Halo 2

Contents

1 Introduction

Starting from the Orchard update of Zcash, Halo 2 replaces Groth16 as the new proving system. This document will explain how Halo 2 works and how it is used both from a theoretical and practical standpoint.
The goal of this document is not to be a self-contained explanation, but rather a description of how the wide variety of sources on Halo 2 and zero-knowledge proofs fits together and interconnects. Therefore, references are everywhere and explanations are intuitive and informal.

2 Resources on zk-SNARKs

zk-SNARKs: A Gentle Introduction [3] provides an overview of current practical zk-SNARK constructions. Halo 2 is a polynomial interactive oracle proof (PIOP) that is made non-interactive using the Fiat-Shamir transformation.
The zkStudyClub [2] is a YouTube playlist that expains a lot of contemporary research on zk-SNARKs and zero-knowledge proofs in general.
There is a Discord server on the Halo 2 Ecosystem that is publicly accessible, where Zcash developers answer individual questions on Halo 2 and related topics.

3 The Halo 2 Proving System

The official reference for Halo 2 is the Halo 2 Book [4]. A previous version of Halo 2 called Halo is described in [5]. Halo and Halo 2 have the core concepts in common, such as polynomial commitments using inner product arguments or an accumulation scheme to enable recursive proofs, but differ in that Halo builds on Sonic [8] while Halo 2 builds on PLONK [6] as well as other details.
A master thesis from Aarhus university [7] elaborates on [4] and explains the basic concepts of Halo 2 very well.

4 Usage in Zcash

Halo 2 does not rely on a trusted setup. While the two previous proving systems, BCTV14 and Groth16, needed an MPC ceremony to create a trusted setup, this is not needed anymore. A video of the (rather spectacular) MPC ceremony for BCTV14 is available on YouTube [1].
Furthermore, Halo 2 enables recursive proofs, referring to the possibility of proving the successful verification of another proof. This is used in Zcash to bundle multiple Action descriptions and create a single proof for the validity of all Action descriptions.

References

[1] Zcash Ceremony. https://www.youtube.com/watch?v=D6dY-3x3teM. Accessed: 2023-07-12.

[2] zkStudyClub. https://www.youtube.com/playlist?list=PLj80z0cJm8QHm_9BdZ1BqcGbgE-BEn-3Y. Accessed: 2023-07-12.

[3] Anca Nitulescu. zk-SNARKs: A Gentle Introduction. https://www.di.ens.fr/~nitulesc/files/Survey-SNARKs.pdf. Accessed: 2023-07-12.

[4] Sean Bowe. The halo2 Book. https://zcash.github.io/halo2/, 2020. Accessed: 2023-04-07.

[5] Sean Bowe, Jack Grigg, and Daira Hopwood. Recursive proof composition without a trusted setup. Cryptology ePrint Archive, Paper 2019/1021, 2019. https://eprint.iacr.org/2019/1021.

[6] Ariel Gabizon, Zachary J. Williamson, and Oana Ciobotaru. Plonk: Permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge. Cryptology ePrint Archive, Paper 2019/953, 2019. https://eprint.iacr.org/2019/953.

[7] Lasse Bramer Schmidt, Rasmus Tomtava Bjerg. High Assurance Specification of the halo2 Protocol. https://forum.zcashcommunity.com/uploads/short-url/bvRHjg39MfC06nERJ3BgknkWHqN.pdf. Accessed: 2023-07-12.

[8] Mary Maller, Sean Bowe, Markulf Kohlweiss, and Sarah Meiklejohn. Sonic: Zero-knowledge snarks from linear-size universal and updateable structured reference strings. Cryptology ePrint Archive, Paper 2019/099, 2019. https://eprint.iacr.org/2019/099.