Privacy Aspects and Subliminal Channels in Zcash

Alex Biryukov, Daniel Feher, Giuseppe Vitto

University of Luxembourg

14 November 2019

Outline

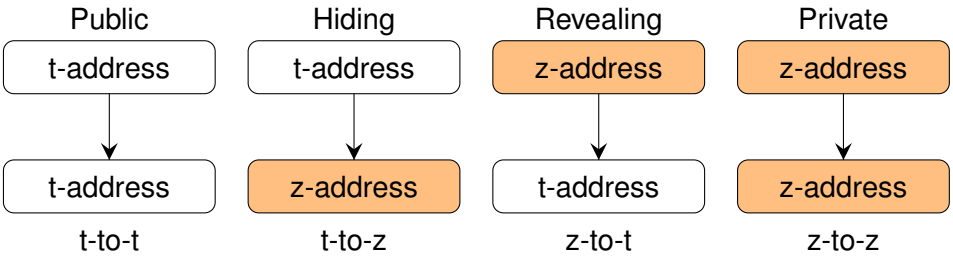
Introduction to Zcash

- Zcash is a privacy oriented digital currency.
- Built on a variety of cryptographic primitives:
  - zkSNARKs, commitment schemes, Merkle trees, encryption, etc.
- Zcash coins are called ZECs. 1 ZEC corresponds to 10^8 Zatoshis.

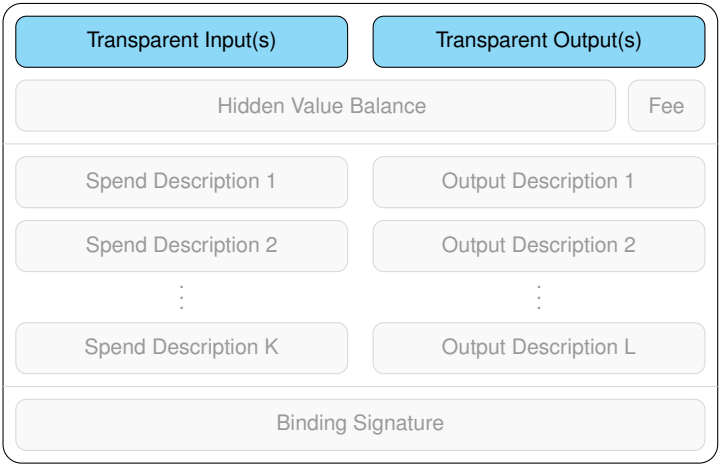
Zcash: Addresses

- Zcash offers two types of addresses:
  - *transparent* or *public*, commonly referred to as *t-addresses*.
  - *shielded* or *private*, commonly referred to as *z-addresses*.

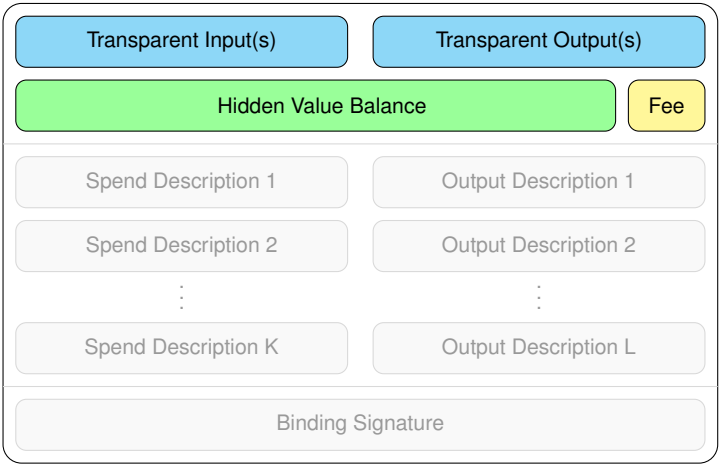
Zcash Transaction Types



Zcash Transaction Layout



Zcash Transaction Layout

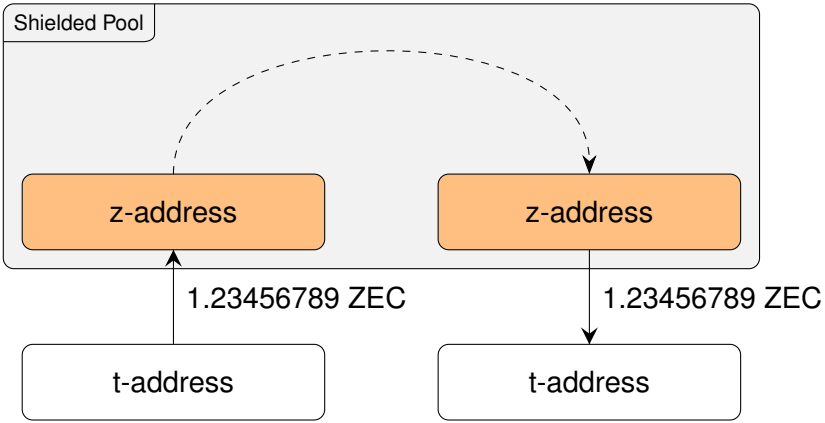


Introduction to Zcash

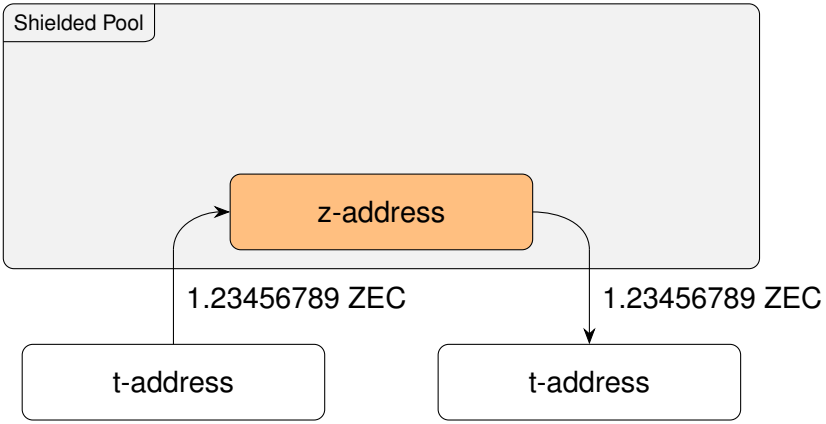
Transaction Linking

Subliminal Channels

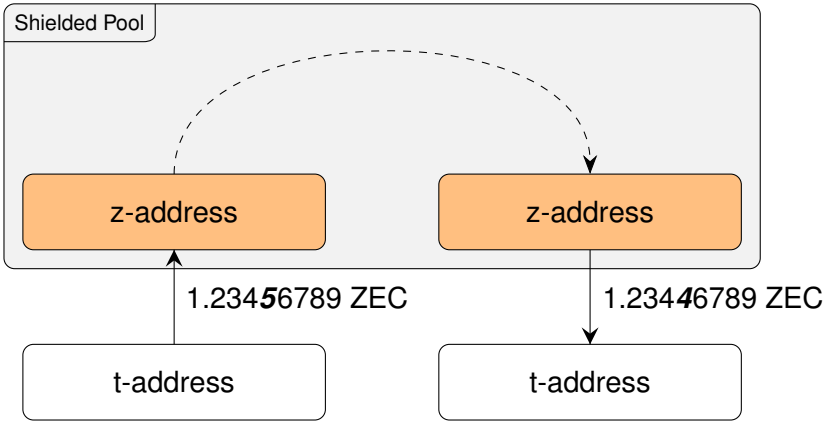
Transaction Linking v1



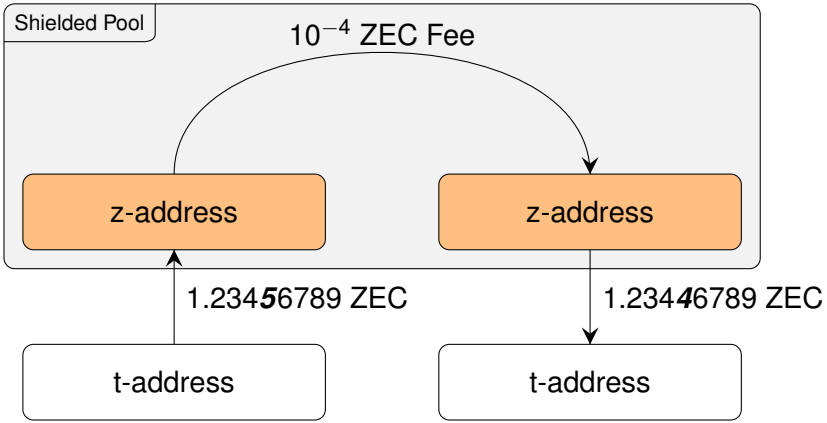
Transaction Linking v1



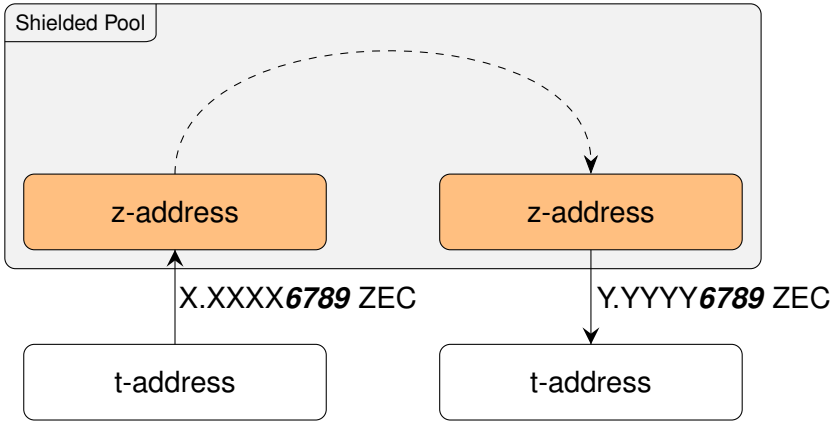
Transaction Linking v2



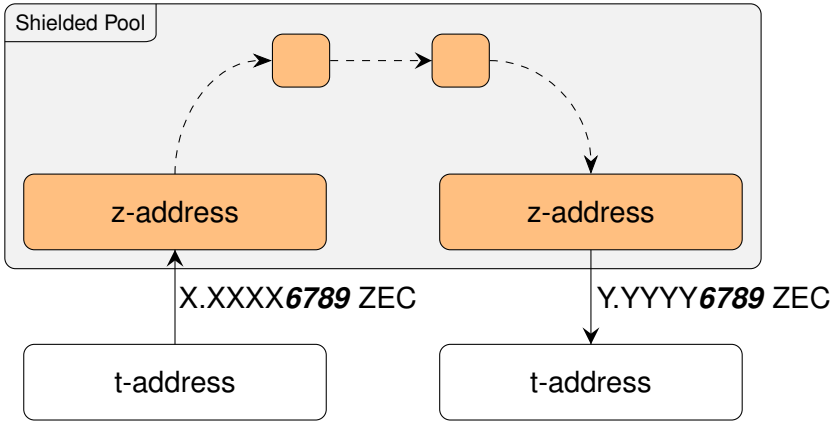
Transaction Linking v2



Transaction Linking v3



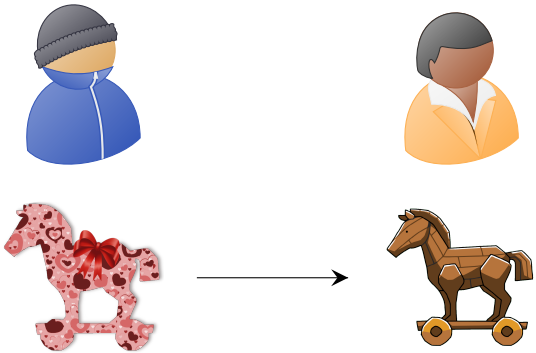
Transaction Linking v3



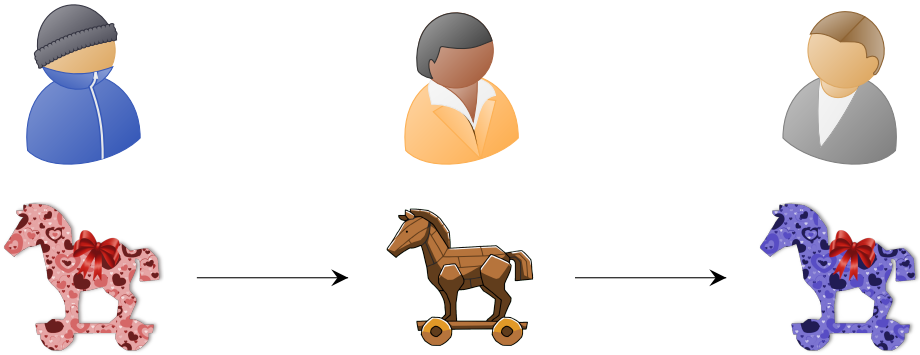
Value Fingerprints

- ~97% of shielded transactions use 10^4 Zatoshis as fee.
- Last 4 digits are not changed by the fee.
- Can be used maliciously

Danaan-Gift Attack



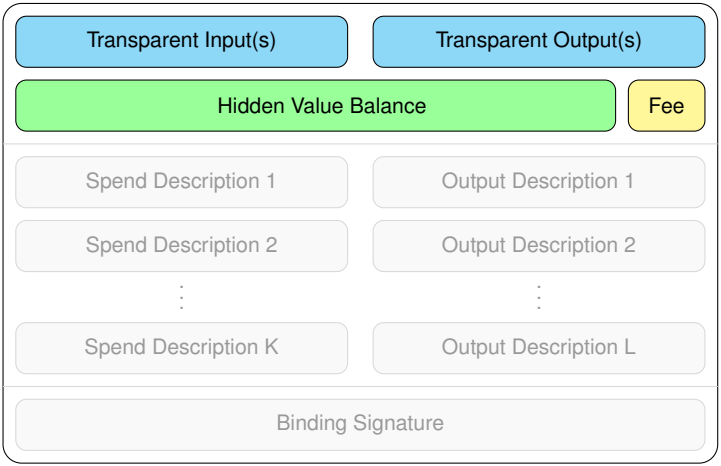
Danaan-Gift Attack



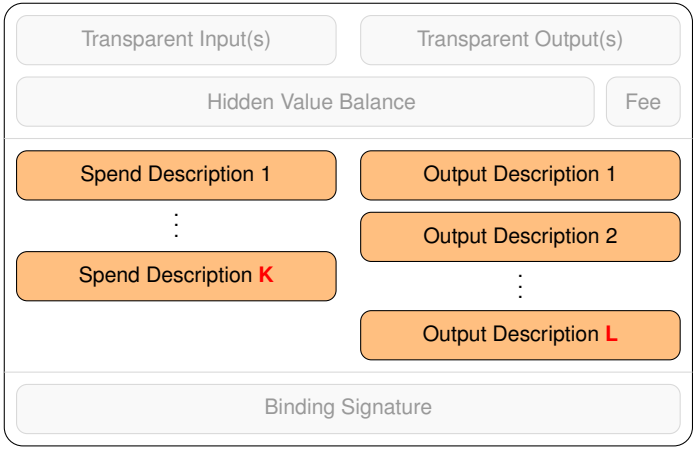
Danaan-Gift Attack

- What is the success ratio of the attack?
- What is the likelihood of a fingerprint surviving?

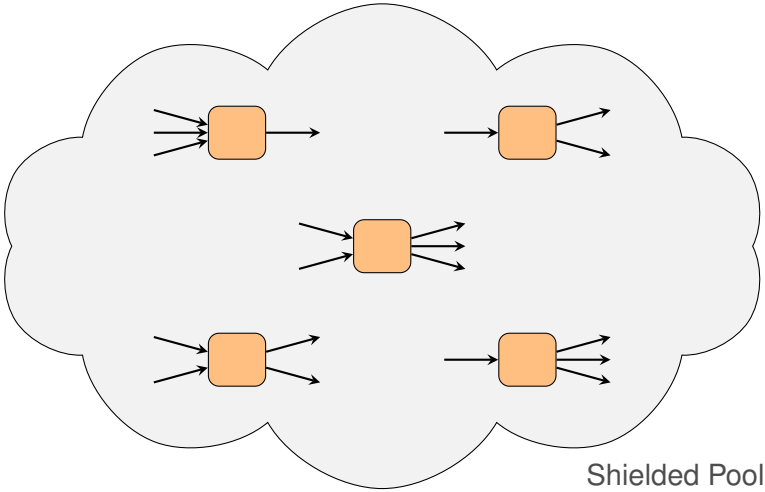
Zcash Transaction Layout



Zcash Transaction Layout

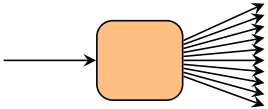


Zcash Transaction Layout

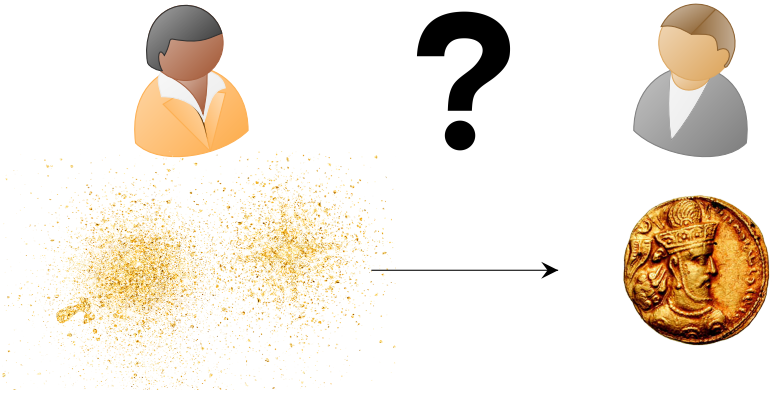


Dust Attack

Dust Attack

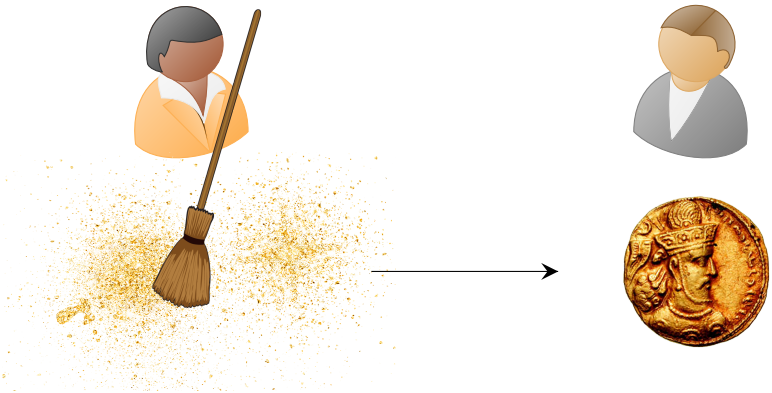


Dust Attack

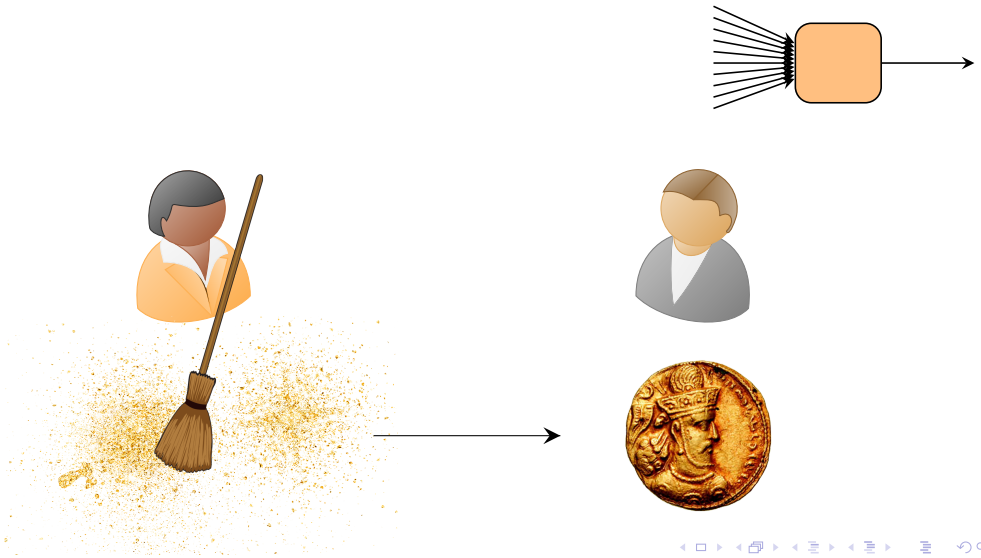


Dust Attack

Dust Attack



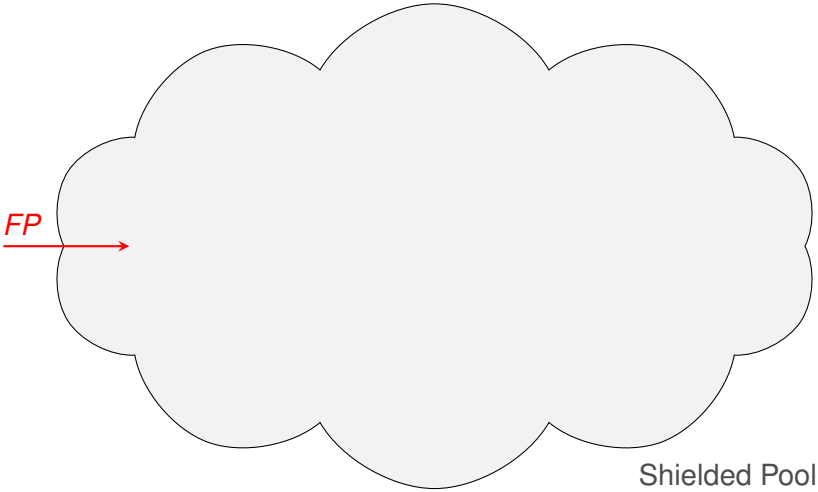
Dust Attack



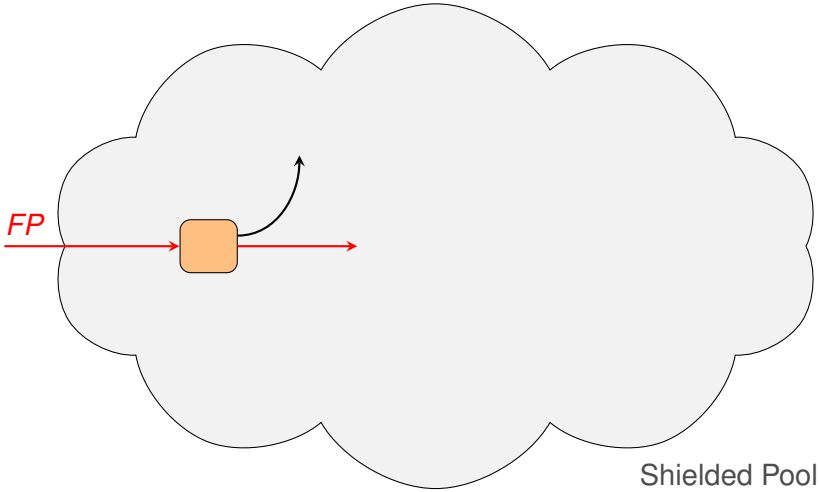
The Survival Probability of Fingerprints

- We have developed a statistical model for the shielded pool.
- Based on the number of inputs and outputs in a shielded transaction.
- Markov-chain of all possible scenarios.
- Sample data based on characteristically the same public transactions.

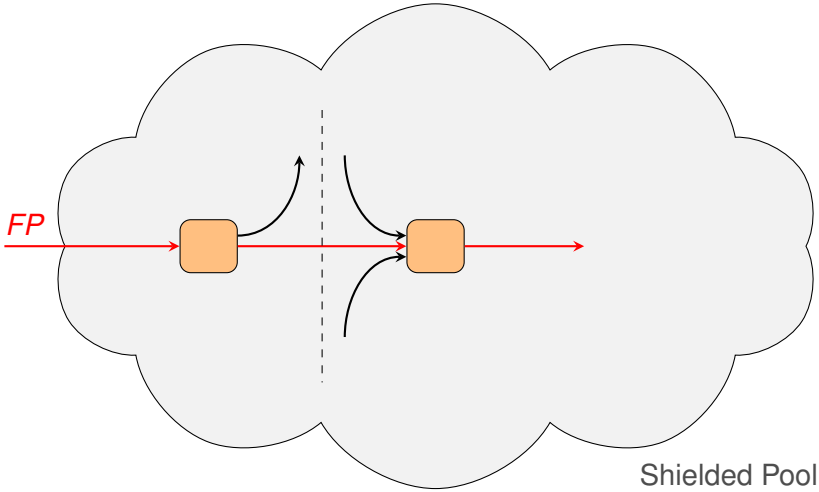
The Survival Probability of Fingerprints



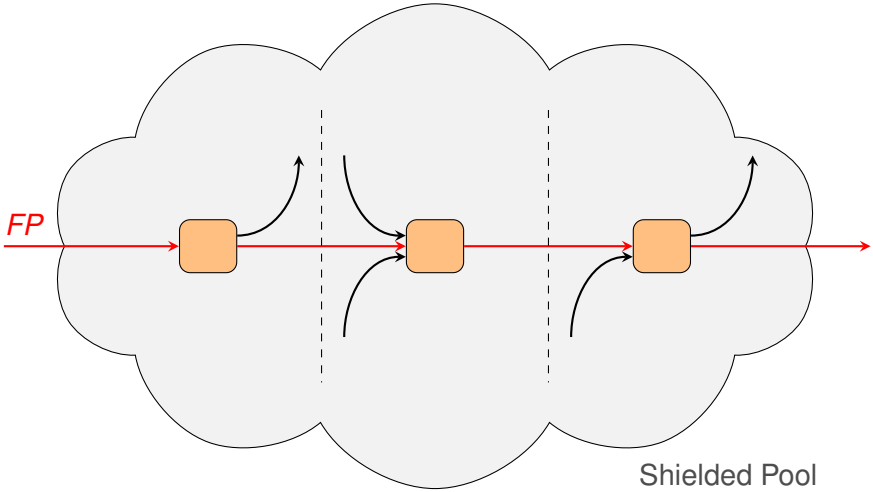
The Survival Probability of Fingerprints



The Survival Probability of Fingerprints



The Survival Probability of Fingerprints



The Survival Probability of Fingerprints

- The average number of hops a path goes through inside the shielded pool is only 1.42.
- The survival probability of *good* fingerprints is ~16.6%.
- The survival probability of fingerprints corresponds, in turn, to the success probability of Danaan-gift Attack.

Countermeasures

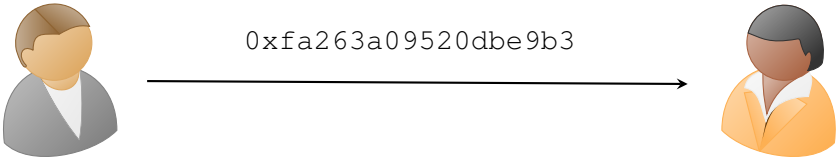
- Dust Attack is recognizable: move funds once.
- Danaan-gift Attack *manual defense*: do not use default fees.
- Danaan-gift Attack *built-in defense*: default fee is a random value between 0.00009500 ZEC and 0.00010500 ZEC.

Introduction to Zcash

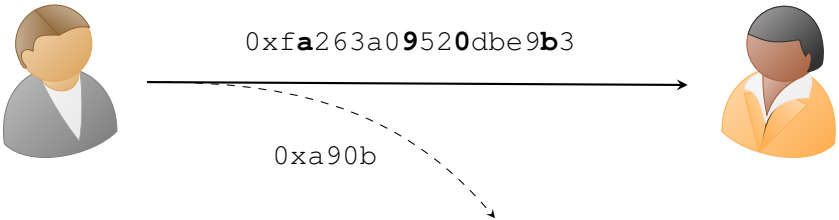
Transaction Linking

Subliminal Channels

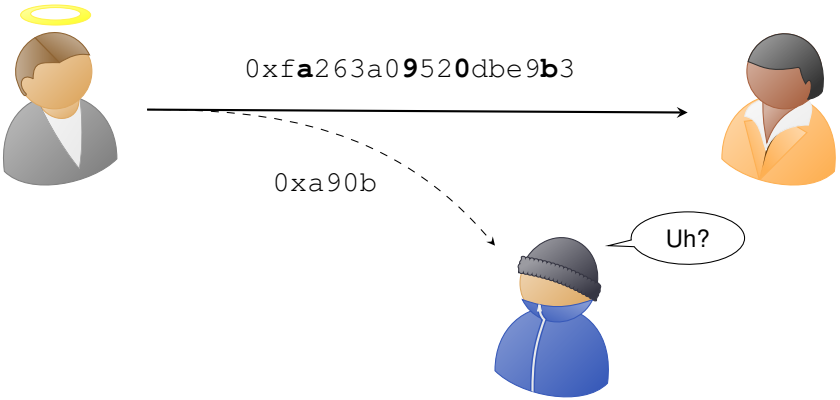
Subliminal Channels



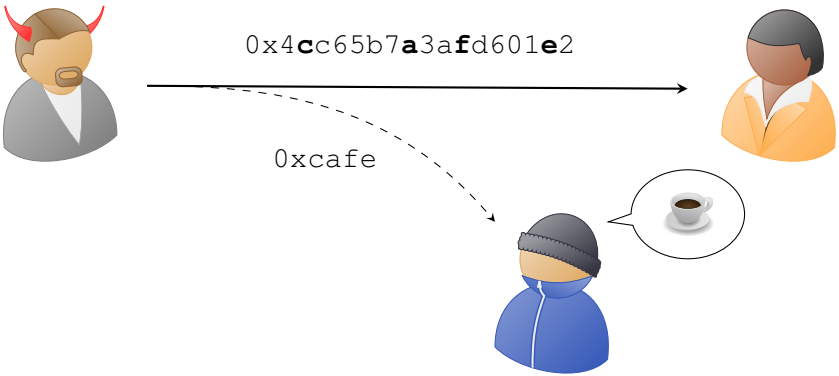
Subliminal Channels



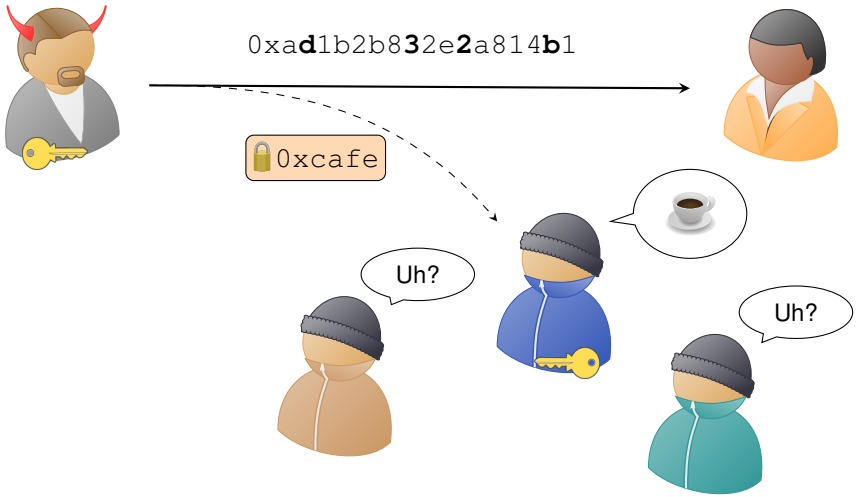
Subliminal Channels



Subliminal Channels



Subliminal Channels

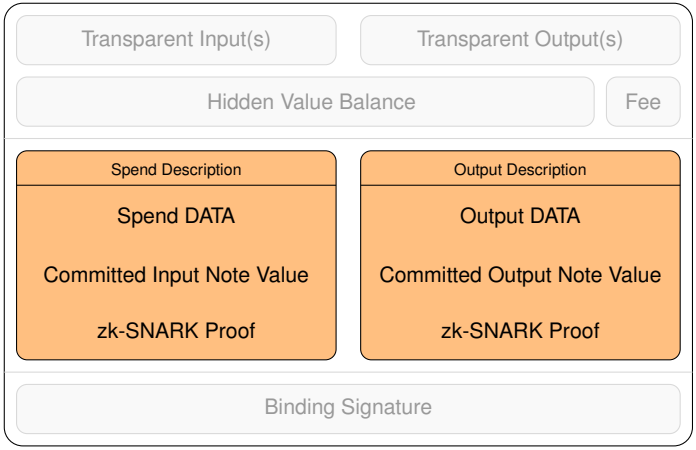


Subliminal Channels

- We found 3 subliminal channels by exploiting malleability of Pedersen's commitments and Groth16's zkSNARKs proofs:
  1. *Pedersen Subliminal Channel (commitment scheme)*
  2. *Inner Subliminal Channel (zkSNARK)*
  3. *Outer Subliminal Channel (zkSNARK)*

- **Key Idea:** use re-randomization until a desired *subliminal message* is successfully embedded.

Shielded Transaction Layout



Pedersen Subliminal Channel

- A note value v is committed to c with randomness r as

$$v \longrightarrow c = g^v h^r = \texttt{0xf2c71e906}$$

- c can be re-randomized to c' as

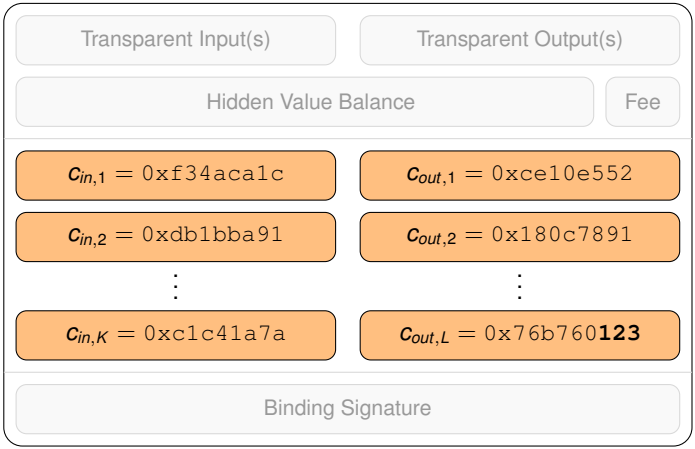
$$c \longrightarrow c' = c \cdot h^s = g^v h^{r+s}$$

- By selecting different random values s, we found that

$$c' = c \cdot h^s = \texttt{0x76b760}\mathbf{123}$$

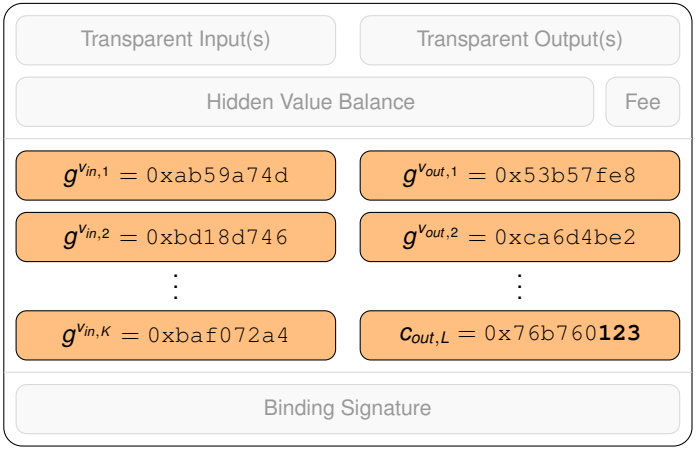
- c' embeds the message `123`.

Pedersen Subliminal Channel



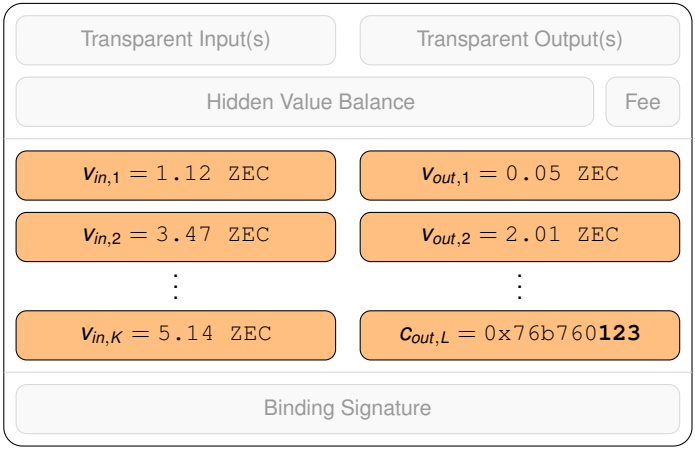
Detect tag $\longrightarrow$ *Partial decommitment* $\longrightarrow$ *Dictionary attack* $\longrightarrow$ *Full decommitment*

Pedersen Subliminal Channel



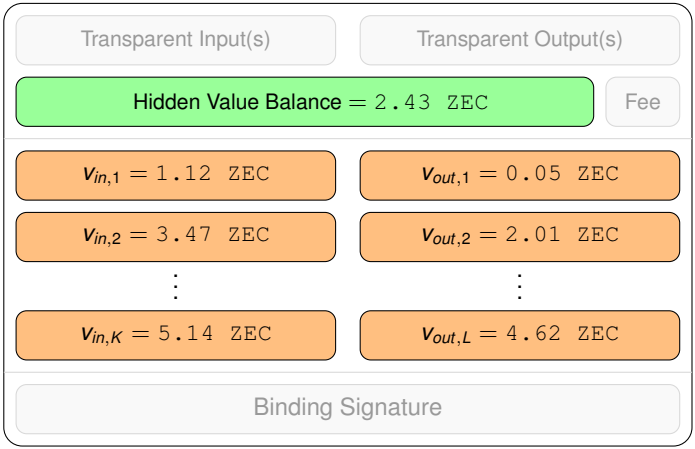
Detect tag $\longrightarrow$ *Partial decommitment* $\longrightarrow$ *Dictionary attack* $\longrightarrow$ *Full decommitment*

Pedersen Subliminal Channel



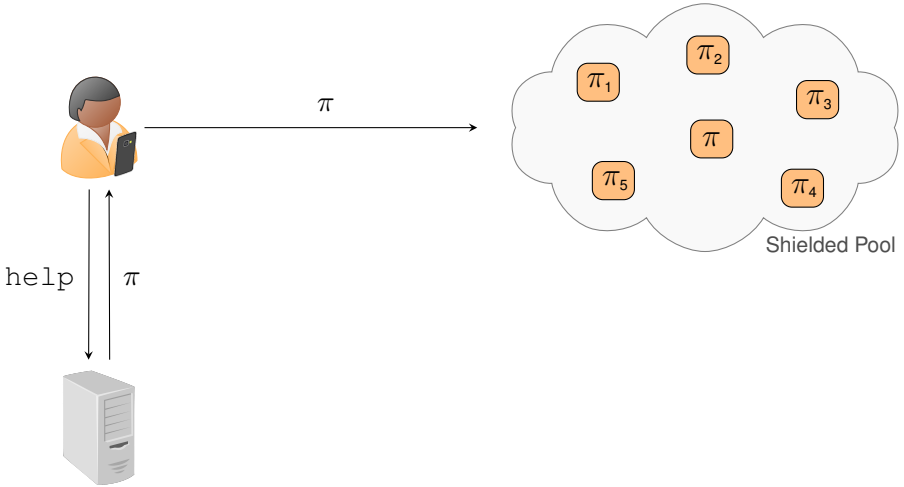
Detect tag $\longrightarrow$ *Partial decommitment* $\longrightarrow$ *Dictionary attack* $\longrightarrow$ *Full decommitment*

Pedersen Subliminal Channel

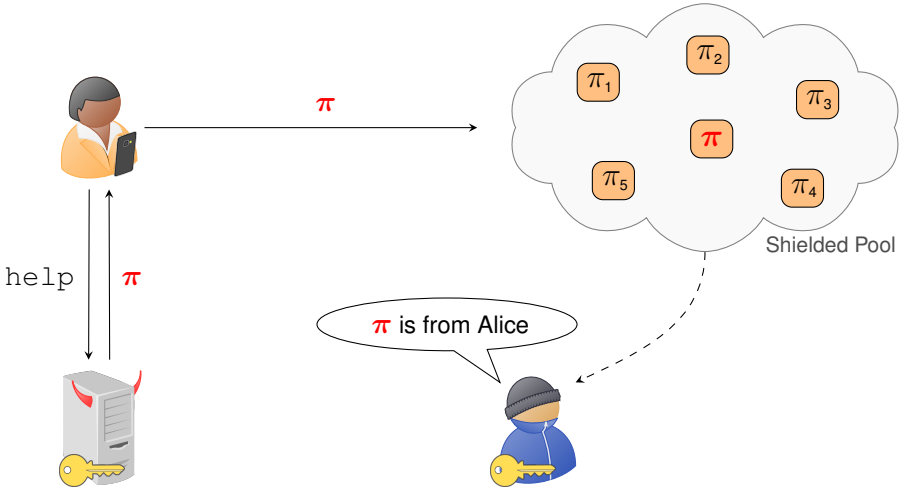


Detect tag $\longrightarrow$ *Partial decommitment* $\longrightarrow$ *Dictionary attack* $\longrightarrow$ *Full decommitment*

Decoupled Spend Authority

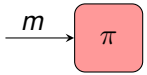


Decoupled Spend Authority



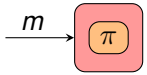
The Inner Subliminal Channel

- A zkSNARK proof is generated by choosing two different random values.
- A malicious proving system can iteratively select different randomness until the resulting π embeds the subliminal message.
- *'Inner'* because a message is embedded *before* π is finalized.



The Outer Subliminal Channel

- A proof π can be re-randomized using some non-expensive elliptic curve operations and without knowing any witness.
- π is iteratively re-randomized until the subliminal message is embedded.
- *'Outer'* because re-randomization is done on an already generated proof.

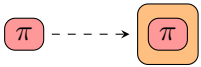


Implementation Results

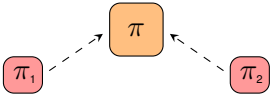
- We embedded 9 bytes in a fully shielded transaction with 1 shielded input and 2 shielded outputs (3 bytes per description).
- On a standard laptop, it took on average 3.0087s compared to 2.8412s normally needed (just a 6% increase).
- Our tagged transaction has a confirmed status on the Zcash testnet:

Countermeasures

- Use proof re-randomization to disrupt any embedded subliminal message.



- Combine two (even tagged) proofs for the same statement.



- Trusted Execution Environments could help to mitigate trust issues in proof delegation and transaction generation.

Summary

- Two different approaches for transaction tagging and linking in Zcash:

1. **Transaction Linking Attacks:**
   - Based on interplay of transparent and hidden transactions;
   - Verified with a rigorous statistical model.
2. **Subliminal Channels:**
   - Based on discovery of subliminal channels in cryptographic primitives used to build hidden transactions;
   - Embedded 3 bytes per description.