–286. Springer, Berlin, Heidelberg, 2009.
- [Sch90] C. P. Schnorr. Efficient Identification and Signatures for Smart Cards. In *CRYPTO 1989*, volume 435 of *LNCS*, pages 239–252, New York, NY, 1990. Springer.