Zcash Protocol Specification
Version 2.0-draft-4

Sean Bowe — Daira Hopwood — Taylor Hornby — Nathan Wilcox

March 16, 2016

Contents

1 Introduction

Zcash is an implementation of the *Decentralized Anonymous Payment* scheme **Zerocash** [2] with some adjustments to terminology, functionality and performance. It bridges the existing *transparent* payment scheme used by **Bitcoin** with a *confidential* payment scheme protected by zero-knowledge succinct non-interactive arguments of knowledge (*zk-SNARKs*).

Changes from the original **Zerocash** are highlighted in magenta.

2 Caution

Zcash security depends on consensus. Should your program diverge from consensus, its security is weakened or destroyed. The cause of the divergence doesn't matter: it could be a bug in your program, it could be an error in this documentation which you implemented as described, or it could be you do everything right but other software on the network behaves unexpectedly. The specific cause will not matter to the users of your software whose wealth is lost.

Having said that, a specification of *intended* behaviour is essential for security analysis, understanding of the protocol, and maintenance of Zcash Core and related software. If you find any mistake in this specification, please contact `<security@z.cash>`. While the production **Zcash** network has yet to be launched, please feel free to do so in public even if you believe the mistake may indicate a security weakness.

3 Conventions

3.1 Integers, Bit Sequences, and Endianness

All integers in ***Zcash**-specific* encodings are unsigned, have a fixed bit length, and are encoded as big-endian. The definition of the encryption scheme based on AEAD_CHACHA20_POLY1305 [9] in § 6 *'In-band secret distribution'* on p. 10 uses length fields encoded as little-endian. Also, Curve25519 public and private keys are defined as byte sequences, which are converted from integers using little-endian encoding.

The notation **0x** followed by a string of **boldface** hexadecimal digits represents the corresponding integer converted from hexadecimal.

In bit layout diagrams, each box of the diagram represents a sequence of bits. The bit length is given explicitly in each box, except for the case of a single bit, or for the notation $[0]^n$ which represents the sequence of n zero bits. If the content of the box is a byte sequence, it is implicitly converted to a sequence of bits using big-endian order. The bit sequences are then concatenated in the order shown from left to right, and the result is converted to a sequence of bytes, again using big-endian order.

For example, the diagram

represents the byte sequence [**0x4A**, **0xBC**, **0xD1**, **0x23**].

The notation 1..N, used as a subscript, means the sequence of values with indices 1 through N inclusive. For example, $\mathsf{a}^{\mathsf{new}}_{\mathsf{pk},1..\mathrm{N}^{\mathsf{new}}}$ means the sequence $[\mathsf{a}^{\mathsf{new}}_{\mathsf{pk},1}, \mathsf{a}^{\mathsf{new}}_{\mathsf{pk},2}, \ldots \mathsf{a}^{\mathsf{new}}_{\mathsf{pk},\mathrm{N}^{\mathsf{new}}}]$.

The symbol $\bot$ is used to indicate unavailable information or a failed decryption.

3.2 Cryptographic Functions

CRH is a collision-resistant hash function. In **Zcash**, the *SHA-256 compression* function is used which takes a 512-bit block and produces a 256-bit hash. This is different from the *SHA-256* function, which hashes arbitrary-length sequences. [10]

PRF_x is a pseudo-random function seeded by x. Four *independent* PRF_x are needed in our scheme: $\mathsf{PRF}^{\mathsf{addr}}_x$, $\mathsf{PRF}^{\mathsf{sn}}_x$, $\mathsf{PRF}^{\mathsf{pk}}_x$, and PRF^{ρ}_x.

It is required that $\mathsf{PRF}^{\mathsf{sn}}_x$ and PRF^{ρ}_x be collision-resistant across all x — i.e. it should not be feasible to find $(x, y) \neq (x', y')$ such that $\mathsf{PRF}^{\mathsf{sn}}_x(y) = \mathsf{PRF}^{\mathsf{sn}}_{x'}(y')$, and similarly for PRF^{ρ}.

In **Zcash**, the *SHA-256 compression* function is used to construct all of these functions.

$$\mathsf{PRF}^{\mathsf{addr}}_x(t) := \mathsf{CRH}\left(\boxed{0}\boxed{0}\boxed{0}\boxed{0}\boxed{x\ \text{252 bit}}\boxed{[0]^{253}}\boxed{t\ \text{3 bit}}\right)$$

$$\mathsf{sn} = \mathsf{PRF}^{\mathsf{sn}}_{\mathsf{a_{sk}}}(\rho) := \mathsf{CRH}\left(\boxed{0}\boxed{1}\boxed{0}\boxed{0}\boxed{\mathsf{a_{sk}}\ \text{252 bit}}\boxed{\rho\ \text{256 bit}}\right)$$

$$\mathsf{h}_i = \mathsf{PRF}^{\mathsf{pk}}_{\mathsf{a_{sk}}}(i, \mathsf{h_{Sig}}) := \mathsf{CRH}\left(\boxed{0}\boxed{i\text{-}1}\boxed{0}\boxed{1}\boxed{\mathsf{a_{sk}}\ \text{252 bit}}\boxed{\mathsf{h_{Sig}}\ \text{256 bit}}\right)$$

$$\rho_i^{\mathsf{new}} = \mathsf{PRF}^{\rho}_{\varphi}(i, \mathsf{h_{Sig}}) := \mathsf{CRH}\left(\boxed{0}\boxed{i\text{-}1}\boxed{1}\boxed{0}\boxed{\varphi\ \text{252 bit}}\boxed{\mathsf{h_{Sig}}\ \text{256 bit}}\right)$$

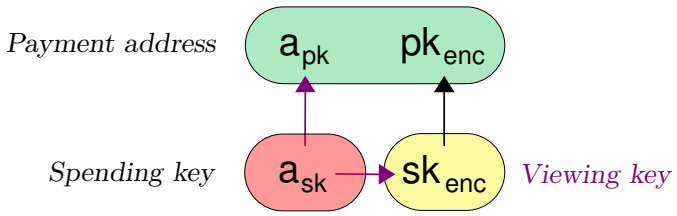
Note: The most significant four bits of the first byte are used to distinguish different uses of CRH, ensuring that the functions are independent. In addition to the inputs shown here, the first four bits `1100` (i.e. a first byte of **0xC**×) are used to distinguish uses of the full *SHA-256* hash function – see § 4.2.1 *'Coin Commitments'* on p. 5 and § 5.1 *'Computation of* $\mathsf{h_{Sig}}$*'* on p. 8.

4 Concepts

4.1 Payment Addresses and Spending Keys

A *key tuple* $(\mathsf{addr_{sk}}, \mathsf{addr_{pk}})$ is generated by users who wish to receive payments under this scheme. The *payment address* $\mathsf{addr_{pk}}$ is derived from the *spending key* $\mathsf{addr_{sk}}$.

The following diagram depicts the relations between key components. Arrows point from a component to any other component(s) that can be derived from it.



The composition of *payment addresses* and *spending keys* is a cryptographic protocol detail that should not normally be exposed to users. However, user-visible operations should be provided to obtain a *payment address* or *viewing key* from a *spending key*.

$\mathsf{a_{sk}}$ is 252 bits. $\mathsf{a_{pk}}$, $\mathsf{sk_{enc}}$, and $\mathsf{pk_{enc}}$, are each 256 bits.

a_{pk}, sk_{enc} and pk_{enc} are derived as follows:

$$a_{pk} := \mathsf{PRF}^{addr}_{a_{sk}}(0)$$
$$sk_{enc} := \mathsf{clamp}_{Curve25519}(\mathsf{PRF}^{addr}_{a_{sk}}(1))$$
$$pk_{enc} := \mathsf{Curve25519}(sk_{enc}, \underline{9})$$

where

- $\mathsf{Curve25519}(\underline{n}, \underline{q})$ performs point multiplication of the Curve25519 public key represented by the byte sequence $\underline{q}$ by the Curve25519 secret key represented by the byte sequence $\underline{n}$, as defined in section 2 of [3];
- $\underline{9}$ is the public byte sequence representing the Curve25519 base point;
- $\mathsf{clamp}_{Curve25519}(\underline{x})$ takes a 32-byte sequence $\underline{x}$ as input and returns a byte sequence representing a Curve25519 private key, with bits "clamped" as described in section 3 of [3]: "clear bits 0, 1, 2 of the first byte, clear bit 7 of the last byte, and set bit 6 of the last byte." Here the bits of a byte are numbered such that bit b has numeric weight 2^b.

Users can accept payment from multiple parties with a single $addr_{pk}$ and the fact that these payments are destined to the same payee is not revealed on the blockchain, even to the paying parties. *However* if two parties collude to compare a $addr_{pk}$ they can trivially determine they are the same. In the case that a payee wishes to prevent this they should create a distinct *payment address* for each payer.

4.2 Coins

A *coin* (denoted $\mathbf{c}$) is a tuple (a_{pk}, v, ρ, r) which represents that a value v is spendable by the recipient who holds the *spending key* a_{sk} corresponding to a_{pk}, as described in the previous section.

- a_{pk} is a 32-byte *authorization* public key of the recipient.
- v is a 64-bit unsigned integer representing the value of the *coin* in *zatoshi* (1 **ZEC** = 10^8 *zatoshi*).
- ρ is a 32-byte $\mathsf{PRF}^{sn}_{a_{sk}}$ preimage.
- r is a 24-byte *COMM trapdoor*.

r is randomly generated by the sender. ρ is generated from a random seed φ using $\mathsf{PRF}^{\rho}_{\varphi}$. Only a commitment to these values is disclosed publicly, which allows the tokens r and ρ to blind the value and recipient *except* to those who possess these tokens.

4.2.1 Coin Commitments

The underlying v and a_{pk} are blinded with ρ and r using the collision-resistant hash function `SHA256`. The resulting hash cm = `CoinCommitment(c)`.

$cm := \mathtt{SHA256}\Big($

8 bit **0xC0**	256 bit a_{pk}	64 bit v	256 bit ρ	192 bit r

$\Big)$

4.2.2 Serial numbers

A *serial number* (denoted sn) equals $\mathsf{PRF}^{sn}_{a_{sk}}(\rho)$. A *coin* is spent by proving knowledge of ρ and a_{sk} in zero knowledge while disclosing sn, allowing sn to be used to prevent double-spending.

4.2.3 Coin plaintexts and memo fields

Transmitted coins are stored on the blockchain in encrypted form, together with a *coin commitment* cm.

The *coin plaintexts* associated with a *Pour description* are encrypted to the respective *transmission* keys $\mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},1..N^{\mathsf{new}}}$, and the result forms part of a *transmitted coins ciphertext* (see § 6 *'In-band secret distribution'* on p. 10 for further details).

Each *coin plaintext* (denoted **cp**) consists of $(\mathsf{a}_{\mathsf{pk}}, \mathsf{v}, \rho, \mathsf{r}, \mathsf{memo})$.

The first four of these fields are as defined earlier. memo is a 64-byte *memo field* associated with this *coin*.

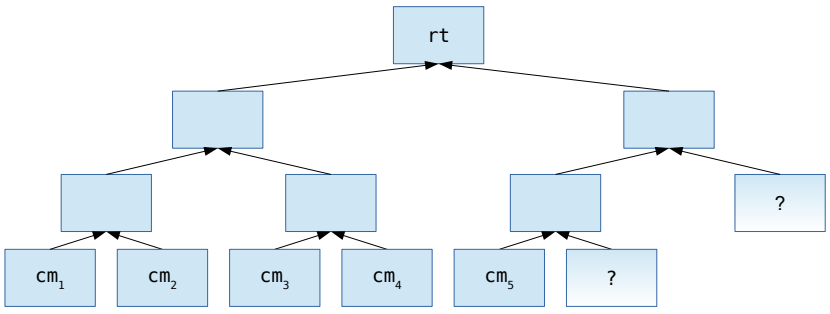
The usage of the *memo field* is by agreement between the sender and recipient of the *coin*. It should be encoded as a UTF-8 human-readable string [4], padded with zero bytes. Wallet software is expected to strip any trailing zero bytes and then display the resulting UTF-8 string to the recipient user, where applicable. Incorrect UTF-8-encoded byte sequences should be displayed as replacement characters (U+FFFD). This does not preclude uses of the *memo field* by automated software, but specification of such usage is not in the scope of this document.

The encoding of a *coin plaintext* consists of, in order:

a_{pk} (32 bytes)	v (8 bytes)	ρ (32 bytes)	r (24 bytes)	memo (64 bytes)

- 32 bytes specifying a_{pk}.
- 8 bytes specifying a big-endian encoding of v.
- 32 bytes specifying ρ.
- 24 bytes specifying r.
- 64 bytes specifying memo.

4.3 Coin Commitment Tree



The *coin commitment tree* is an *incremental merkle tree* of depth d used to store *coin commitments* that *Pour transfers* produce. Just as the *unspent transaction output set* (UTXO) used in Bitcoin, it is used to express the existence of value and the capability to spend it. However, unlike the UTXO, it is *not* the job of this tree to protect against double-spending, as it is append-only.

Blocks in the blockchain are associated (by all nodes) with the root of this tree after all of its constituent *Pour descriptions*' *coin commitments* have been entered into the tree associated with the previous block.

4.4 Spent Serials Map

Transactions insert *serial numbers* into a *spent serial numbers map* which is maintained alongside the UTXO by all nodes.

Eli: a tx is just a string, so it doesn't insert anything. Rather, nodes process tx's and the "good" ones lead to the addition of serials to the spent serials map.

Transactions that attempt to insert a *serial number* into this map that already exists within it are invalid as they are attempting to double-spend.

Eli: After defining *transaction*, one should define what a *legal tx* is (this definition depends on a particular blockchain [view]) and only then can one talk about "attempts" of transactions, and insertions of serial numbers into the spent serials map.

4.5 The Blockchain

At a given point in time, the *blockchain view* of each *full node* consists of a sequence of one or more valid *blocks*. Each *block* consists of a sequence of one or more *transactions*. In a given node's *blockchain view*, *treestates* are chained in an obvious way:

- The input *treestate* of the first *block* is the empty *treestate*.
- The input *treestate* of the first *transaction* of a *block* is the final *treestate* of the immediately preceding *block*.
- The input *treestate* of each subsequent *transaction* in a *block* is the output *treestate* of the immediately preceding *transaction*.
- The final *treestate* of a *block* is the output *treestate* of its last *transaction*.

An *anchor* is a Merkle tree root of a *treestate*, and uniquely identifies that *treestate* given the assumed security properties of the Merkle tree's hash function.

Each *transaction* is associated with a sequence of *Pour descriptions*. TODO: They also have a transparent value flow that interacts with the Pour v^{old}_{pub} and v^{new}_{pub}. Inputs and outputs are associated with a value.

The total value of the outputs must not exceed the total value of the inputs.

The *anchor* of the first *Pour description* in a *transaction* must refer to some earlier *block*'s final *treestate*.

The *anchor* of each subsequent *Pour description* may refer either to some earlier *block*'s final *treestate*, or to the output *treestate* of the immediately preceding *Pour description*.

These conditions act as constraints on the blocks that a *full node* will accept into its *blockchain view*.

We rely on Bitcoin-style consensus for *full nodes* to eventually converge on their views of valid *blocks*, and therefore of the sequence of *treestates* in those *blocks*.

Value pool Transaction inputs insert value into a *value pool*, and transaction outputs remove value from this pool. The remaining value in the pool is available to miners as a fee.

5 Pour Transfers and Descriptions

A *Pour description* is data included in a *block* that describes a *Pour transfer*, i.e. a confidential value transfer. This kind of value transfer is the primary **Zerocash**-specific operation performed by transactions; it uses, but should not be confused with, the *POUR circuit* used for the *zk-SNARK* proof and verification.

A *Pour transfer* spends N^{old} *coins* $\mathbf{c}^{old}_{1..N^{old}}$ and transparent input v^{old}_{pub}, and creates N^{new} *coins* $\mathbf{c}^{new}_{1..N^{new}}$ and transparent output v^{new}_{pub}. **Zcash** transactions have an additional field `vpour`, which is a sequence of *Pour descriptions*.

Each *Pour description* consists of:

`vpub_old` which is a value v^{old}_{pub} that the *Pour transfer* removes from the value pool.

`vpub_new` which is a value v^{new}_{pub} that the *Pour transfer* inserts into the value pool.

`anchor` which is a merkle root rt of the *coin commitment tree* at some block height in the past, or the merkle root produced by a previous pour in this transaction. Sean: We need to be more specific here.

`pourPubKey` which is an ECDSA public verification key using the secp256k1 curve and parameters defined in [11] and [12].

`pourSig` which is a signature on the *transaction* as specified in § 5.3 *'Non-malleability'* on p. 8, to be verified using `pourPubKey`.

`serials` which is an N^{old} size sequence of serials $\mathsf{sn}^{old}_{1..N^{old}}$.

`commitments` which is a N^{new} size sequence of *coin commitments* $\mathsf{cm}^{new}_{1..N^{new}}$.

`ephemeralKey` which is a Curve25519 public key epk.

`encCiphertexts` which is a N^{new} size sequence of ciphertext components, $\mathbf{C}^{enc}_{1..N^{new}}$.
(The preceding two fields form the *transmitted coins ciphertext*.)

`randomSeed` which is a 256-bit seed that must be chosen independently at random for each *Pour description*.

`vmacs` which is a N^{old} size sequence of message authentication tags $\mathsf{h}_{1..N^{old}}$ that bind h_{Sig} to each a_{sk} of the *Pour description*.

`zkproof` which is an encoding, as determined by the libsnark library [7], of the zero-knowledge proof $\pi_{\mathtt{POUR}}$.

TODO: Describe case where there are fewer than N^{old} real input coins.

5.1 Computation of h_{Sig}

Given a *Pour description*, we define:

$\mathsf{h}_{Sig} := \mathtt{SHA256}\Big($ | 8 bit **0xC1** | 256 bit sn^{old}_1 ... | 256 bit $\mathsf{sn}^{old}_{N^{old}}$ | `randomSeed` | `pourPubKey` | $\Big)$

5.2 Merkle root validity

A *Pour description* is valid if rt is a *coin commitment tree* root found in either the blockchain or a merkle root produced by inserting the *coin commitments* of a previous *Pour description* in the transaction to the *coin commitment tree* identified by that previous *Pour description*'s *anchor*.

5.3 Non-malleability

A *Pour description* is correctly signed if:

- `pourSig` can be verified as an encoding of a signature on TODO: what precisely?, using the ECDSA public key encoded as `pourPubKey`; and
- `pourSig` has an `s` value in the lower half of the possible range (i.e. `s` must be in the range from 0x1 to 0x7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF5D576E7357A4501DDFE92F46681B20A0, inclusive).

If s is not in the given range, the signature is treated as invalid.

The encoding of a signature is:

256 bit r	256 bit s

where r and s are as defined in [11].

The encoding of a public key is as defined in section E.2.3.2 of [13] for a compressed elliptic curve point with x-coordinate x_P and compressed y-coordinate $\tilde{y}_P$:

$[0]^6$	1	1 bit $\tilde{y}_P$	256 bit x_P

Note that only compressed public keys are valid.

The condition § 5.6 *'Non-malleability'* on p. 10 in the *zk-SNARK* statement ensures that a holder of all of $\mathsf{a}^{\mathsf{old}}_{\mathsf{sk},1..\mathrm{N}^{\mathsf{old}}}$ has authorized the use of the private key corresponding to `pourPubKey` to sign this transaction.

5.4 Balance

A *Pour transfer* can be seen, from the perspective of the transaction, as an input and an output simultaneously. $\mathsf{v}^{\mathsf{old}}_{\mathsf{pub}}$ takes value from the value pool and $\mathsf{v}^{\mathsf{new}}_{\mathsf{pub}}$ adds value to the value pool. As a result, $\mathsf{v}^{\mathsf{old}}_{\mathsf{pub}}$ is treated like an *output* value, whereas $\mathsf{v}^{\mathsf{new}}_{\mathsf{pub}}$ is treated like an *input* value.

Note that unlike original **Zerocash** [2], **Zcash** does not have a distinction between Mint and Pour transfers. The addition of $\mathsf{v}^{\mathsf{old}}_{\mathsf{pub}}$ to a *Pour description* subsumes the functionality of Mint. Also, *Pour descriptions* are indistinguishable regardless of the number of real input *coins*.

5.5 Commitments and Serial Numbers

A *transaction* that contains one or more *Pour descriptions*, when entered into the blockchain, appends to the *coin commitment tree* with all constituent *coin commitments*. All of the constituent *serial numbers* are also entered into the *spent serial numbers map* of the *blockchain view and mempool*. A *transaction* is not valid if it attempts to add a *serial number* to the *spent serial numbers map* that already exists in the map.

5.6 Pour Circuit and Proofs

In **Zcash**, $\mathrm{N}^{\mathsf{old}}$ and $\mathrm{N}^{\mathsf{new}}$ are both 2.

A valid instance of $\pi_{\mathtt{POUR}}$ assures that given a *primary input*:

$$(\mathsf{rt}, \mathsf{sn}^{\mathsf{old}}_{1..\mathrm{N}^{\mathsf{old}}}, \mathsf{cm}^{\mathsf{new}}_{1..\mathrm{N}^{\mathsf{new}}}, \mathsf{v}^{\mathsf{old}}_{\mathsf{pub}}, \mathsf{v}^{\mathsf{new}}_{\mathsf{pub}}, \mathsf{h}_{\mathsf{Sig}}, \mathsf{h}_{1..\mathrm{N}^{\mathsf{old}}}),$$

there exists a witness of *auxiliary input*:

$$(\mathsf{path}_{1..\mathrm{N}^{\mathsf{old}}}, \mathbf{c}^{\mathsf{old}}_{1..\mathrm{N}^{\mathsf{old}}}, \mathsf{a}^{\mathsf{old}}_{\mathsf{sk},1..\mathrm{N}^{\mathsf{old}}}, \mathbf{cp}^{\mathsf{new}}_{1..\mathrm{N}^{\mathsf{new}}}, \varphi)$$

where:

for each $i \in \{1..\mathrm{N}^{\mathsf{old}}\}$: $\mathbf{c}^{\mathsf{old}}_i = (\mathsf{a}^{\mathsf{old}}_{\mathsf{pk},i}, \mathsf{v}^{\mathsf{old}}_i, \rho^{\mathsf{old}}_i, \mathsf{r}^{\mathsf{old}}_i)$;

for each $i \in \{1..\mathrm{N}^{\mathsf{new}}\}$: $\mathbf{c}^{\mathsf{new}}_i = (\mathsf{a}^{\mathsf{new}}_{\mathsf{pk},i}, \mathsf{v}^{\mathsf{new}}_i, \rho^{\mathsf{new}}_i, \mathsf{r}^{\mathsf{new}}_i)$

such that the following conditions hold:

Merkle path validity for each $i \in \{1..\mathsf{N}^{\mathsf{old}}\} \mid \mathsf{v}_i^{\mathsf{old}} \neq 0$: path_i must be a valid path of depth d from $\mathtt{CoinCommitment}(\mathbf{c}_i^{\mathsf{old}})$ to *coin commitment tree* root rt.

Balance $\mathsf{v}_{\mathsf{pub}}^{\mathsf{old}} + \sum_{i=1}^{\mathsf{N}^{\mathsf{old}}} \mathsf{v}_i^{\mathsf{old}} = \mathsf{v}_{\mathsf{pub}}^{\mathsf{new}} + \sum_{i=1}^{\mathsf{N}^{\mathsf{new}}} \mathsf{v}_i^{\mathsf{new}}$.

Serial integrity for each $i \in \{1..\mathsf{N}^{\mathsf{new}}\}$: $\mathsf{sn}_i^{\mathsf{old}} = \mathsf{PRF}^{\mathsf{sn}}_{\mathsf{a}_{\mathsf{sk},i}^{\mathsf{old}}}(\rho_i^{\mathsf{old}})$.

Spend authority for each $i \in \{1..\mathsf{N}^{\mathsf{old}}\}$: $\mathsf{a}_{\mathsf{pk},i}^{\mathsf{old}} = \mathsf{PRF}^{\mathsf{addr}}_{\mathsf{a}_{\mathsf{sk},i}^{\mathsf{old}}}(0)$.

Non-malleability for each $i \in \{1..\mathsf{N}^{\mathsf{old}}\}$: $\mathsf{h}_i = \mathsf{PRF}^{\mathsf{pk}}_{\mathsf{a}_{\mathsf{sk},i}^{\mathsf{old}}}(i, \mathsf{h}_{\mathsf{Sig}})$.

Uniqueness of ρ_i^{new} for each $i \in \{1..\mathsf{N}^{\mathsf{new}}\}$: $\rho_i^{\mathsf{new}} = \mathsf{PRF}^{\rho}_{\varphi}(i, \mathsf{h}_{\mathsf{Sig}})$.

Commitment integrity for each $i \in \{1..\mathsf{N}^{\mathsf{new}}\}$: $\mathsf{cm}_i^{\mathsf{new}} = \mathtt{CoinCommitment}(\mathbf{c}_i^{\mathsf{new}})$.

6 In-band secret distribution

In order to transmit the secret v, ρ, and r (necessary for the recipient to later spend) and also a *memo field* to the recipient *without* requiring an out-of-band communication channel, the *transmission* public key $\mathsf{pk}_{\mathsf{enc}}$ is used to encrypt these secrets. The recipient's possession of the associated $(\mathsf{addr}_{\mathsf{pk}}, \mathsf{addr}_{\mathsf{sk}})$ (which contains both a_{pk} and $\mathsf{sk}_{\mathsf{enc}}$) is used to reconstruct the original *coin* and *memo field*.

All of the resulting ciphertexts are combined to form a *transmitted coins ciphertext*.

6.1 Encryption

Let $\mathsf{SymEncrypt}_{\mathsf{K}}(\mathbf{P})$ be authenticated encryption using a variation of AEAD_CHACHA20_POLY1305 [9] encryption of plaintext $\mathbf{P}$, with empty "associated data", all-zero nonce $[0]^{96}$, and 256-bit key K. The variation is that the ChaCha20 keystream is used to encrypt the plaintext starting immediately after the 32 bytes of the Poly1305 key, without discarding 32 bytes as in [9].

Similarly, let $\mathsf{SymDecrypt}_{\mathsf{K}}(\mathbf{C})$ be decryption using the same AEAD_CHACHA20_POLY1305 variation of ciphertext $\mathbf{C}$, with empty "associated data", all-zero nonce $[0]^{96}$, and 256-bit key K. The result is either the plaintext byte sequence, or $\perp$ indicating failure to decrypt.

Define $\mathsf{KDF}(\mathsf{dhsecret}_i, \mathsf{epk}, \mathsf{pk}_{\mathsf{enc},i}^{\mathsf{new}}, i) :=$

$$\mathtt{SHA256}\Big(\boxed{\text{8 bit } \mathbf{0xC2}}\boxed{\text{256 bit } \mathsf{dhsecret}_i}\boxed{\text{256 bit } \mathsf{epk}}\boxed{\text{256 bit } \mathsf{pk}_{\mathsf{enc},i}^{\mathsf{new}}}\boxed{\text{8 bit } i-1}\Big).$$

Let $\mathsf{pk}_{\mathsf{enc},1..\mathsf{N}^{\mathsf{new}}}^{\mathsf{new}}$ be the Curve25519 public keys for the intended recipient addresses of each new *coin*, and let $\mathbf{cp}_{1..\mathsf{N}^{\mathsf{new}}}$ be the *coin plaintexts*.

Then to encrypt:

- Generate a new Curve25519 (public, private) key pair $(\mathsf{epk}, \mathsf{esk})$.
- For $i \in \{1..\mathsf{N}^{\mathsf{new}}\}$,
  - Let $\mathbf{P}_i^{\mathsf{enc}}$ be the raw encoding of $\mathbf{cp}_i$.

- Let $\mathsf{dhsecret}_i := \mathsf{Curve25519}(\mathsf{esk}, \mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},i})$.
- Let $\mathsf{K}^{\mathsf{enc}}_i := \mathsf{KDF}(\mathsf{dhsecret}_i, \mathsf{epk}, \mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},i}, i)$.
- Let $\mathbf{C}^{\mathsf{enc}}_i := \mathsf{SymEncrypt}_{\mathsf{K}^{\mathsf{enc}}_i}(\mathbf{P}^{\mathsf{enc}}_i)$.

The resulting *transmitted coins ciphertext* is $(\mathsf{epk}, \mathbf{C}^{\mathsf{enc}}_{1..\mathrm{N}^{\mathsf{new}}})$.

6.2 Decryption by a Recipient

Let $(\mathsf{pk}_{\mathsf{enc}}, \mathsf{sk}_{\mathsf{enc}})$ be the recipient's Curve25519 (public, private) key pair, and let $\mathsf{cm}^{\mathsf{new}}_{1..\mathrm{N}^{\mathsf{new}}}$ be the coin commitments of each output coin. Then for each $i \in \{1..\mathrm{N}^{\mathsf{new}}\}$, the recipient will attempt to decrypt that ciphertext component as follows:

- Let $\mathsf{dhsecret}_i := \mathsf{Curve25519}(\mathsf{sk}_{\mathsf{enc}}, \mathsf{epk})$.
- Let $\mathsf{K}^{\mathsf{enc}}_i := \mathsf{KDF}(\mathsf{dhsecret}_i, \mathsf{epk}, \mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},i}, i)$.
- Return $\mathtt{DecryptCoin}(\mathsf{K}^{\mathsf{enc}}_i, \mathbf{C}^{\mathsf{enc}}_i, \mathsf{cm}^{\mathsf{new}}_i)$.

$\mathtt{DecryptCoin}(\mathsf{K}^{\mathsf{enc}}_i, \mathbf{C}^{\mathsf{enc}}_i, \mathsf{cm}^{\mathsf{new}}_i)$ is defined as follows:

- Let $\mathbf{P}^{\mathsf{enc}}_i := \mathsf{SymDecrypt}_{\mathsf{K}^{\mathsf{enc}}_i}(\mathbf{C}^{\mathsf{enc}}_i)$.
- If $\mathbf{P}^{\mathsf{enc}}_i = \bot$, return $\bot$.
- Extract $\mathbf{cp}_i = (\mathsf{a}^{\mathsf{new}}_{\mathsf{pk},i}, \mathsf{v}^{\mathsf{new}}_i, \rho^{\mathsf{new}}_i, \mathsf{r}^{\mathsf{new}}_i, \mathsf{memo}_i)$ from $\mathbf{P}^{\mathsf{enc}}_i$.
- If $\mathtt{CoinCommitment}((\mathsf{a}^{\mathsf{new}}_{\mathsf{pk},i}, \mathsf{v}^{\mathsf{new}}_i, \rho^{\mathsf{new}}_i, \mathsf{r}^{\mathsf{new}}_i)) \neq \mathsf{cm}^{\mathsf{new}}_i$, return $\bot$, else return $\mathbf{cp}_i$.

Note that this corresponds to step 3 (b) i. and ii. (first bullet point) of the Receive algorithm shown in Figure 2 of [2].

To test whether a *coin* is unspent in a particular *blockchain view* also requires the *authorization* private key a_{sk}; the coin is unspent if and only if $\mathsf{sn} = \mathsf{PRF}^{\mathsf{sn}}_{\mathsf{a}_{\mathsf{sk}}}(\rho)$ is not in the *spent serial number set* for that *blockchain view*.

Note that a coin may change from being unspent to spent on a given *blockchain view*, as transactions are added to that view. Also, blockchain reorganisations may cause the transaction in which a coin was output to no longer be on the consensus blockchain.

6.3 Commentary

The public key encryption used in this part of the protocol is based loosely on other encryption schemes based on Diffie-Hellman over an elliptic curve, such as ECIES or the crypto_box_seal algorithm defined in libsodium [8]. Note that:

- The same ephemeral key is used for all encryptions to the recipient keys in a given *Pour description*.
- In addition to the Diffie-Hellman secret, the KDF takes as input the public keys of both parties, and the index i.
- The nonce parameter to AEAD_CHACHA20_POLY1305 is not used.

7 Encoding Addresses and Keys

This section describes how **Zcash** encodes *payment addresses* and *spending keys*.

Addresses and keys can be encoded as a byte sequence; this is called the *raw encoding*. This byte sequence can then be further encoded using Base58Check. The Base58Check layer is the same as for upstream **Bitcoin** addresses [1].

SHA-256 compression function outputs are always represented as sequences of 32 bytes.

The language consisting of the following encoding possibilities is prefix-free.

7.1 Transparent Payment Addresses

These are encoded in the same way as in **Bitcoin** [1].

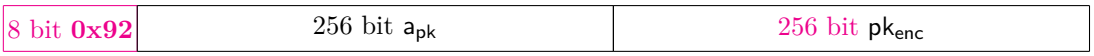
7.2 Transparent Private Keys

These are encoded in the same way as in **Bitcoin** [1].

7.3 Private Payment Addresses

A *payment address* consists of a_{pk} and $\mathsf{pk}_{\mathsf{enc}}$. a_{pk} is a SHA-256 compression function output. $\mathsf{pk}_{\mathsf{enc}}$ is a Curve25519 public key, for use with the encryption scheme defined in § 6 *'In-band secret distribution'* on p. 10.

The raw encoding of a *payment address* consists of:



- A byte, **0x92**, indicating this version of the raw encoding of a **Zcash** public address.
- 256 bits specifying a_{pk}.
- 256 bits specifying $\mathsf{pk}_{\mathsf{enc}}$, using the normal encoding of a Curve25519 public key [3].

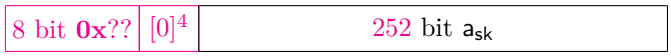
Daira: check that this lead byte is distinct from other Bitcoin stuff, and produces 'z' as the Base58Check leading character.

Nathan: what about the network version byte?

7.4 Spending Keys

A *spending key* consists of a_{sk}.

The raw encoding of a *spending key* consists of, in order:



- A byte **0x**?? indicating this version of the raw encoding of a **Zcash** *spending key*.
- 4 zero padding bits.
- 252 bits specifying a_{sk}.

Note that, consistent with big-endian encoding, the zero padding occupies the high-order 4 bits of the second byte.

Daira: check that this lead byte is distinct from other Bitcoin stuff, and produces a suitable Base58Check leading character.

Nathan: what about the network version byte?

8 Differences from the Zerocash paper

8.1 Transaction Structure

Zerocash introduces two new operations, which are described in the paper as new transaction types, in addition to the original transaction type of the cryptocurrency on which it is based (e.g. **Bitcoin**).

In **Zcash**, there is only the original **Bitcoin** transaction type, which is extended to contain a sequence of zero or more **Zcash**-specific operations.

This allows for the possibility of chaining transfers of protected value in a single transaction, e.g. to spend a protected coin that has just been created. (In **Zcash**, we refer to value stored in UTXOs as "transparent", and value stored in Pour output coins as "protected".) This was not possible in the **Zerocash** design without using multiple transactions. It also allows transparent and protected transfers to happen atomically — possibly under the control of nontrivial script conditions, at some cost in distinguishability.

8.2 Unification of Mints and Pours

In the original **Zerocash** protocol, there were two kinds of transaction relating to protected coins:

- a "Mint" transaction takes value from transparent UTXOs as input and produces a new protected coin as output.
- a "Pour" transaction takes up to N^{old} protected coins as input, and produces up to N^{new} protected coins and a transparent UTXO as output.

Only "Pour" transactions included a *zk-SNARK* proof.

In **Zcash**, the sequence of operations added to a transaction (described in § 8.1 *'Transaction Structure'* on p. 13) consists only of Pours. A Pour is generalized to take a transparent UTXO as input, allowing Pours to subsume the functionality of Mints. An advantage of this is that a transaction that takes input from an UTXO can produce up to N^{new} output coins, improving the indistinguishability properties of the protocol. A related change conceals the input arity of the Pour: an unused (zero-value) input is indistinguishable from an input that takes value from a coin.

This unification also simplifies the fix to the Faerie Gold attack described below, since no special case is needed for Mints.

8.3 Memo fields

Zerocash adds a memo field sent from the creator of a Pour to the recipient of each output coin. This feature is described in more detail in § 4.2.3 *'Coin plaintexts and memo fields'* on p. 6.

8.4 Faerie Gold attack and fix

When a protected *coin* is created in **Zerocash**, the creator is supposed to choose a new ρ value at random. The *serial number* of the *coin* is derived from its *spending key* ($\mathsf{a_{sk}}$) and ρ. The *coin commitment* is derived from the recipient address component $\mathsf{a_{pk}}$, the value v, and the commitment trapdoor r, as well as ρ. However nothing prevents creating multiple *coins* with different v and r (hence different *coin commitments*) but the same ρ.

An adversary can use this to mislead a coin recipient, by sending two coins both of which are verified as valid by $\mathsf{Receive}$ (as defined in Figure 2 of [2]), but only one of which can be spent.

We call this a "Faerie Gold" attack — referring to various Celtic legends in which faeries pay mortals in what appears to be gold, but which soon after reveals itself to be leaves, gorse blossoms, gingerbread cakes, or other less valuable things [6].

This attack does not violate the security definitions given in [2]. The issue could be framed as a problem either with the definition of Completeness, or the definition of Balance:

- The Completeness property asserts that a validly received *coin* can be spent provided that its *serial number* does not appear on the ledger. This does not take into account the possibility that distinct *coins*, which are validly received, could have the same *serial number*. That is, the security definition depends on a protocol detail –*serial numbers*– that is not part of the intended abstract security property, and that could be implemented incorrectly.
- The Balance property only asserts that an adversary cannot obtain *more* funds than they have minted or received via payments. It does not prevent an adversary from causing others' funds to decrease. In a Faerie Gold attack, an adversary can cause spending of a *coin* to reduce (to zero) the effective value of another *coin* for which the attacker does not know the *spending key*, which violates an intuitive conception of global balance.

These problems with the security definitions need to be repaired, but doing so is outside the scope of this specification. Here we only describe how **Zcash** addresses the immediate attack.

It would be possible to address the attack by requiring that a recipient remember all of the ρ values for all coins they have ever received, and reject duplicates (as proposed in [5]). However, this requirement would interfere with the intended **Zcash** feature that a holder of a *spending key* can recover access to (and be sure that they are able to spend) all of their funds, even if they have forgotten everything but the *spending key*.

Instead, **Zcash** enforces that an adversary must choose distinct values for each ρ, by making use of the fact that all of the *serial numbers* in *Pour descriptions* that appear in a valid *blockchain view* must be distinct. The *serial numbers* are used as input to `SHA256` to derive a public value $\mathsf{h_{Sig}}$ which uniquely identifies the transaction, as described in § 5.1 *'Computation of* $\mathsf{h_{Sig}}$*'* on p. 8. ($\mathsf{h_{Sig}}$ was already used in **Zerocash** in a way that requires it to be unique in order to maintain indistinguishability of *Pour descriptions*; adding the *serial numbers* to the input of the hash used to calculate it has the effect of making this uniqueness property robust even if the *transaction* creator is an adversary.)

The ρ value for each output coin is then derived from a random private seed φ and $\mathsf{h_{Sig}}$ using $\mathsf{PRF}^{\rho}_{\varphi}$. The correct construction of ρ for each output coin is enforced by the circuit (see § 5.6 *'Uniqueness of* ρ_i^{new}*'* on p. 10).

Now even if the creator of a *Pour description* does not choose φ randomly, uniqueness of *serial numbers* and collision resistance of both `SHA256` and PRF^{ρ} will ensure that the derived ρ values are unique, at least for any two *Pour descriptions* that get into a valid *blockchain view*. This is sufficient to prevent the Faerie Gold attack.

8.5 Internal hash collision attack and fix

The **Zerocash** security proof requires that the composition of $\mathsf{COMM_r}$ and $\mathsf{COMM_s}$ is a computationally binding commitment to its inputs $\mathsf{a_{pk}}$, v, and ρ. However, the instantiation of $\mathsf{COMM_r}$ and $\mathsf{COMM_s}$ in section 5.1 of the paper did not meet the definition of a binding commitment at a 128-bit security level. Specifically, the internal hash of $\mathsf{a_{pk}}$ and ρ is truncated to 128 bits (motivated by providing statistical hiding security). This allows an attacker, with a work factor on the order of 2^{64}, to find distinct values of ρ with colliding outputs of the truncated hash, and therefore the same *coin commitment*. This would have allowed such an attacker to break the balance property by double-spending coins, potentially creating arbitrary amounts of currency for themself.

Zcash uses a simpler construction with a single `SHA256` evaluation for the commitment. The motivation for the nested construction in **Zerocash** was to allow Mint transactions to be publically verified without requiring a ZK proof (as described under step 3 in section 1.3 of [2]). Since **Zcash** combines "Mint" and "Pour" transactions into a generalized Pour which always uses a ZK proof, it does not require the nesting. A side benefit is that this reduces the number of `SHA256Compress` evaluations needed to compute each *coin commitment* from three to two, saving a total of four `SHA256Compress` evaluations in the *`POUR` circuit*.

Note that **Zcash** coin commitments are not statistically hiding, and so **Zcash** does not support the "everlasting anonymity" property described in section 8.1 of the **Zerocash** paper [2], even when used as described in that section. While it is possible to define a statistically hiding, computationally binding commitment scheme for this use at a 128-bit security level, the overhead of doing so within the circuit was not considered to justify the benefits.

8.6 Changes to PRF inputs and truncation

TODO:

8.7 In-band secret distribution

TODO:

8.8 Miscellaneous

- The paper defines a coin as a tuple $(\mathsf{a_{pk}}, \mathsf{v}, \rho, \mathsf{r}, \mathsf{s}, \mathsf{cm})$, whereas this specification defines it as $(\mathsf{a_{pk}}, \mathsf{v}, \rho, \mathsf{r})$. This is just a clarification, because the instantiation of $\mathsf{COMM_s}$ in section 5.1 of the paper did not use s (and neither does the new instantiation of `CoinCommitment`). cm can be computed from the other fields.

9 Acknowledgements

The inventors of **Zerocash** are Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza.

The authors would like to thank everyone with whom they have discussed the **Zerocash** protocol design; in addition to the inventors, this includes Mike Perry, Isis Lovecruft, Leif Ryge, Andrew Miller, Zooko Wilcox, Samantha Hulsey, and no doubt others.

The Faerie Gold attack was found by Zooko Wilcox. The internal hash collision attack was found by Taylor Hornby.

10 References

[1] Base58Check encoding – bitcoin wiki. `https://en.bitcoin.it/wiki/Base58Check_encoding`. Accessed: 2016-01-26.

[2] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized Anonymous Payments from Bitcoin. In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland) 2014*, pages 459–474. IEEE, 2014.

[3] Daniel Bernstein. Curve25519: new Diffie-Hellman speed records. In *Public Key Cryptography - PKC 2006. Proceedings of the 9th International Conference on Theory and Practice in Public-Key Cryptography, New York, NY, USA, April 24-26*. Springer-Verlag, 2006. Document ID: 4230efdfa673480fc079449d90f322c0. Date: 2006-02-09. `http://cr.yp.to/papers.html#curve25519`.

[4] The Unicode Consortium. *The Unicode Standard*. The Unicode Consortium, 2015. `http://www.unicode.org/versions/latest/`.

[5] Christina Garman, Matthew Green, and Ian Miers. Accountable Privacy for Decentralized Anonymous Payments. Cryptology ePrint Archive: Report 2016/061. `https://eprint.iacr.org/2016/061`. Last revised 24 Jan 2016.

[6] Eddie Lenihan and Carolyn Eve Green. *Meeting the Other Crowd: The Fairy Stories of Hidden Ireland*. 2004. Pages 109–110. ISBN: 1-58542-206-1.

[7] libsnark: a c++ library for zksnark proofs. `https://github.com/scipr-lab/libsnark`. Accessed: 2016-03-15.

[8] libsodium documentation: Sealed boxes. `https://download.libsodium.org/doc/public-key_cryptography/sealed_boxes.html`. Accessed: 2016-02-01.

[9] Yoav Nir and Adam Langley. Request for Comments 7539: ChaCha20 and Poly1305 for IETF Protocols. Internet Research Task Force (IRTF). https://tools.ietf.org/html/rfc7539. As modified by verified errata at https://www.rfc-editor.org/errata_search.php?rfc=7539.

[10] NIST. FIPS 180-4: Secure Hash Standard (SHS). http://csrc.nist.gov/publications/PubsFIPS.html#180-4, August 2015. DOI: 10.6028/NIST.FIPS.180-4.

[11] Certicom Research. Standards for Efficient Cryptography 2 (SEC 2). http://www.secg.org/sec2-v2.pdf, January 27 2010. Version 2.0.

[12] Secp256k1 – bitcoin wiki. https://en.bitcoin.it/wiki/Secp256k1. Accessed: 2016-03-14.

[13] IEEE Computer Society. *IEEE Std 1363-2000: IEEE Standard Specifications for Public-Key Cryptography*. Institute of Electrical and Electronic Engineers, 2000. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=891000&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F7168%2F19282%2F00891000. Accessed 2016-03-15.