

Zcash Protocol Specification

Version 2.0-alpha-1

Sean Bowe — Daira Hopwood — Taylor Hornby — Nathan Wilcox

March 31, 2016

Contents

1	Introduction	3
2	Caution	3
3	Conventions	3
3.1	Integers, Bit Sequences, and Endianness	3
3.2	Cryptographic Functions	4
4	Concepts	5
4.1	Payment Addresses and Spending Keys	5
4.2	Notes	6
4.2.1	Note Commitments	6
4.2.2	Nullifiers	6
4.2.3	Note Plaintexts and Memo Fields	6
4.3	Note Commitment Tree	7
4.4	Nullifier Set	8
4.5	The Blockchain	8
5	JoinSplit Operations and Descriptions	9
5.1	Computation of h_{sig}	10
5.2	Merkle root validity	10
5.3	Non-malleability	10
5.4	Balance	11
5.5	Note Commitments and Nullifiers	12
5.6	<i>JoinSplit</i> circuit and Proofs	12
6	In-band secret distribution	13

6.1	Encryption	13
6.2	Decryption by a Recipient	13
6.3	Commentary	14
7	Encoding Addresses and Keys	14
7.1	Transparent Payment Addresses	14
7.2	Transparent Private Keys	14
7.3	Protected Payment Addresses	15
7.4	Spending Keys	15
8	Differences from the Zerocash paper	15
8.1	Transaction Structure	15
8.2	Unification of Mints and Pours	16
8.3	Memo Fields	16
8.4	Faerie Gold attack and fix	16
8.5	Internal hash collision attack and fix	17
8.6	Changes to PRF inputs and truncation	17
8.7	In-band secret distribution	17
8.8	Miscellaneous	18
9	Acknowledgements	18
10	References	18

1 Introduction

Eli: A few general comments that will re-appear numerous times:

- The “intended usage” explanations are confusing: What happens if some player does not play as intended? Suggest using standard Crypto terminology: the algorithms specified in the paper refer to the *honest* player(s). Any deviation is treated non-honest. Some deviations harm only their perpetrator, and we should state this; other deviations threaten other honest players and we should explain how these are mitigated.
- Suggest having two separate parts: first (i) an abstract functionality, stated in terms of crypto primitives with a parameterized security parameter, and (ii) concrete instantiations. I’ll call these “abstract” and “instantiation” later on.

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

Eli: Should this section appear in this paper? This paper describes *our implementation* so what does divergence mean? Perhaps this refers to non-honest players? **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.

Eli: I don’t understand what intended behavior means? This paper specifies how an *honest player* should act, and whenever there’s deviation we should have something that mitigates it. 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

Eli: Suggest this subsection be moved to “instantiation”

All integers in *Zcash-specific* encodings are unsigned, have a fixed bit length, and are encoded in little-endian byte order. The definition of the encryption scheme based on AEAD.CHACHA20.POLY1305 [11] in §6 ‘*In-band secret distribution*’ on p. 13 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.

The notation “...” represents the given string represented as a sequence of bytes in US-ASCII. For example, “**abc**” represents the byte sequence [**0x61**, **0x62**, **0x63**].

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.

The entire diagram represents the sequence of *bytes* formed by first concatenating these bit sequences, and then treating each subsequence of 8 bits as a byte with the bits ordered from *most significant* to *least significant*. Thus the *most significant* bit in each byte is toward the left of a diagram. Where bit fields are used, the text will clarify their position in each case.

$\text{LeadingBytes}_k(x)$, where k is an integer, returns the leading (initial) k bytes of x .

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

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

3.2 Cryptographic Functions

Eli: Would be good to start with “abstract”, using only a single security parameter λ and multiples of it, and then in “instantiations” have the specific details. In more detail, in “abstract” we’ll have only CRH with security λ , and multiple PRF_a^b ’s all with same (?) security λ , and we demand that the PRFs are “computationally pairwise independent”, i.e., PRF_a^b is pseudorandom given $\text{PRF}_{a'}^{b'}$ whenever $(a, b) \neq (a', b')$.

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. [12]

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

It is required that PRF_x^{nf} and PRF_x^{p} be collision-resistant across all x — i.e. it should not be feasible to find $(x, y) \neq (x', y')$ such that $\text{PRF}_x^{\text{nf}}(y) = \text{PRF}_{x'}^{\text{nf}}(y')$, and similarly for PRF_x^{p} . Eli: we likely need more than just not having a collision. Likely various bad things would happen if PRF_x^{p} can be predicted given $\text{PRF}_{x'}^{\text{p}}$. So we really need them to be pairwise distinct pseudorandom functions.

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

$$\begin{aligned}
\text{PRF}_x^{\text{addr}}(t) &:= \text{CRH} \left(\begin{array}{|c|c|c|c|} \hline 1 & 1 & 0 & 0 \\ \hline \end{array} \parallel \begin{array}{|c|} \hline 252 \text{ bit } x \\ \hline \end{array} \parallel \begin{array}{|c|} \hline 8 \text{ bit } t \\ \hline \end{array} \parallel \begin{array}{|c|} \hline [0]^{248} \\ \hline \end{array} \right) \\
\text{nf} = \text{PRF}_{a_{\text{sk}}}^{\text{nf}}(\rho) &:= \text{CRH} \left(\begin{array}{|c|c|c|c|} \hline 1 & 1 & 1 & 0 \\ \hline \end{array} \parallel \begin{array}{|c|} \hline 252 \text{ bit } a_{\text{sk}} \\ \hline \end{array} \parallel \begin{array}{|c|} \hline 256 \text{ bit } \rho \\ \hline \end{array} \right) \\
h_i = \text{PRF}_{a_{\text{sk}}}^{\text{pk}}(i, h_{\text{Sig}}) &:= \text{CRH} \left(\begin{array}{|c|c|c|c|} \hline 0 & i-1 & 0 & 0 \\ \hline \end{array} \parallel \begin{array}{|c|} \hline 252 \text{ bit } a_{\text{sk}} \\ \hline \end{array} \parallel \begin{array}{|c|} \hline 256 \text{ bit } h_{\text{Sig}} \\ \hline \end{array} \right) \\
\rho_i^{\text{new}} = \text{PRF}_{\varphi}^{\text{p}}(i, h_{\text{Sig}}) &:= \text{CRH} \left(\begin{array}{|c|c|c|c|} \hline 0 & i-1 & 1 & 0 \\ \hline \end{array} \parallel \begin{array}{|c|} \hline 252 \text{ bit } \varphi \\ \hline \end{array} \parallel \begin{array}{|c|} \hline 256 \text{ bit } h_{\text{Sig}} \\ \hline \end{array} \right)
\end{aligned}$$

Note: The first four bits —i.e. 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 bits 1011 in this position are used to distinguish uses of the full *SHA-256* hash function — see § 4.2.1 ‘*Note Commitments*’ on p. 6. (The specific bit patterns chosen here are motivated by the possibility of future extensions that either increase N^{old} and/or N^{new} to 3, or that add an additional bit to a_{sk} to encode a new key type, or that require an additional PRF.)

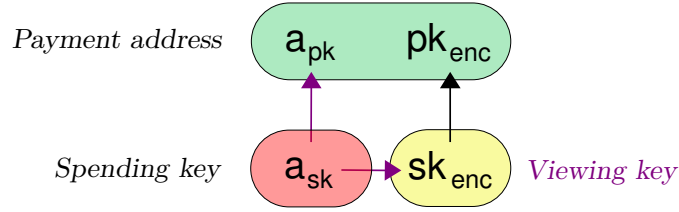
BLAKE2b is also used to construct a Key Derivation Function and as a hash function for the computation of h_{Sig} . The notation $\text{BLAKE2b}(p, x)$ represents the application of unkeyed *BLAKE2b* to a 16-byte personalization string p and input x , as defined in [1].

4 Concepts

4.1 Payment Addresses and Spending Keys

A key tuple $(\text{addr}_{\text{sk}}, \text{addr}_{\text{pk}})$ is generated by users Eli: “who wish to receive payments” is an intended usage explanation, suggest removing who wish to receive payments under this scheme. The payment address addr_{pk} is derived Eli: it’s not clear what “derived” means, suggest putting the formal derivations right away here from the spending key 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. Eli: formally, any a can be derived from any b as long as “derived” remains undefined, hence think the derivation rule should be explicitly stated here



Eli: following sentence is an intended usage explanation, and its very confusing: what happens if a player deviates? will it ruin the system? Additionally, its not clear what happens in our system, how is it “not exposed to users”? 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 Eli: what’s a user-visible operation? what’s an operation? how is it provided? should be provided to obtain a payment address or viewing key from a spending key.

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

a_{pk} , sk_{enc} and pk_{enc} are derived as follows: Eli: this be moved up. Additionally, the clamp/curve stuff is an “instantiation” and here we should have abstract PKC functionality (public key, private key)

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

where

- $\text{Curve25519}(\underline{n}, \underline{q})$ 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;
- $\text{clamp}_{\text{Curve25519}}(\underline{x})$ 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 .

Eli: following paragraph talks about intended usage, hence confusing. 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 Notes

A *note* (denoted \mathbf{n}) is a tuple $(\mathbf{a}_{pk}, \mathbf{v}, \mathbf{p}, \mathbf{r})$ Eli: shouldn't \mathbf{r} be part of the note commitment, not the note? which represents that a value \mathbf{v} is spendable by the recipient who holds the *spending key* \mathbf{a}_{sk} corresponding to \mathbf{a}_{pk} , as described in the previous section.

Eli: following list mixes abstract and instantiation stuff

- \mathbf{a}_{pk} is a 32-byte *authorization* public key Eli: this should have been defined in the previous section of the recipient.
- \mathbf{v} is a 64-bit unsigned integer representing the value of the *note* in *zatoshi* (1 **ZEC** = 10^8 *zatoshi*).
- \mathbf{p} is a 32-byte $\text{PRF}_{\mathbf{a}_{sk}}^{\text{nf}}$ preimage.
- \mathbf{r} is a 32-byte *COMM* trapdoor.

\mathbf{r} is randomly generated by the sender. Eli: previous and next sentence should be merged into bullets above \mathbf{p} is generated from a random seed φ using $\text{PRF}_{\varphi}^{\mathbf{p}}$. Only a commitment to these values is disclosed publicly, which allows the tokens \mathbf{r} and \mathbf{p} to blind the value and recipient *except* to those who possess these tokens Eli: inaccurate, even if you have these tokens you'd have to exhaustively try all address keys (not all of them are necessarily known to you) and values to find the recipient.

4.2.1 Note Commitments

The underlying \mathbf{v} and \mathbf{a}_{pk} are blinded with \mathbf{p} and \mathbf{r} using the collision-resistant hash function **SHA256**. Eli: The note commitment of \mathbf{n} , denoted \mathbf{cm} , is defined as ... The resulting hash $\mathbf{cm} = \text{NoteCommitment}(\mathbf{n})$.

$$\mathbf{cm} := \text{SHA256} \left(\begin{array}{|c|c|c|c|c|c|c|c|c|c|} \hline 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & & \\ \hline \end{array} \begin{array}{|c|c|c|c|} \hline 256 \text{ bit } \mathbf{a}_{pk} & 64 \text{ bit } \mathbf{v} & 256 \text{ bit } \mathbf{p} & 256 \text{ bit } \mathbf{r} \\ \hline \end{array} \right)$$

Note: The leading byte of the **SHA256** input is **0xB0**.

4.2.2 Nullifiers

A *nullifier* (denoted \mathbf{nf}) is derived from the \mathbf{p} component of a *note* as $\text{PRF}_{\mathbf{a}_{sk}}^{\mathbf{nf}}(\mathbf{p})$. A *note* is spent by proving knowledge of \mathbf{p} and \mathbf{a}_{sk} in zero knowledge while disclosing its *nullifier* \mathbf{nf} , allowing \mathbf{nf} to be used to prevent double-spending.

4.2.3 Note Plaintexts and Memo Fields

Eli: what's a transmitted note? is it different from a note? and who encrypts them? Transmitted *notes* are stored on the blockchain in encrypted form, together with a *note commitment* \mathbf{cm} .

Eli: next paragraph mentions "note plaintext", "joinsplit description", "transmission keys", "transmitted notes cyphertext" all of which are undefined yet. It seems the main thing defined here is the memo, and then a note-plaintext. In the "abstract" part both are easy to describe, and the rest of the details should likely be moved to "instantiation" The *note plaintexts* associated with a *JoinSplit* description are encrypted to the respective *transmission* keys $\mathbf{pk}_{\text{enc}, 1 \dots N}^{\text{new}}$, and the result forms part of a *transmitted notes ciphertext* (see §6 'In-band secret distribution' on p.13 for further details).

Each *note plaintext* (denoted \mathbf{np}) consists of $(\mathbf{v}, \mathbf{p}, \mathbf{r}, \mathbf{memo})$.

The first three of these fields are as defined earlier. **memo** is a 128-byte *memo field* associated with this *note*.

The usage of the *memo field* is by agreement between the sender and recipient of the *note*. The memo **SHOULD** be encoded either as:

- a UTF-8 human-readable string [6], padded with zero bytes; or

- an arbitrary sequence of 128 bytes starting with a byte value of **0xF5** or greater, which is therefore not a valid UTF-8 string.

In the former case, 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).

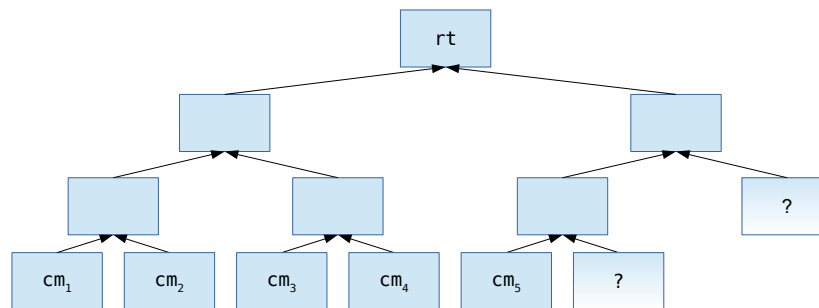
In the latter case, the contents of the *memo field* SHOULD NOT be displayed. A start byte of **0xF5** is reserved for use by automated software by private agreement. A start byte of **0xF6** or greater is reserved for use in future **Zcash** protocol extensions.

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

8 bit 0x00	v (8 bytes)	ρ (32 bytes)	r (32 bytes)	memo (128 bytes)
-------------------	-------------	-------------------	--------------	------------------

- A byte, **0x00**, indicating this version of the encoding of a *note plaintext*.
- 8 bytes specifying v.
- 32 bytes specifying ρ .
- 32 bytes specifying r.
- 128 bytes specifying **memo**.

4.3 Note Commitment Tree



Eli: Prefer “A *note commitment tree*” because all that follows works for any tree and we expect it to dynamically change

The *note commitment tree* is an *incremental merkle tree* of depth d used to store *note commitments* that *JoinSplit* operations produce Eli: undefined yet because *JoinSplit operation*. Why not define it just as in the figure, it’s a merkle tree of *note commitments*. 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 Eli: intended usage. particularly confusing because we now assign a job to a tree. to protect against double-spending, as it is append-only.

Eli: more intendend usage: how does the honest player associate blocks with a tree? and what happens if a user deviates from this? We’re going to describe the split-join circuit. For this purpose we only need to have defined a tree of commitments and define (or assume knowledge) of authentication paths in a merkle tree Blocks in the blockchain are associated (by all nodes) with the root of this tree after all of its constituent *JoinSplit descriptions*’ *note commitments* have been entered into the tree associated with the previous block.

4.4 Nullifier Set

Eli: intended usage. Prefer to have defined (i) a nullifier set and (ii) commitment tree, and now talk about join-split. Later we'll explain how these two objects are modified. Eli: tx undefined yet Transactions insert *nullifiers* into a *nullifier set* 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 *nullifiers* to the *nullifier set*.

Transactions that attempt to insert a *nullifier* into this set 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 *nullifiers* into the *nullifier set*.

Eli: suggest to move the discussion of the split-join circuit to here, so that we first completely discuss the single-tx level (with respect to some fixed comm-tree and nullifier set). Then we'll move to the topic of consensus and blockchain.

4.5 The Blockchain

Eli: For the "abstract" part, all we care about is that each block-chain is converted to a merkle tree in a deterministic manner, so that all honest players agree on it's structure (assuming they see the same blockchain). so the particular way the "canonical" tree is constructed should appear in "instantiation". At a given point in time, the *blockchain* view of each *full node* Eli: undefined. So far we had "users". Are there several kinds? 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 Eli: defined? 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 JoinSplit descriptions* Eli: this is undefined yet. let's work bottom up: first define a join-split assuming a fixed tree. TODO: They also have a transparent value flow that interacts with the *JoinSplit description's* v_{pub}^{old} and v_{pub}^{new} . Inputs and outputs are associated with a value. Eli: what're inputs/outputs of join-split?

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

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

The *anchor* of each subsequent *JoinSplit description* may refer either to some earlier *block's* final *treestate*, or to the output *treestate* of the immediately preceding *JoinSplit 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 Eli: who maintains the value pool? is this part of the specification? seems like more intended usage? Eli: tx undefined yet 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 JoinSplit Operations and Descriptions

A *JoinSplit description* is data included in a *transaction* Eli: lets first define split-join, then tx that describes a *JoinSplit operation*, i.e. a confidential value transfer. This kind of value transfer is the primary **Zcash**-specific operation performed by *transactions* Eli: we keep referring to undefined tx. furthermore, it's not clear from last sentence if tx is a type of data or a process, as it performs something; it uses, but should not be confused with, the *JoinSplit circuit* used for the *zk-SNARK* proof and verification.

A *JoinSplit operation* spends N^{old} notes $\mathbf{n}_{1..N^{\text{old}}}^{\text{old}}$ Eli: confusing notation, usually one uses x_1, \dots, x_n for a sequence of n objects, not $x_{1\dots,n}$ and transparent input $v_{\text{pub}}^{\text{old}}$, and creates N^{new} notes $\mathbf{n}_{1..N^{\text{new}}}^{\text{new}}$ and transparent output $v_{\text{pub}}^{\text{new}}$.

Consensus rule: Eli: what's a consensus rule? what happens if I deviate from it? Either $v_{\text{pub}}^{\text{old}}$ or $v_{\text{pub}}^{\text{new}}$ MUST be zero. Eli: why? what harm would follow if we allow both nonzero?

Zcash transactions have the following additional fields Eli: additional to what?:

Bytes	Name	Data Type	Description
<i>Varies</i>	<code>nJoinSplit</code>	<code>compactSize uint</code>	The number of <i>JoinSplit descriptions</i> in <code>vJoinSplit</code> .
$1026 \times \text{nJoinSplit}$	<code>vJoinSplit</code>	<code>JoinSplitDescription [nJoinSplit]</code>	The sequence of <i>JoinSplit descriptions</i> in this <i>transaction</i> .
33 †	<code>joinSplitPubKey</code>	<code>char[33]</code>	An encoding of a ECDSA public verification key, using the secp256k1 curve and parameters defined in [13] and [5].
64 †	<code>joinSplitSig</code>	<code>char[64]</code>	A signature on a prefix of the <i>transaction</i> encoding, to be verified using <code>joinSplitPubKey</code> .

† The `joinSplitPubKey` and `joinSplitSig` fields are present if and only if `nJoinSplit` > 0.

The encoding of `joinSplitPubKey` and the data to be signed are specified in more detail in § 5.3 ‘*Non-malleability*’ on p. 10.

Each `JoinSplitDescription` consists of: Eli: maybe move this up, to beginning of section?

Bytes	Name	Data Type	Description
8	vpub_old	int64_t	A value v_{pub}^{old} that the <i>JoinSplit</i> operation removes from the value pool.
8	vpub_new	int64_t	A value v_{pub}^{new} that the <i>JoinSplit</i> operation inserts into the value pool.
32	anchor	char[32]	A merkle root rt of the <i>note commitment tree</i> at some block height in the past, or the merkle root produced by a previous <i>JoinSplit</i> operation in this <i>transaction</i> . Sean: We need to be more specific here.
64	nullifiers	char[32] [N^{old}]	A sequence of <i>nullifiers</i> of the input <i>notes</i> $nf_{1..N^{old}}^{old}$.
64	commitments	char[32] [N^{new}]	A sequence of <i>note commitments</i> for the output <i>notes</i> $cm_{1..N^{new}}^{new}$.
32	ephemeralKey	char[32]	A Curve25519 public key epk .
434	encCiphertexts	char[217] [N^{new}]	A sequence of ciphertext components for the encrypted output <i>notes</i> , $C_{1..N^{new}}^{enc}$.
32	randomSeed	char[32]	A 256-bit seed that must be chosen independently at random for each <i>JoinSplit description</i> .
64	vmacs	char[32] [N^{old}]	A sequence of message authentication tags $h_{1..N^{old}}$ that bind h_{sig} to each a_{sk} of the <i>JoinSplit description</i> .
288	zkproof	char[288]	An encoding, as determined by the libsnark library [9], of the zero-knowledge proof $\pi_{JoinSplit}$.

The `ephemeralKey` and `encCiphertexts` fields together form the *transmitted notes ciphertext*.

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

5.1 Computation of h_{sig}

Eli: this is mostly “instantiation” but I notice we use a different crypto primitive instantiation (Blake) not mentioned previously. Let’s use the “abstract” notation here: what is it? a CRH? PRF? requires different multiple of the security parameter λ ? does it require special properties not needed by other instances of these that we used previously?

Given a *JoinSplit description*, we define:

$$\begin{aligned}
 h_{sigtag} &:= \boxed{72 \text{ bit “ZcashhSig”}} \parallel \boxed{[0]^{56}} \\
 h_{sig} &:= \text{BLAKE2b} \left(h_{sigtag}, \boxed{\text{randomSeed}} \parallel \boxed{256 \text{ bit } nf_1^{old}} \dots \parallel \boxed{256 \text{ bit } nf_{N^{old}}^{old}} \parallel \boxed{\text{joinSplitPubKey}} \right)
 \end{aligned}$$

5.2 Merkle root validity

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

5.3 Non-malleability

Eli: mix of “abstract” and “instantiation”. Can we first describe abstractly what’s going on here? I got pretty lost pretty quickly. In particular, what are the abstract functionalities of SIGHASH, SIGHASHALL, ECDSA, the “compressed elliptic curve point”, are they CRH and digital signature, respectively? what security (as multiple of λ)

Bitcoin defines several *SIGHASH* types that cover various parts of a transaction. In **Zcash**, all of these *SIGHASH* types are extended to cover the **Zcash**-specific fields `nJoinSplit`, `vJoinSplit`, and `joinSplitPubKey`. They *do not* cover the field `joinSplitSig`.

Consensus rule: **Eli:** what's a consensus rule? If `nJoinSplit` > 0, the *transaction* MUST NOT use *SIGHASH* types other than `SIGHASH_ALL`.

Let `dataToBeSigned` be the hash of the *transaction* using the `SIGHASH_ALL` *SIGHASH* type. Note that this *excludes* all of the `scriptSig` fields in the non-**Zcash**-specific parts of the *transaction*.

In order to ensure that a *JoinSplit* description is cryptographically bound to the transparent inputs and outputs corresponding to v_{pub}^{new} and v_{pub}^{old} , and to the other *JoinSplit* descriptions in the same *transaction*, an ephemeral ECDSA key pair is generated for each *transaction*, and the `dataToBeSigned` is signed with the private signing key of this key pair. The corresponding public verification key is included in the *transaction* encoding as `joinSplitPubKey`.

If `nJoinSplit` is zero, the `joinSplitPubKey` and `joinSplitSig` fields are omitted. Otherwise, a *transaction* has a correct *JoinSplit* signature if:

- `joinSplitSig` can be verified as an encoding of a signature on `dataToBeSigned`, using the ECDSA public key encoded as `joinSplitPubKey`; and
- `joinSplitSig` has an `s` value in the lower half of the possible range (i.e. `s` must be in the range from 0x1 to 0x7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF5D576E7357A4501DDFE92F46681B20A0, inclusive).

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

The encoding of a signature is:

256 bit <code>r</code>	256 bit <code>s</code>
------------------------	------------------------

where `r` and `s` are as defined in [13].

The encoding of a public key is as defined in section E.2.3.2 of [14] for a compressed elliptic curve point with *x*-coordinate x_P and compressed *y*-coordinate \tilde{y}_P :

0	0	0	0	0	0	1	1 bit \tilde{y}_P	256 bit x_P
---	---	---	---	---	---	---	---------------------	---------------

Note that only compressed public keys are valid.

The condition enforced by the *JoinSplit* circuit specified in § 5.6 ‘*Non-malleability*’ on p.12 ensures that a holder of all of $a_{sk,1..N}^{old}$ for each *JoinSplit* description has authorized the use of the private signing key corresponding to `joinSplitPubKey` to sign this *transaction*.

5.4 Balance

A *JoinSplit* operation can be seen **Eli:** more intended usage, from the perspective of the *transaction* **Eli:** does a transaction “see”?, as an input and an output simultaneously. v_{pub}^{old} takes value from the value pool and v_{pub}^{new} adds value to the value pool. As a result, v_{pub}^{old} is treated **Eli:** by whom? like an *output* value, whereas v_{pub}^{new} is treated like an *input* value.

Note that unlike original **Zerocash** [2], **Zcash** does not have a distinction between Mint and Pour operations. The addition of v_{pub}^{old} to a *JoinSplit* description subsumes the functionality of both Mint and Pour. Also, *JoinSplit* descriptions are indistinguishable regardless of the number of real input *notes*.

As stated in § 5 ‘*JoinSplit Operations and Descriptions*’ on p.9, either v_{pub}^{old} or v_{pub}^{new} MUST be zero. No generality is lost because, if a *transaction* in which both v_{pub}^{old} and v_{pub}^{new} were nonzero were allowed, it could be replaced by an equivalent one in which $\min(v_{pub}^{old}, v_{pub}^{new})$ is subtracted from both of these values. This restriction helps to avoid

unnecessary distinctions between *transactions* according to client implementation.

5.5 Note Commitments and Nullifiers

A *transaction* **Eli**: **undefined yet** that contains one or more *JoinSplit* descriptions, when entered into the blockchain, appends to the *note commitment tree* with all constituent *note commitments*. All of the constituent *nullifiers* are also entered into the *nullifier set* of the *blockchain view and mempool*. A *transaction* is not valid if it attempts to add a *nullifier* to the *nullifier set* that already exists in the set.

5.6 JoinSplit circuit and Proofs

In **Zcash**, N^{old} and N^{new} are both 2.

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

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

there exists a witness of *auxiliary input*:

$$(\text{path}_{1..N^{\text{old}}}, \mathbf{n}_{1..N^{\text{old}}}^{\text{old}}, \mathbf{a}_{\text{sk}, 1..N^{\text{old}}}^{\text{old}}, \mathbf{n}_{1..N^{\text{new}}}^{\text{new}}, \varphi)$$

where:

$$\begin{aligned} \text{for each } i \in \{1..N^{\text{old}}\}: \mathbf{n}_i^{\text{old}} &= (\mathbf{a}_{\text{pk}, i}^{\text{old}}, \mathbf{v}_i^{\text{old}}, \rho_i^{\text{old}}, r_i^{\text{old}}); \\ \text{for each } i \in \{1..N^{\text{new}}\}: \mathbf{n}_i^{\text{new}} &= (\mathbf{a}_{\text{pk}, i}^{\text{new}}, \mathbf{v}_i^{\text{new}}, \rho_i^{\text{new}}, r_i^{\text{new}}) \end{aligned}$$

such that the following conditions hold:

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

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

$$\text{Nullifier integrity } \text{for each } i \in \{1..N^{\text{new}}\}: \text{nf}_i^{\text{old}} = \text{PRF}_{\mathbf{a}_{\text{sk}, i}^{\text{old}}}^{\text{nf}}(\rho_i^{\text{old}}).$$

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

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

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

$$\text{Commitment integrity } \text{for each } i \in \{1..N^{\text{new}}\}: \text{cm}_i^{\text{new}} = \text{NoteCommitment}(\mathbf{n}_i^{\text{new}}).$$

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 pk_{enc} is used to encrypt these secrets. The recipient's possession of the associated $(\text{addr}_{\text{pk}}, \text{addr}_{\text{sk}})$ (which contains both a_{pk} and sk_{enc}) is used to reconstruct the original *note and memo field*.

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

6.1 Encryption

Let $\text{SymEncrypt}_K(\mathbf{P})$ be authenticated encryption using AEAD_CHACHA20_POLY1305 [11] encryption of plaintext \mathbf{P} , with empty “associated data”, all-zero nonce $[0]^{96}$, and 256-bit key K .

Similarly, let $\text{SymDecrypt}_K(\mathbf{C})$ be AEAD_CHACHA20_POLY1305 decryption 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:

$$\text{KDF}(i, \text{h}_{\text{Sig}}, \text{dhsecret}_i, \text{epk}, \text{pk}_{\text{enc},i}^{\text{new}}) := \text{LeadingBytes}_{32}(\text{BLAKE2b}(\text{kdf}_{\text{tag}}, \text{kdf}_{\text{input}}))$$

where:

$$\text{kdf}_{\text{tag}} := \begin{array}{|c|c|c|} \hline 64 \text{ bit “ZcashKDF”} & 8 \text{ bit } i-1 & [0]^{56} \\ \hline \end{array}$$

$$\text{kdf}_{\text{input}} := \begin{array}{|c|c|c|c|} \hline 256\text{-bit } \text{h}_{\text{Sig}} & 256 \text{ bit } \text{dhsecret}_i & 256 \text{ bit } \text{epk} & 256 \text{ bit } \text{pk}_{\text{enc},i}^{\text{new}} \\ \hline \end{array}.$$

Let $\text{pk}_{\text{enc},1..N^{\text{new}}}^{\text{new}}$ be the **Curve25519** public keys for the intended recipient addresses of each new *note*, and let $\text{np}_{1..N^{\text{new}}}$ be the *note plaintexts*. Let h_{Sig} be the value computed in § 5.1 ‘*Computation of h_{Sig}* ’ on p. 10.

Then to encrypt:

- Generate a new **Curve25519** (public, private) key pair (epk, esk) .
- For $i \in \{1..N^{\text{new}}\}$,
 - Let $\mathbf{P}_i^{\text{enc}}$ be the raw encoding of np_i .
 - Let $\text{dhsecret}_i := \text{Curve25519}(\text{esk}, \text{pk}_{\text{enc},i}^{\text{new}})$.
 - Let $K_i^{\text{enc}} := \text{KDF}(i, \text{h}_{\text{Sig}}, \text{dhsecret}_i, \text{epk}, \text{pk}_{\text{enc},i}^{\text{new}})$.
 - Let $\mathbf{C}_i^{\text{enc}} := \text{SymEncrypt}_{K_i^{\text{enc}}}(\mathbf{P}_i^{\text{enc}})$.

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

6.2 Decryption by a Recipient

Let $\text{addr}_{\text{pk}} = (\text{a}_{\text{pk}}, \text{pk}_{\text{enc}})$ be the recipient's *payment address*, and let sk_{enc} be the recipient's **Curve25519** private key. Let h_{Sig} be the value computed in § 5.1 ‘*Computation of h_{Sig}* ’ on p. 10. Let $\text{cm}_{1..N^{\text{new}}}^{\text{new}}$ be the *note commitments* of each output coin. Then for each $i \in \{1..N^{\text{new}}\}$, the recipient will attempt to decrypt that ciphertext component as follows:

- Let $\text{dhsecret}_i := \text{Curve25519}(\text{sk}_{\text{enc}}, \text{epk})$.
- Let $K_i^{\text{enc}} := \text{KDF}(i, \text{h}_{\text{Sig}}, \text{dhsecret}_i, \text{epk}, \text{pk}_{\text{enc},i}^{\text{new}})$.
- Return $\text{DecryptNote}(K_i^{\text{enc}}, \mathbf{C}_i^{\text{enc}}, \text{cm}_i^{\text{new}}, \text{a}_{\text{pk}})$.

$\text{DecryptNote}(\mathbf{K}_i^{\text{enc}}, \mathbf{C}_i^{\text{enc}}, \mathbf{cm}_i^{\text{new}}, \mathbf{a}_{\text{pk}})$ is defined as follows:

- Let $\mathbf{P}_i^{\text{enc}} := \text{SymDecrypt}_{\mathbf{K}_i^{\text{enc}}}(\mathbf{C}_i^{\text{enc}})$.
- If $\mathbf{P}_i^{\text{enc}} = \perp$, return \perp .
- Extract $\mathbf{np}_i = (v_i^{\text{new}}, \rho_i^{\text{new}}, r_i^{\text{new}}, \text{memo}_i)$ from $\mathbf{P}_i^{\text{enc}}$.
- If $\text{NoteCommitment}((\mathbf{a}_{\text{pk}}, v_i^{\text{new}}, \rho_i^{\text{new}}, r_i^{\text{new}})) \neq \mathbf{cm}_i^{\text{new}}$, return \perp , else return \mathbf{np}_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 *note* is unspent in a particular *blockchain* view also requires the *authorization* private key \mathbf{a}_{sk} ; the coin is unspent if and only if $\text{nf} = \text{PRF}_{\mathbf{a}_{\text{sk}}}^{\text{nf}}(\rho)$ is not in the *nullifier set* for that *blockchain* view.

Note that a *note* 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 *note* 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 [10]. Note that:

- The same ephemeral key is used for all encryptions to the recipient keys in a given *JoinSplit description*.
- In addition to the Diffie-Hellman secret, the KDF takes as input the seed \mathbf{h}_{sig} , the public keys of both parties, and the index i .
- The nonce parameter to `AEAD_CHACHA20_POLY1305` is not used.
- The “IETF” definition of `AEAD_CHACHA20_POLY1305` from [11] is used; this uses a 32-bit block count and a 96-bit nonce, rather than a 64-bit block count and 64-bit nonce as in the original definition of `ChaCha20`.

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 [4].

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** [4].

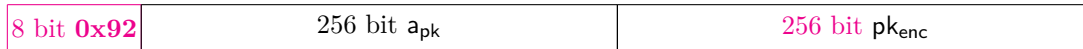
7.2 Transparent Private Keys

These are encoded in the same way as in **Bitcoin** [4].

7.3 Protected Payment Addresses

A *payment address* consists of a_{pk} and pk_{enc} . a_{pk} is a SHA-256 compression function output. pk_{enc} is a **Curve25519** public key, for use with the encryption scheme defined in § 6 ‘*In-band secret distribution*’ on p. 13.

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 pk_{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} , which is a sequence of 252 bits.

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} .

The zero padding occupies the most significant 4 bits of the second byte.

Note: If an implementation represents a_{sk} internally as a sequence of 32 bytes with the 4 bits of zero padding intact, it will be in the correct form for use as an input to PRF^{addr} , PRF^{nf} , and PRF^{pk} without need for bit-shifting. Future key representations may make use of these padding bits.

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 **Zcash** *transaction*, e.g. to spend a protected *note* that has just been created. (In **Zcash**, we refer to value stored in UTXOs as “transparent”, and value stored in *JoinSplit operation* output *notes* 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.

TODO: Describe changes to signing.

8.2 Unification of Mints and Pours

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

- a “Mint” transaction takes value from transparent UTXOs as input and produces a new protected *note* as output.
- a “Pour” transaction takes up to N^{old} protected *notes* as input, and produces up to N^{new} protected *notes* 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.15) consists only of *JoinSplit operations*. A *JoinSplit operation* is a Pour operation generalized to take a transparent UTXO as input, allowing *JoinSplit operations* to subsume the functionality of Mints. An advantage of this is that a **Zcash** *transaction* that takes input from an UTXO can produce up to N^{new} output *notes*, improving the indistinguishability properties of the protocol. A related change conceals the input arity of the *JoinSplit operation*: an unused (zero-value) input is indistinguishable from an input that takes value from a *note*.

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

Zcash adds a *memo field* sent from the creator of a *JoinSplit description* to the recipient of each output *note*. This feature is described in more detail in § 4.2.3 ‘*Note Plaintexts and Memo Fields*’ on p.6.

8.4 Faerie Gold attack and fix

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

An adversary can use this to mislead a *note* recipient, by sending two *notes* both of which are verified as valid by 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 [8].

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 *note* can be spent provided that its *nullifier* does not appear on the ledger. This does not take into account the possibility that distinct *notes*, which are validly received, could have the same *nullifier*. That is, the security definition depends on a protocol detail — *nullifiers* — 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 *note* to reduce (to zero) the effective value of another *note* 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 *notes* they have ever received, and reject duplicates (as proposed in [7]). 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 *nullifiers* in *JoinSplit descriptions* that appear in a valid *blockchain view* must be distinct. The *nullifiers* are used as input to *BLAKE2b* to derive a public value h_{sig} which uniquely identifies the transaction, as described in § 5.1 ‘*Computation of h_{sig}* ’ on p. 10. (h_{sig} was already used in **Zerocash** in a way that requires it to be unique in order to maintain indistinguishability of *JoinSplit descriptions*; adding the *nullifiers* 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 *note* is then derived from a random private seed φ and h_{sig} using $\text{PRF}_{\varphi}^{\rho}$. The correct construction of ρ for each output *note* is enforced by the circuit (see § 5.6 ‘*Uniqueness of ρ_i^{new}* ’ on p. 12).

Now even if the creator of a *JoinSplit description* does not choose φ randomly, uniqueness of *nullifiers* and collision resistance of both *BLAKE2b* and PRF^{ρ} will ensure that the derived ρ values are unique, at least for any two *JoinSplit 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 COMM_r and COMM_s is a computationally binding commitment to its inputs a_{pk} , v , and ρ . However, the instantiation of COMM_r and 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 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 *note commitment*. This would have allowed such an attacker to break the balance property by double-spending *notes*, potentially creating arbitrary amounts of currency for themselves.

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 *JoinSplit operation* 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 *note commitment* from three to two, saving a total of four *SHA256Compress* evaluations in the *JoinSplit circuit*.

Note that **Zcash note 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 *note* as a tuple $(a_{pk}, v, \rho, r, s, cm)$, whereas this specification defines it as (a_{pk}, v, ρ, r) . This is just a clarification, because the instantiation of $COMM_s$ in section 5.1 of the paper did not use s (and neither does the new instantiation of $NoteCommitment$). 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] Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O’Hearn, and Christian Winnerlein. BLAKE2: simpler, smaller, fast as MD5. <https://blake2.net/#sp>, January 29 2013.
- [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] Base58Check encoding – Bitcoin Wiki. https://en.bitcoin.it/wiki/Base58Check_encoding. Accessed: 2016-01-26.
- [5] Secp256k1 – Bitcoin Wiki. <https://en.bitcoin.it/wiki/Secp256k1>. Accessed: 2016-03-14.
- [6] The Unicode Consortium. *The Unicode Standard*. The Unicode Consortium, 2015. <http://www.unicode.org/versions/latest/>.
- [7] 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.
- [8] 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.
- [9] libsnark: a C++ library for zkSNARK proofs. <https://github.com/scipr-lab/libsnark>. Accessed: 2016-03-15.
- [10] Sealed boxes — libsodium. https://download.libsodium.org/doc/public-key_cryptography/sealed_boxes.html. Accessed: 2016-02-01.

- [11] 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.
- [12] 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.
- [13] Certicom Research. Standards for Efficient Cryptography 2 (SEC 2). <http://www.secg.org/sec2-v2.pdf>, January 27 2010. Version 2.0.
- [14] IEEE Computer Society. *IEEE Std 1363-2000: Standard Specifications for Public-Key Cryptography*. IEEE, August 29 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.