Attacking Zcash Protocol For Fun And Profit
Whitepaper Version 0.1

Duke Leto + The Hush Developers[†]

May 5, 2020

Abstract.

This paper will outline, for the first time, exactly how the "ITM Attack" (a linkability attack against shielded transactions) works against Zcash Protocol and how Hush is the first cryptocoin with a defensive mitigation against it, called "Sietch". Sietch is already running live in production and undergoing rounds of improvement from expert feedback. This is not an academic paper about pipedreams. It describes production code and networks.

We begin with a literature review of all known metadata attack methods that can be used against Zcash Protocol blockchains. This includes their estimated attack costs and threat model. This paper then describes the "ITM Attack" which is a specific instance of a new class of metadata attacks against blockchains which the author describes as "Metaverse Metadata" attacks.

The paper then explains Sietch in detail, which was a response to these new attacks. We hope this knew knowledge and theory helps cryptocoins increase their defenses against very well-funded adversaries including nation states and chain analysis companies.

A few other new privacy issues and metadata attacks against Zcash Protocol coins will also be enumerated for the first time publicly. The ideas in this paper apply to all cryptocoins which utilize transaction graphs, which is to say just about all known coins. Specifically, the Metaverse Metadata class of attacks is applicable to all Bitcoin source code forks (including Dash, Verge, Zerocoin and their forks), CryptoNote Protocol coins (Monero and friends) and MimbleWimble Protocol (Grin, Beam, etc) coins but these will not be addressed here other than a high-level description of how to apply these methods to those chains.

> In privacy zdust we trust.
>
> If dust can attack us, dust can protect us.
>
> – Sietch Mottos

Keywords: anonymity, zcash protocol, cryptographic protocols, zk-SNARKs, metadata leakage, deanonymization, electronic commerce and payment, financial privacy, zero knowledge mathematics, linkability, transaction graphs, shielded transactions, blockchain analysis .

Contents

[†] myhush.org, https://keybase.io/dukeleto, F162 19F4 C23F 9111 2E9C 734A 8DFC BF8E 5A4D 8019

1 Introduction

2 Metadata Analysis of Zcash Protocol Blockchains: Basics

3 Metadata Analysis of Zcash Protocol Blockchains: Advanced

4 De-anonymization techniques literature review

5 ITM Attack: z2z Transaction Linkability

...

6 Metaverse Metadata Attacks

TODO: Explain how they can be used on all blockchains with transaction graphs, including CryptoNote Protocol and MimbleWimble Protocol

7 Sietch: Theory

8 Sietch: Code In Production

9 Advice To Zcash Protocol Coins

10 Special Thanks

Special thanks to jl777, ITM and denioD for their feedback.

11 References