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

2.1 Concepts and Definitions

This paper will be concerned with **transaction graphs**, which we define in the traditional mathematical sense, of a set of nodes with a set of vertices connecting nodes. In cryptocoins these always happen to be directed graphs, since there are always funds which are unspent becoming spent, i.e. a direction associated with each transaction.

There is a great deal of mathematical history devoted to the study of **graph theory** that has not been applied to blockchain analysis, mostly because there was no blockchains to analyze just a few years ago and there was no financial profit in studying the data. That has obviously drastically changed.

This paper will be primarily concered with **shielded transaction graphs** which are **directed acyclic graphs (DAGs)**. A ***shielded*** transaction does not reveal the address of Alice, nor Bob, nor the amount transacted but it does leak a large amount of metadata at the protocol level, which is not rendered by block explorers nor well understood by the industry.

A ***shielded*** transaction has at least one ***shielded*** address, referred to as a ***zaddr***.

We here concern ourselves only with **Zcash Protocol** which allows us to specify a coherent language and symbols to describe the new ITM ***zaddr*** linkability attack and mitigations against it. All techniques here could technically also be used against transparent blockchains, but since they leak all the useful metadata already, it would serve no purpose. These new attacks can be thought of as "squeezing" new metadata leakage from zaddrs out of places that nobody thought to look.

For those coins which only have a transaction graph at the network p2p level but not stored on their blockchain (such as MimbleWimble coins), it does raise the bar and attack cost. Since nation-states and are not cost-sensitive and obviously have a vested interest to de-anonymize all blockchains, MW coins are not immune to these new attacks being applied. A transaction graph still exists and so the core concepts here can be applied.

2.2 Types Of Shielded Transactions

There are many types of shielded transactions, mirroring the complexity of transparent transactions in Bitcoin Protocol. Here we introduce a convention for describing transactions.

- A fully shielded transaction T with change $T : z \to z, z$
- A fully shielded transaction T with no change $T : z \to z$
- A shielded transaction T with transparent change $T : z \to z, t$
- A dehielding transaction T with change $T : z \to t, z$
- A dehielding transaction T with no change $T : z \to t$
- A shielding transaction T with no change $T : t \to z$
- A shielding transaction T with shielded change $T : t \to z, z$
- A shielding transaction T with transparent change $T : t \to z, t$

The above summarizes the most common transactions. Now say we want to describe a transaction which sends to 5 ***zaddrs*** and 3 transparent addresses with no change: $z \to z, z, z, z, z, t, t, t$. To describe very large transactions subscripts can be used : $z \to z_{52}, t_{39}$.

An individual transaction T is a sub-graph of the full transaction graph $T \subset \mathbb{T}$ with vertex count of one.

3 Metadata Analysis of Zcash Protocol Blockchains: Advanced

3.1 Active vs Passive Attacks/Analysis

3.2 Timing Analysis

3.3 Value Analysis

3.4 Fee Analysis

3.5 Input/Output Arity Analysis

3.6 Dust Attacks

3.7 Exchanges and Mining Pools

4 De-anonymization techniques literature review

4.1 Applications to new Shielded-only Chains

5 ITM Attack: z2z Transaction Linkability

The **ITM Attack** specifically "attacks" a transaction $T : z \to z, z$, i.e. a fully-shielded Zcash Protocol transaction which has the highest level of privacy. First we describe the definition of the attack success, if any of the following datums can be ascertained:

- The value in the ***zaddr***sending funds.
- The value any of the ***zaddrs***receiving funds.
- The value of any ShieldedInputs spent in the transaction.
- A range of possible values being sent to any ***zaddr***, such as $0.42, 1.7$
- A range of possible values stored in the sending ***zaddr***.

If any of the above metadata can be "leaked", the attack is a success. We note that this attack is completely passive in it's core, but can be greatly improved by adding active components "to taste". This is why metadata leakage attacks such as this can be thought of a method of analysis or an outright attack.

The **ITM Attack** takes transaction id's and ***zaddrs***as input, or other OSINT which is readily available on Github, Twitter, Discord, Slack, public forms, mailing lists, IRC and many other locations. With these public resources, the **ITM Attack** can bridge the gap from theoretically interesting attack to actually de-anonymizing a ***zaddr***to it's corresponding social media accounts.

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