MantaPay Protocol Specification
v1.0.0

Shumo Chu, Boyuan Feng, Brandon H. Gomes, Francisco Hernández Iglesias, and Todd Norton *

September 28, 2022

Abstract

MantaPay is an implementation of a *decentralized anonymous payment* scheme based on the MANTA$_{\text{DAP}}$ protocol outlined in the original MANTA whitepaper.

Contents

*ordered alphabetically

1 Introduction

$\mathsf{MantaPay}$ aims to solve the long-standing privacy problems facing cryptocurrencies. At its heart, it uses various cryptographic constructions including NIZK (non-interactive zero knowledge proof) systems to ensure user privacy from *first principles* and to build the foundational layer for programmable private money. The $\mathsf{MantaPay}$ protocol provides the following features:

1. Elastic Multi-Asset Shielded Pool: A shielded pool for every kind of asset with elastic annonymity set resizing
2. Verifiable Viewing Keys: Opt-in transaction transparency with audit correctness assurance
3. Programmable $\mathsf{zkAssets}$: New Transparent UTXO model allowing programmability layers to be built on top of the shielded pool
4. Delegated Proof Generation: Decoupling the spending access from the proof generation access gives hardware wallets native support for $\mathsf{zkAssets}$

2 Notation

The following notation is used throughout this specification:

- Type is the type of types[1].
- If $x : T$ then x is a value and T is a type, denoted $T : \mathsf{Type}$, and we say that x *has type* T.
- Bool is the type of booleans with values True and False.
- For any types $A : \mathsf{Type}$ and $B : \mathsf{Type}$ we denote the *type of functions* from A to B as $A \to B : \mathsf{Type}$.
- For any types $A : \mathsf{Type}$ and $B : \mathsf{Type}$ we denote the *product type* over A and B as $A \times B : \mathsf{Type}$ with constructor $(-,-) : A \to (B \to A \times B)$. Depending on context, we may omit the constructor and inline the pair into another constructor/destructor. For example, if $f : A \times B \to C$ we can denote $f((a,b))$ as $f(a,b)$ to reduce the number of parentheses.
- For any type $T : \mathsf{Type}$, we define $\mathsf{Option}\langle T\rangle : \mathsf{Type}$ as the inductive type with constructors:

$$\begin{gathered}\mathsf{None} : \mathsf{Option}\langle T\rangle \\ \mathsf{Some} : T \to \mathsf{Option}\langle T\rangle\end{gathered}$$

- We denote the *type of finite sets* over a type $T : \mathsf{Type}$ as $\mathsf{FinSet}\langle T\rangle : \mathsf{Type}$. The membership predicate for a value $x : T$ in a finite set $S : \mathsf{FinSet}(T)$ is denoted $x \in S$.
- We denote the *type of finite ordered sets* over a type $T : \mathsf{Type}$ as $\mathsf{List}\langle T\rangle : \mathsf{Type}$. This can either be defined by an inductive type or as a $\mathsf{FinSet}(T)$ with a fixed ordering. We denote the constructor for a list as $[\ldots]$ for an arbitrary set of elements.
- We denote the *type of distributions* over a type $T : \mathsf{Type}$ as $\mathfrak{D}\langle T\rangle : \mathsf{Type}$. A value x sampled from $\mathfrak{D}\langle T\rangle$ is denoted $x \sim \mathfrak{D}\langle T\rangle$ and the fact that the value x belongs to the range of $\mathfrak{D}\langle T\rangle$ is denoted $x \in \mathfrak{D}\langle T\rangle$. So namely, $y \in \{x \mid x \sim \mathfrak{D}\langle T\rangle\} \leftrightarrow y \in \mathfrak{D}\langle T\rangle$.
- We denote the equality predicate as $(- = -) : T \times T \to \mathsf{Type}$ and the equality function as $\mathsf{eq} : T \times T \to \mathsf{Bool}$ whenever they exist.
- We denote the selection function as $\mathsf{select} : \mathsf{Bool} \times T \times T \to T$. For a boolean $b : \mathsf{Bool}$ and two values $t_1, t_2 : T$, $\mathsf{select}(b, t_1, t_2)$ returns t_1 when $b = \mathsf{True}$ and returns t_2 when $b = \mathsf{False}$.
- Depending on the context, the notation $|\cdot|$ denotes either the absolute value of a quantity, the length of a list, the number of characters in a string, or the cardinality of a set.
- We denote $\mathsf{iszero} : T \to \mathsf{Bool}$ the function that returns True whenever the input element is equal to the zero element of T (this function is only defined whenever T has a well-defined zero element).
- We denote $\mathsf{select} : \mathsf{Bool} \times T \times T \to T$ the function that selects a value from a pair, using the left element if the input boolean is False and the right element if the input boolean is True.

[1] By *type of types*, we mean the type of *first-level* types in some family of type universes. Discussion of the type theory necessary to make these notions rigorous is beyond the scope of this paper.

3 Concepts

3.1 zkAssets

The zkAsset is the fundamental currency object in the MantaPay protocol. An asset a : zkAsset is a tuple

$$a = (a.\mathsf{id}, a.\mathsf{value}) : \mathsf{AssetId} \times \mathsf{AssetValue}$$

where the AssetId encodes the type of currency stored in a and the AssetValue encodes how many units of that currency are stored in a. MantaPay is a *decentralized anonymous payment* protocol which facilitiates the private ownership and private transfer of zkAssets.

zkAssets are the basic building-blocks of *transactions* which consume a set of input zkAssets and produce a set of transformed output zkAssets. To preserve the economic value stored in zkAssets, the sum of the input AssetValues must balance the sum of the output AssetValues, and all assets in a single transaction must have the same AssetId[2]. This is called a *balanced transfer*: no value is created or destroyed in the process. The MantaPay protocol uses a distributed algorithm called Transfer to perform balanced transfers and ensure that they are valid.

3.2 UTXOs

But zkAssets are not private on their own. A UTXO is a container for a zkAsset that hides its value and its owner and is the main object that MantaPay uses to transfer the spending power of zkAssets between different protocol participants. A UTXO is a cryptographic commitment along with some associated data that represents a spendable subset of an account stored in the protocol. In the MantaPay protocol, UTXOs come in two flavors, *opaque* and *transparent*. The *opaque* UTXOs are completely private and they do not reveal the owner or underlying asset contained in them, whereas *transparent* UTXOs reveal the underlying asset but not the owner. The *opaque* UTXO is used for the private transfer of zkAssets and the *transparent* UTXO is used to give programability to zkAssets whenever the MantaPay protocol lives in the same environment as other smart contracts by allowing contracts to control the AssetId and AssetValue stored in the *transparent* UTXO.

3.3 Nullifiers

One of the important ways that privacy is preserved for zkAssets across many transactions is that the exact transaction where a UTXO is spent is not known to the public. Instead, only the owner of the zkAsset, or anyone with the appropriate viewing key, can know this information. The Nullifier is another cryptographic commitment that takes the place of the UTXO when it is spent and it is cryptographically hard for any particular UTXO to be derived from its Nullifier.

3.4 zkAddresses

In order for MantaPay participants to receive zkAssets via the Transfer protocol, they create zkAddress which they use as identifiers to represent them on the ledger.

$$\begin{tikzcd}
& \mathsf{sk} \arrow[dl] \arrow[dr] & & & \\
\mathsf{sk}_\alpha \arrow[dr] & & \mathsf{ak} \arrow[dl] \arrow[r] & \mathsf{vk} \arrow[r] & \mathsf{pk} \\
& \mathsf{ak}_\alpha & & &
\end{tikzcd}$$

Figure 1: Key Schedule for MantaPay.

MantaPay uses four kinds of keys all derived from a base secret, spending key sk, which give the following kinds of privileged access in the protocol:

- **zkAddress** (send): Access to the zk-address pk gives the user the right to send zkAssets to the owner of the associated sk.
- **Viewing Key** (view): Access to the viewing key vk gives the user the right to view all transactions for the owner of the associated sk.

[2]It is beyond the scope of this paper to discuss transactions with inputs and outputs that feature different AssetIds, like those that would be featured in a *decentralized anonymous exchange*.

- **Proof Authorization Key** (prove): Proof authorization key ak gives the user the right to build the Transfer proof on behalf of the owner of sk. This key is used when delegating proof generation to a semi-trusted entity while still protecting the spending rights associated to the sk, for example, if a hardware wallet holds sk it can ask a more capable computer to produce the Transfer proof for it without sending the spending rights off of the hardware wallet.
- **Spending Key** (spend): Access to the spending key sk gives total control over the assets owned by this secret, including spending, proof generation, and viewing.

Participants in MantaPay are represented by their zk-addresses, but they are not unique representations, since one participant may have access to more than one secret key. See § 4.2 for more information on how these keys are constructed and used for spending, proving, viewing, and receiving.

3.5 Notes

The encrypted Note is the primary means of communication in the MantaPay protocol. For a zkAddress owner to know that they have received a zkAsset and can now spend it they decrypt Notes with their viewing key to discover how much of an asset they have received and what information they need to spend it. The Note is also used to keep track of the balances of an entire account over its transaction history.

There are two kinds of Notes in the MantaPay protocol, *incoming* Notes and *outgoing* Notes. The IncomingNote is attached to every new UTXO and contains the same zkAsset as the UTXO and also a secret randomizer used to hide the UTXO commitment. The OutgoingNote is attached to every new Nullifier and contains the same zkAsset as the UTXO that the Nullifier is marking. When performing accounting over a zkAddress to measure how much of a particular AssetId that address controls, the AssetValue stored in the IncomingNotes should be *added* to the running total whereas the AssetValue stored in the OutgoingNotes should be *subtracted* from the running total as they represent inflows and outflows respectively.

3.6 ShieldedPool

The ShieldedPool is an object that contains the necessary data to enable the MantaPay Transfer protocol. The ShieldedPool is made up of the following three general storage groups:

- UTXO Storage: Contains all of the UTXOs that have ever been created along with their IncomingNotes
- Nullifier Storage: Contains all of the Nullifiers that have ever been created along with their OutgoingNotes
- Public Pool Account: The public account of the pool itself that holds a backing of all the zkAssets held in the UTXOs in the pool. Depositing into or withdrawing out of the pool has to go through this account.

There are two general requirements on the UTXO and Nullifier storage items:

1. Fast non-membership query for UTXOs and Nullifiers
2. Fast insertion and insertion-order iteration over $(\mathsf{UTXO}, \mathsf{IncomingNote})$ and $(\mathsf{Nullifier}, \mathsf{OutgoingNote})$ pairs

In order to satisfy both of these requirements we have the following breakdown of the storage:

- UTXO Storage:
  - $\mathsf{UTXOSet} : \mathsf{UTXO} \to \mathsf{Bool}$
  - $\mathsf{UTXOStorageInsertionOrder} : \mathbb{N} \to (\mathsf{UTXO}, \mathsf{IncomingNote})$
- Nullifier Storage:
  - $\mathsf{NullifierSet} : \mathsf{Nullifier} \to \mathsf{Bool}$
  - $\mathsf{NullifierStorageInsertionOrder} : \mathbb{N} \to (\mathsf{Nullifier}, \mathsf{OutgoingNote})$

where we use the sets for fast non-membership checks and the insertion order maps for insertion-order preserving insertion and iteration.

4 Abstract Protocol

4.1 Abstract Cryptographic Schemes

In the following section, we outline the formal specifications for all of the *cryptographic schemes* used in the MantaPay protocol.

Definition 4.1.1 (Commitment Scheme)**.** A *commitment scheme* COM is defined by the schema:

$$\begin{aligned}\mathsf{Randomness} &: \mathsf{Type}\\ \mathsf{Input} &: \mathsf{Type}\\ \mathsf{Output} &: \mathsf{Type}\\ \mathsf{commit} &: \mathsf{Randomness} \times \mathsf{Input} \to \mathsf{Output}\end{aligned}$$

with the following properties:

- **Binding**: It is infeasible to find an $x, y : \mathsf{Input}$ and $r, s : \mathsf{Randomness}$ such that $x \neq y$ and $\mathsf{commit}(r, x) = \mathsf{commit}(s, y)$.
- **Hiding**: For all $x, y : \mathsf{Input}$, the distributions $\{\mathsf{commit}(r, x) \mid r \sim \mathsf{Randomness}\}$ and $\{\mathsf{commit}(r, y) \mid r \sim \mathsf{Randomness}\}$ are *computationally indistinguishable.*

Notation: For convenience, we may refer to $\mathsf{COM.commit}(r, x)$ by $\mathsf{COM}(r, x)$.

Definition 4.1.2 (Hash Function)**.** A *hash function* HASH is defined by the schema:

$$\begin{aligned}\mathsf{Input} &: \mathsf{Type}\\ \mathsf{Output} &: \mathsf{Type}\\ \mathsf{hash} &: \mathsf{Input} \to \mathsf{Output}\end{aligned}$$

with the following properties:

- **Collision Resistance**: It is infeasible to find $a, b : \mathsf{Input}$ such that $a \neq b$ and $\mathsf{hash}(a) = \mathsf{hash}(b)$.
- **Pre-Image Resistance**: Given $y : \mathsf{Output}$, it is infeasible to find an $x : \mathsf{Input}$ such that $\mathsf{hash}(x) = y$.
- **Second Pre-Image Resistance**: Given $a : \mathsf{Input}$, it is infeasible to find another $b : \mathsf{Input}$ such that $a \neq b$ and $\mathsf{hash}(a) = \mathsf{hash}(b)$.

We can also ask that a hash function be *binding* or *hiding* as in the above *Commitment Scheme* definition if we partition the Input space into a separate $\mathsf{Randomness}$ and Input space.

Notation: For convenience, we may refer to $\mathsf{HASH.hash}(x)$ by $\mathsf{HASH}(x)$.

Definition 4.1.3 (Signature Scheme)**.** A *signature scheme* SIG is defined by the schema:

$$\begin{aligned}\mathsf{SigningKey} &: \mathsf{Type}\\ \mathsf{VerifyingKey} &: \mathsf{Type}\\ \mathsf{Randomness} &: \mathsf{Type}\\ \mathsf{Message} &: \mathsf{Type}\\ \mathsf{Signature} &: \mathsf{Type}\\ \mathsf{derive} &: \mathsf{SigningKey} \to \mathsf{VerifyingKey}\\ \mathsf{sign} &: \mathsf{SigningKey} \times \mathsf{Randomness} \times \mathsf{Message} \to \mathsf{Signature}\\ \mathsf{verify} &: \mathsf{VerifyingKey} \times \mathsf{Signature} \times \mathsf{Message} \to \mathsf{Bool}\end{aligned}$$

with the following properties:

- **Correctness**: For a given $\mathsf{sk} : \mathsf{SigningKey}$, $r : \mathsf{Randomness}$, and $m : \mathsf{Message}$, we have that

$$\mathsf{verify}(\mathsf{derive}(\mathsf{sk}), \mathsf{sign}(\mathsf{sk}, r, m), m) = \mathsf{True}$$

Definition 4.1.4 (Authenticated Encryption Scheme)**.** An *authenticated encryption* scheme AUTH is defined by the schema:

$$\begin{aligned}\mathsf{Key} &: \mathsf{Type}\\ \mathsf{Plaintext} &: \mathsf{Type}\\ \mathsf{Ciphertext} &: \mathsf{Type}\\ \mathsf{encrypt} &: \mathsf{Key} \times \mathsf{Plaintext} \to \mathsf{Ciphertext}\\ \mathsf{decrypt} &: \mathsf{Key} \times \mathsf{Ciphertext} \to \mathsf{Option}(\mathsf{Plaintext})\end{aligned}$$

with the following properties:

- **Correctness**: For a given $k : \mathsf{Key}$, $p : \mathsf{Plaintext}$, we have that $\mathsf{decrypt}(k, \mathsf{encrypt}(k, p)) = \mathsf{Some}(p)$.

Definition 4.1.5 (Dynamic Cryptographic Accumulator)**.** A *dynamic cryptographic accumulator* DCA is defined by the schema:

$$\begin{aligned}
\mathsf{Item} &: \mathsf{Type} \\
\mathsf{Output} &: \mathsf{Type} \\
\mathsf{Witness} &: \mathsf{Type} \\
\mathsf{State} &: \mathsf{Type} \\
\mathsf{current} &: \mathsf{State} \to \mathsf{Output} \\
\mathsf{insert} &: \mathsf{Item} \times \mathsf{State} \to \mathsf{State} \\
\mathsf{contains} &: \mathsf{Item} \times \mathsf{State} \to \mathsf{Option}(\mathsf{Output} \times \mathsf{Witness}) \\
\mathsf{verify} &: \mathsf{Item} \times \mathsf{Output} \times \mathsf{Witness} \to \mathsf{Bool}
\end{aligned}$$

with the following properties:

- **Unique Accumulated Values**: For any initial state $s : \mathsf{State}$ and any list of items $I : \mathsf{List}(\mathsf{Item})$ we can generate the sequence of states:
$$s_0 := s, \quad s_{i+1} := \mathsf{insert}(I_i, s_i)$$
Then, if we collect the accumulated values for these states, $z_i := \mathsf{current}(s_i)$, there should be exactly $|I|$-many unique values, one for each state update.
- **Provable Membership**: For any initial state $s : \mathsf{State}$ and any list of items $I : \mathsf{List}(\mathsf{Item})$ we can generate the sequences of states:
$$s_0 := s, \quad s_{i+1} := \mathsf{insert}(I_i, s_i)$$
Then, if we collect the states s_i into a set S, we have the following property for all $s \in S$ and $t \in I$,
$$\mathsf{Some}(z, w) := \mathsf{contains}(t, s), \quad \mathsf{verify}(t, z, w) = \mathsf{True}$$

Definition 4.1.6 (Non-Interactive Zero-Knowledge Proving System)**.** A *non-interactive zero-knowledge proving system* NIZK is defined by the schema:

$$\begin{aligned}
\mathsf{Statement} &: \mathsf{Type} \\
\mathsf{ProvingKey} &: \mathsf{Type} \\
\mathsf{VerifyingKey} &: \mathsf{Type} \\
\mathsf{PublicInput} &: \mathsf{Type} \\
\mathsf{SecretInput} &: \mathsf{Type} \\
\mathsf{Proof} &: \mathsf{Type} \\
\mathsf{keys} &: \mathsf{Statement} \to \mathfrak{D}(\mathsf{ProvingKey} \times \mathsf{VerifyingKey}) \\
\mathsf{prove} &: \mathsf{Statement} \times \mathsf{ProvingKey} \times \mathsf{PublicInput} \times \mathsf{SecretInput} \to \mathfrak{D}(\mathsf{Option}(\mathsf{Proof})) \\
\mathsf{verify} &: \mathsf{VerifyingKey} \times \mathsf{PublicInput} \times \mathsf{Proof} \to \mathsf{Bool}
\end{aligned}$$

Notation: We use the following notation for a NIZK:

- We write the Statement and ProvingKey arguments of prove in the superscript and subscript respectively,
$$\mathsf{prove}^P_{\mathsf{pk}}(x, w) := \mathsf{prove}(P, \mathsf{pk}, x, w)$$
- We write the VerifyingKey argument of verify in the subscript,
$$\mathsf{verify}_{\mathsf{vk}}(x, \pi) := \mathsf{verify}(\mathsf{vk}, x, \pi)$$
- Given P: Statement and pk: ProvingKey, we define the function
$$\mathsf{satisfying}^P_{\mathsf{pk}} : \mathsf{PublicInput} \times \mathsf{SecretInput} \longrightarrow \mathsf{Bool},$$
which is true if $\exists \pi : \mathsf{Proof}$ such that $\mathsf{Some}(\pi) \in \mathsf{prove}^P_{\mathsf{pk}}(x, w)$ and false otherwise. If $\mathsf{satisfying}^P_{\mathsf{pk}}(x, w) = \mathsf{True}$, we call the pair (x, w) a *satisfying input*.

Every NIZK has the following properties for a fixed statement $P : \mathsf{Statement}$ and keys $(\mathsf{pk}, \mathsf{vk}) \sim \mathsf{keys}(P)$:

- **Completeness**: For all $(x, w) : \mathsf{PublicInput} \times \mathsf{SecretInput}$, if $\mathsf{satisfying}^P_{\mathsf{pk}}(x, w) = \mathsf{True}$ with proof witness π, then $\mathsf{verify}_{\mathsf{vk}}(x, \pi) = \mathsf{True}$.
- **Knowledge Soundness**: For any polynomial-size adversary $\mathcal{A}$ such that the probability

$$\Pr\left[\mathsf{verify}_{\mathsf{vk}}(x, \pi) = \mathsf{True} \;\middle|\; \begin{array}{l}(\mathsf{pk}, \mathsf{vk}) \sim \mathsf{keys}(P) \\ (x, \pi) \sim \mathcal{A}(\mathsf{pk}, \mathsf{vk})\end{array}\right]$$

  is non-negligible, there exists a polynomial-size extractor $\mathcal{E}_{\mathcal{A}}$

$$\mathcal{E}_{\mathcal{A}} : \mathsf{ProvingKey} \times \mathsf{VerifyingKey} \to \mathfrak{D}\langle \mathsf{SecretInput} \rangle$$

  such that the difference

$$\left| \Pr\left[\mathsf{verify}_{\mathsf{vk}}(x, \pi) = \mathsf{True} \;\middle|\; \begin{array}{l}(\mathsf{pk}, \mathsf{vk}) \sim \mathsf{keys}(P) \\ (x, \pi) \sim \mathcal{A}(\mathsf{pk}, \mathsf{vk})\end{array}\right] - \Pr\left[\mathsf{satisfying}^P_{\mathsf{pk}}(x, w) = \mathsf{True} \;\middle|\; w \sim \mathcal{E}_{\mathcal{A}}(\mathsf{pk}, \mathsf{vk})\right] \right|$$

  is negligible.
- **Statistical Zero-Knowledge**: There exists a stateful simulator $\mathcal{S}$, such that for all stateful distinguishers $\mathcal{D}$, the difference between the following two probabilities is negligible:

$$\Pr\left[\begin{array}{c}\mathsf{satisfying}^P_{\mathsf{pk}}(x, w) = \mathsf{True} \\ \mathcal{D}(\pi) = \mathsf{True}\end{array} \;\middle|\; \begin{array}{l}(\mathsf{pk}, \mathsf{vk}) \sim \mathsf{keys}(P) \\ (x, w) \sim \mathcal{D}(\mathsf{pk}, \mathsf{vk}) \\ \mathsf{Some}(\pi) \sim \mathsf{prove}^P_{\mathsf{pk}}(x, w)\end{array}\right] \text{ and } \Pr\left[\begin{array}{c}\mathsf{satisfying}^P_{\mathsf{pk}}(x, w) = \mathsf{True} \\ \mathcal{D}(\pi) = \mathsf{True}\end{array} \;\middle|\; \begin{array}{l}(\mathsf{pk}, \mathsf{vk}) \sim \mathcal{S}(P) \\ (x, w) \sim \mathcal{D}(\mathsf{pk}, \mathsf{vk}) \\ \pi \sim \mathcal{S}(x)\end{array}\right]$$

- **Succinctness**: For all $(x, w) : \mathsf{PublicInput} \times \mathsf{SecretInput}$, if $\mathsf{Some}(\pi) \sim \mathsf{prove}(P, \mathsf{pk}, x, w)$, then $|\pi| = \mathcal{O}(1)$, and $\mathsf{verify}(\mathsf{vk}, x, \pi)$ runs in time $\mathcal{O}(|x|)$.

Definition 4.1.7 (Cryptographic Group)**.** We define a *cryptographic group* $(\mathbb{G}, p, g)$ as a finite cyclic group $\mathbb{G}$, of prime order p with generator g where the discrete logarithm problem is hard, namely, given $X \in \mathbb{G}$ it is infeasible to find x such that $X = g^x$. We may omit the prime p when convenient.

4.2 Addresses and Key Components

For the $\mathsf{Transfer}$ protocol we use a multi-layered system of keys:

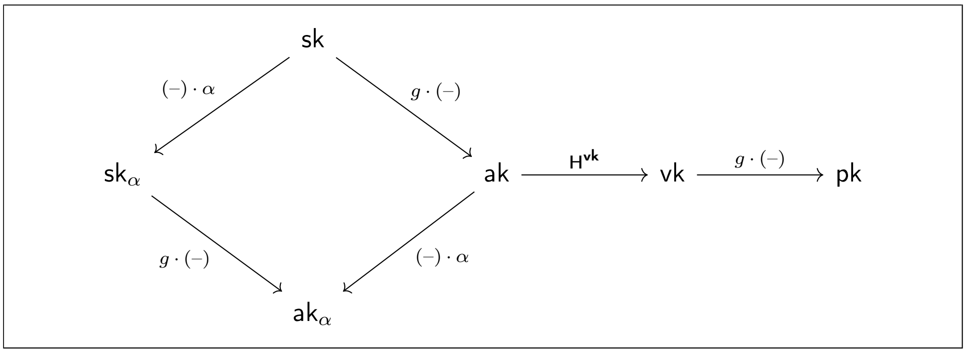

Figure 2: Detailed Key Schedule for $\mathsf{MantaPay}$ where α is a random scalar and g is a generator.

Here we define each key and its function in the $\mathsf{Transfer}$ protocol:

Definition 4.2.1 (Key Schedule)**.** A $\mathsf{KeySchedule}$ is a collection of implementations of the following abstract cryptographic primitives as described in the above definitions:

- **Cryptographic Group**: $(\mathbb{G}, p, g)$
- **Viewing Key Derivation Function**: H^{vk}
- **Proof Authorization Signature**: SIG

with the following notational conventions:

$$\begin{aligned} \mathsf{SpendingKey} &:= \mathbb{Z}_p \\ \mathsf{ProofAuthorizingKey} &:= \mathbb{G} \\ \mathsf{ViewingKey} &:= \mathbb{Z}_p \\ \mathsf{zkAddress} &:= \mathbb{G} \end{aligned}$$

with the following constraints:

$$\begin{aligned} \mathsf{SIG.SecretKey} &= \mathbb{Z}_p \\ \mathsf{SIG.PublicKey} &= \mathbb{G} \\ \mathsf{SIG.derive} &= g \cdot (-) \end{aligned}$$

To derive the zkAddress, pk, we use the following:

$$\mathsf{sk} \quad \mapsto \quad \mathsf{ak} := g \cdot \mathsf{sk} \quad \mapsto \quad \mathsf{vk} := \mathsf{H}^{\mathsf{vk}}(\mathsf{ak}) \quad \mapsto \quad \mathsf{pk} := g \cdot \mathsf{vk}$$

For signing a message m with a randomized key, the owner of the SpendingKey, sk, and owner of the ProofAuthorizingKey, ak, perform the following protocol:

1. Spender samples α randomly and sends it to prover.
2. Prover computes $\mathsf{ak}_\alpha := \mathsf{ak} \cdot \alpha$ and binds it to the message m and sends the message to spender.
3. Spender computes $\mathsf{sk}_\alpha := \mathsf{sk} \cdot \alpha$ and checks that $\mathsf{ak}_\alpha = g \cdot \mathsf{sk}_\alpha$ and signs the message m with sk_α.

4.3 Transfer Protocol

The Transfer protocol is the core abstraction of MantaPay and facilitiates the valid transfer of zkAssets among participants while preserving their privacy. The Transfer is made up of cryptographic constructions called Senders and Receivers that represent the private input and private output of a transaction respectively. To perform a Transfer, a protocol participant chooses a SpendingKey they own, selects a subset of the UTXOs they have still not yet spent (for a fixed AssetId), collects zkAddresses from other participants for the private outputs, assigning each key a subset of the input zkAssets, and then builds a Transfer object representing the desired transaction. From this Transfer object, they construct a TransferPost, a representation of the transaction that contains only public information, and send it to the Ledger to be verified. The transformation from a Transfer to a TransferPost involves producing a *zero-knowledge proof* that attests to the valid construction of this public data from the private data.

We begin by defining the cryptographic primitives involved in the Transfer protocol:

Definition 4.3.1. UTXO For a field $\mathbb{F}$, we define a UTXO as the following record:

t : Bool	*transparency flag*
pa : Asset	*public AssetId and AssetValue pair*
cm : $\mathbb{F}$	*asset and public key commitment*

A UTXO represents the ownership of a zkAsset that can be in one of two forms, either *transparent* when $t =$ True or *opaque* when $t =$ False. Whenever a UTXO is transparent, the zkAsset it represents is written in the pa field in plain-text and the owner is hidden by the commitment cm. Whenever a UTXO is opaque, the zkAsset it represents and the owner are both hidden by the commitment cm and the pa is unused. We will see below how this UTXO is constructed.

Definition 4.3.2 (Transfer Configuration)**.** A TransferConfiguration is a collection of implementations of the following abstract cryptographic primitives:

- **Key Schedule**: KeySchedule
- **Incoming Authenticated Encryption Scheme**: $\mathsf{AUTH}^{\mathsf{in}}$
- **Outgoing Authenticated Encryption Scheme**: $\mathsf{AUTH}^{\mathsf{out}}$
- **UTXO Commitment Scheme**: $\mathsf{COM}^{\mathsf{U}} : \mathbb{F} \times \mathbb{G} \times \mathsf{Asset} \to \mathbb{F}$
- **Nullifier Commitment Scheme**: $\mathsf{COM}^{\mathsf{N}} : \mathbb{G} \times \mathbb{F} \to \mathbb{F}$
- **UTXO Hash Function**: $\mathsf{H}^{\mathsf{U}} : \mathsf{UTXO} \to \mathbb{F}$
- **UTXO Dynamic Cryptographic Accumulator**: UTXOSet
- **Zero-Knowledge Proving System**: NIZK

where $\mathbb{F}$ is a prime field and $\mathbb{G}$ is a cryptographic group. The Nullifier type is defined as the output of $\mathsf{COM}^{\mathsf{N}}$.

For the rest of this section, we assume the existence of a $\mathsf{TransferConfiguration}$ and use the primitives outlined above explicitly. We continue by defining the Sender and $\mathsf{Receiver}$ constructions as well as their public counterparts, the $\mathsf{SenderPost}$ and $\mathsf{ReceiverPost}$.

Definition 4.3.3 (Transfer Sender)**.** A Sender is the following record:

$$
\begin{aligned}
r &: \mathbb{F} && \textit{UTXO commitment randomness} \\
\mathsf{sa} &: \mathsf{Asset} && \textit{secret AssetId and AssetValue pair} \\
\mathsf{pa} &: \mathsf{Asset} && \textit{public AssetId and AssetValue pair} \\
t &: \mathsf{Bool} && \textit{transparency flag} \\
\mathsf{asset} &: \mathsf{Asset} && \textit{representative non-zero AssetId and AssetValue pair} \\
\mathsf{cm} &: \mathbb{F} && \textit{asset and public key commitment} \\
\mathsf{utxo} &: \mathsf{UTXO} && \textit{full UTXO} \\
h &: \mathbb{F} && \textit{UTXO hash} \\
h_z &: \mathsf{UTXOSet.Output} && \textit{UTXO hash accumulator output} \\
h_w &: \mathsf{UTXOSet.Witness} && \textit{UTXO hash accumulator witness} \\
n &: \mathsf{Nullifier} && \textit{Nullifier} \\
\mathsf{esk} &: \mathbb{Z}_p && \textit{Ephemeral Secret Key} \\
\mathsf{epk} &: \mathbb{G} && \textit{Ephemeral Public Key} \\
\mathsf{C_{out}} &: \mathsf{AUTH^{out}.Ciphertext} && \textit{Outgoing Encrypted Note Ciphertext}
\end{aligned}
$$

A Sender, S, is constructed from a public key $\mathsf{pk} : \mathsf{zkAddress}$ with the following algorithm:

$$
\begin{aligned}
t &:= \mathsf{iszero}(\mathsf{sa.id}) \wedge \mathsf{iszero}(\mathsf{sa.value}) \\
\mathsf{asset} &:= \mathsf{select}(t, \mathsf{sa}, \mathsf{pa}) \\
\mathsf{cm} &:= \mathsf{COM^U}(r, \mathsf{pk}, \mathsf{sa}) \\
\mathsf{utxo} &:= (t, \mathsf{pa}, \mathsf{cm}) \\
h &:= \mathsf{H^U}(\mathsf{utxo}) \\
\mathsf{Some}\,(h_z, h_w) &:= \mathsf{UTXOSet.contains}(h, \mathsf{Ledger.utxos}()) \\
n &:= \mathsf{COM^N}(\mathsf{ak}, h) \\
\mathsf{epk} &:= g \cdot \mathsf{esk} \\
\mathsf{C_{out}} &:= \mathsf{AUTH^{out}.encrypt}(\mathsf{pk} \cdot \mathsf{esk}, \mathsf{select}(t, \mathsf{sa}, \mathsf{pa}))
\end{aligned}
$$

Definition 4.3.4 (Transfer Sender Post)**.** A $\mathsf{SenderPost}$ is the following record extracted from a Sender:

$$
\begin{aligned}
h_z &: \mathsf{UTXOSet.Output} \\
n &: \mathsf{Nullifier} \\
\mathsf{epk} &: \mathbb{G} \\
\mathsf{C_{out}} &: \mathsf{AUTH^{out}.Ciphertext}
\end{aligned}
$$

which are the parts of a Sender which should be *posted* to the Ledger.

Definition 4.3.5 (Transfer Receiver)**.** A $\mathsf{Receiver}$ is the following record:

$$
\begin{aligned}
r &: \mathbb{F} && \textit{UTXO commitment randomness} \\
\mathsf{sa} &: \mathsf{Asset} && \textit{secret AssetId and AssetValue pair} \\
\mathsf{pa} &: \mathsf{Asset} && \textit{public AssetId and AssetValue pair} \\
t &: \mathsf{Bool} && \textit{transparency flag} \\
\mathsf{asset} &: \mathsf{Asset} && \textit{representative non-zero AssetId and AssetValue pair} \\
\mathsf{cm} &: \mathbb{F} && \textit{asset and public key commitment} \\
\mathsf{utxo} &: \mathsf{UTXO} && \textit{full UTXO} \\
\mathsf{esk} &: \mathbb{Z}_p && \textit{Ephemeral Secret Key} \\
\mathsf{epk} &: \mathbb{G} && \textit{Ephemeral Public Key} \\
\mathsf{C_{in}} &: \mathsf{AUTH^{in}.Ciphertext} && \textit{Incoming Encrypted Note Ciphertext}
\end{aligned}
$$

A $\mathsf{Receiver}$, R, is constructed from a public key $\mathsf{pk} : \mathsf{zkAddress}$ with the following algorithm:

$$\begin{aligned} t &:= \mathsf{iszero}(\mathsf{sa.id}) \wedge \mathsf{iszero}(\mathsf{sa.value}) \\ \mathsf{asset} &:= \mathsf{select}(t, \mathsf{sa}, \mathsf{pa}) \\ \mathsf{cm} &:= \mathsf{COM}^{\mathsf{U}}(r, \mathsf{pk}, \mathsf{sa}) \\ \mathsf{utxo} &:= (t, \mathsf{pa}, \mathsf{cm}) \\ \mathsf{epk} &:= g \cdot \mathsf{esk} \\ \mathsf{C_{in}} &:= \mathsf{AUTH}^{\mathsf{in}}.\mathsf{encrypt}(\mathsf{pk} \cdot \mathsf{esk}, (r, \mathsf{sa})) \end{aligned}$$

Definition 4.3.6 (Transfer Receiver Post)**.** A ReceiverPost is the following record extracted from a Receiver:

$$\begin{aligned} \mathsf{utxo} &: \mathsf{UTXO} \\ \mathsf{epk} &: \mathbb{G} \\ \mathsf{C_{in}} &: \mathsf{AUTH}^{\mathsf{in}}.\mathsf{Ciphertext} \end{aligned}$$

which are the parts of a Receiver which should be *posted* to the Ledger.

Definition 4.3.7 (Transfer Sources and Sinks)**.** A Source (or a Sink) is an Asset representing a public input (or output) of a Transfer.

Definition 4.3.8 (Transfer Object)**.** A Transfer is the following record:

$$\begin{aligned} \mathsf{id} &: \mathsf{Option}(\mathsf{AssetId}) \\ \mathsf{sources} &: \mathsf{List}(\mathsf{AssetValue}) \\ \mathsf{senders} &: \mathsf{List}(\mathsf{Sender}) \\ \mathsf{receivers} &: \mathsf{List}(\mathsf{Receiver}) \\ \mathsf{sinks} &: \mathsf{List}(\mathsf{AssetValue}) \end{aligned}$$

The *shape* of a Transfer is the following 4-tuple of cardinalities of those sets

$$\left(|T.\mathsf{sources}|\,, |T.\mathsf{senders}|\,, |T.\mathsf{receivers}|\,, |T.\mathsf{sinks}|\right)$$

Also, note that the id value is optional. This is inhabited whenever there are sources or sinks, but if the shape of the transaction is $(0, m, n, 0)$ then $\mathsf{id} = \mathsf{None}$.

In order for a Transfer to be considered *valid*, it must adhere to the following constraints:

- **Correct Key Signing**: The keys used to construct Senders and Receivers are valid and can be signed by a unique SpendingKey.
- **Same Id**: All the AssetIds in the Transfer must be equal.
- **Balanced**: The sum of input AssetValues must be equal to the sum of output AssetValues.
- **Well-formed Senders**: All of the Senders in the Transfer must be constructed according to the above Sender definition.
- **Well-formed Receivers**: All of the Receivers in the Transfer must be constructed according to the above Receiver definition.

In order to prove that these constraints are satisfied for a given Transfer, we build a zero-knowledge proof which will witness that the Transfer is valid and should be accepted by the Ledger.

Definition 4.3.9 (Transfer Validity Statement)**.** A transfer $T : \mathsf{Transfer}$ is considered *valid* if and only if

1. The signing authority is correctly constructed:

$$\begin{aligned} \mathsf{ak}_\alpha &:= \mathsf{ak} \cdot \alpha \\ \mathsf{vk} &:= \mathsf{H}^{\mathsf{vk}}(\mathsf{ak}) \\ \mathsf{pk} &:= g \cdot \mathsf{vk} \end{aligned}$$

2. All the AssetIds in T are equal:

$$\left| T.\mathsf{id} \cup \left(\bigcup_{S \in T.\mathsf{senders}} S.\mathsf{asset.id} \right) \cup \left(\bigcup_{R \in T.\mathsf{receivers}} R.\mathsf{asset.id} \right) \right| = 1$$

3. The sum of input AssetValues is equal to the sum of output AssetValues:

$$\left(\sum_{a \in T.\mathsf{sources}} a\right) + \left(\sum_{S \in T.\mathsf{senders}} S.\mathsf{asset.value}\right) = \left(\sum_{R \in T.\mathsf{receivers}} R.\mathsf{asset.value}\right) + \left(\sum_{a \in T.\mathsf{sinks}} a\right)$$

4. For all $S \in T.\mathsf{senders}$, the Sender S is well-formed:

$$\begin{aligned} S.t &= \mathsf{iszero}(S.\mathsf{sa.id}) \wedge \mathsf{iszero}(S.\mathsf{sa.value}) \\ S.\mathsf{asset} &= \mathsf{select}(S.t, S.\mathsf{sa}, S.\mathsf{pa}) \\ S.\mathsf{cm} &= \mathsf{COM}^{\mathsf{U}}(S.r, S.\mathsf{pk}, S.\mathsf{sa}) \\ S.\mathsf{utxo} &= (S.t, S.\mathsf{pa}, S.\mathsf{cm}) \\ S.h &= \mathsf{H}^{\mathsf{U}}(S.\mathsf{utxo}) \\ \mathsf{iszero}(S.\mathsf{asset.value}) &\vee \mathsf{UTXOSet.verify}(S.h, S.h_z, S.h_w) = \mathsf{True} \\ S.n &= \mathsf{COM}^{\mathsf{N}}(\mathsf{ak}, S.h) \\ S.\mathsf{epk} &= g \cdot S.\mathsf{esk} \\ S.\mathsf{C}_{\mathsf{out}} &= \mathsf{AUTH}^{\mathsf{out}}.\mathsf{encrypt}(\mathsf{pk} \cdot S.\mathsf{esk}, S.\mathsf{asset}) \end{aligned}$$

5. For all $R \in T.\mathsf{receivers}$, the Receiver R is well-formed:

$$\begin{aligned} R.t &= \mathsf{iszero}(R.\mathsf{sa.id}) \wedge \mathsf{iszero}(R.\mathsf{sa.value}) \\ R.\mathsf{asset} &= \mathsf{select}(R.t, R.\mathsf{sa}, R.\mathsf{pa}) \\ R.\mathsf{cm} &= \mathsf{COM}^{\mathsf{U}}(R.r, R.\mathsf{pk}, R.\mathsf{sa}) \\ R.\mathsf{utxo} &= (R.t, R.\mathsf{pa}, R.\mathsf{cm}) \\ R.\mathsf{epk} &= g \cdot R.\mathsf{esk} \\ R.\mathsf{C}_{\mathsf{in}} &= \mathsf{AUTH}^{\mathsf{in}}.\mathsf{encrypt}(R.\mathsf{pk} \cdot R.\mathsf{esk}, (R.r, R.\mathsf{sa})) \end{aligned}$$

Notation: This statement is denoted ValidTransfer and is assumed to be expressible as a Statement of NIZK.

To finish the transfer, the SpendingKey for the Transfer.ak : ProofAuthorizingKey needs to sign the public side of the transaction. The public part of the transaction is the following post body:

Definition 4.3.10 (Transfer Post Body)**.** A TransferPostBody is the following record:

$$\begin{aligned} \mathsf{id} &: \mathsf{Option}(\mathsf{AssetId}) \\ \mathsf{sources} &: \mathsf{List}(\mathsf{Source}) \\ \mathsf{senders} &: \mathsf{List}(\mathsf{SenderPost}) \\ \mathsf{receivers} &: \mathsf{List}(\mathsf{ReceiverPost}) \\ \mathsf{sinks} &: \mathsf{List}(\mathsf{Sink}) \\ \pi &: \mathsf{NIZK.Proof} \end{aligned}$$

A TransferPostBody, B, is constructed by assembling the zero-knowledge proof of Transfer validity from a known proving key pk : NIZK.ProvingKey and a given T : Transfer:

$$\begin{aligned} x &:= \mathsf{Transfer.public}(T) \\ w &:= \mathsf{Transfer.secret}(T) \\ \mathsf{Some}(\pi) &\sim \mathsf{NIZK.prove}_{\mathsf{pk}}^{\mathsf{ValidTransfer}}(x, w) \\ B.\mathsf{id} &:= x.\mathsf{id} \\ B.\mathsf{sources} &:= x.\mathsf{sources} \\ B.\mathsf{senders} &:= x.\mathsf{senders} \\ B.\mathsf{receivers} &:= x.\mathsf{receivers} \\ B.\mathsf{sinks} &:= x.\mathsf{sinks} \\ B.\pi &:= \pi \end{aligned}$$

where Transfer.public returns SenderPosts for each Sender in T and ReceiverPosts for each Receiver in T, keeping Sources and Sinks as they are, and Transfer.secret returns all the rest of T which is not part of the output of Transfer.public.

Now we can sign this body with $\mathsf{sk}_\alpha : \mathsf{SpendingKey} := \mathsf{sk} \cdot \alpha$ where the signature scheme has TransferPostBody as the SIG.Message type and we use ak_α as the verifying key:

Definition 4.3.11 (Transfer Post)**.** A TransferPost is the following record:

$$\begin{aligned} \sigma &: \mathsf{Option}(\mathsf{SIG.VerifyingKey} \times \mathsf{SIG.Signature}) \\ \mathsf{body} &: \mathsf{TransferPostBody} \end{aligned}$$

Note that the σ value is optional. This is inhabited whenever the number of Senders in a transaction is positive.

Now that a participant has constructed a transfer post P : TransferPost they can send it to the Ledger for verification.

Definition 4.3.12 (Ledger-side Transfer Validity)**.** To check that P represents a valid Transfer, the ledger checks the following:

- **Verify Signature**: Check that $\mathsf{SIG.verify}(P.\sigma_0, P.\sigma_1, P.\mathsf{body}) = \mathsf{True}$. This check is only performed if the transfer shape includes at least one Sender.
- **Public Withdraw**: All the public addresses corresponding to the Assets in P.body.sources have enough public balance (i.e. in the PublicAssetLedger) to withdraw the given Asset.
- **Public Deposit**: All the public addresses corresponding to the Assets in P.body.sinks exist.
- **Current Accumulated State**: The UTXOSet.Output stored in each P.body.senders is equal to current accumulated value, UTXOSet.current(Ledger.utxos()), for the current state of the Ledger.
- **New Nullifiers**: All the Nullifiers in P.body.senders are unique, and no Nullifier in P.body.senders has already been stored in the Ledger.NullifierSet.
- **New UTXOs**: All the UTXOs in P.body.receivers are unique, and no UTXO in P.body.receivers has already been stored on the ledger.
- **Verify Transfer**: Check that the following relation holds:

$$\begin{aligned} &\mathsf{NIZK.verify}_{\mathsf{vk}}(\\ &\qquad P.\sigma_0 \,||\, P.\mathsf{body.id} \,||\, P.\mathsf{body.sources} \,||\, P.\mathsf{body.senders} \,||\, P.\mathsf{body.receivers} \,||\, P.\mathsf{body.sinks}, \\ &\qquad P.\mathsf{body}.\pi \\ &\ ) = \mathsf{True} \end{aligned}$$

  where $P.\sigma_0$ is included whenever the transfer shape includes at least one Sender and P.body.id is included whenever the transfer shape includes at least one of Sources or Sinks.

Definition 4.3.13 (Ledger Transfer Update)**.** After checking that a given TransferPost P is valid, the Ledger updates its state by performing the following changes:

- **Public Updates**: All the relevant public accounts on the PublicAssetLedger are updated to reflect their new balances using the Sources and Sinks present in P.
- **UTXOSet Update**: The new UTXOs are appended to the UTXOSet.
- **NullifierSet Update**: The new Nullifiers are appended to the NullifierSet.

4.4 Batched Transactions

For MantaPay participants to use the Transfer protocol, they will need to keep track of the current state of their zkAssets and use them to build TransferPosts to send to the Ledger. The balance of any participant is the sum of the balances of their zkAssets, but this balance may be fragmented into arbitrarily many pieces, as each piece represents an independent asset that the participant received as the output of some Transfer. To then spend a subset of their balance, the participant would need to accumulate all of the relevant fragments into a large enough zkAsset to spend all at once, building a collection of TransferPosts to send to the Ledger.

Any wallet implementation should see that their users need not keep track of this complexity themselves. Instead, like a public ledger, the notion of a *transaction* between one participant and another should be viewed as a single atomic action that the user can take, performing a withdrawl from their balance. To describe such a *batched transaction*, we assume the existence of two transfer shapes[3]: Mint with shape $(1, 0, 1, 0)$ and PrivateTransfer with shape $(0, N, N, 0)$ for some natural number $N > 1$.

[3] Other Transfer accumulation algorithms are possible with different starting shapes.

Algorithm 1 Batched Transaction Algorithm

```
procedure BUILDBATCH(sk, 𝓑, total, pk)
    B ← Sample(total, 𝓑)                          ▷ Samples coins from 𝓑 that total at least total
    if len(B) = 0 then
        return [ ]                                 ▷ Insufficient Balance
    end if
    P ← [ ]                                        ▷ Allocate a new list for TransferPosts
    while len(B) > N do                            ▷ While there are enough pairs to make another Transfer
        A ← [ ]
        for b ∈ (B, N) do                          ▷ Get the next N pairs from B
            S ← BuildSenders_sk(b)
            [acc, zs...] ← BuildAccumulatorAndZeroes_sk(S)    ▷ Build a new accumulator and zeroes
            P ← P + TransferPost(Transfer([], S, [acc, zs...], []))
            (A, Z) ← (A + acc, Z + zs)             ▷ Save acc for the next loop, zs for the end
        end for
        B ← A + remainder(B, N)
    end while
    S ← PrepareZeroes_sk(N, B, Z, P)               ▷ Use Z and Mints to make B go up to N in size.
    R ← BuildReceiver_sk(pk, S)
    [c, zs...] ← BuildAccumulatorAndZeroes_sk(S)
    return P + TransferPost(Transfer([], S, [R, c, zs...], []))
end procedure
```

For a fixed spending key, $\mathsf{sk} : \mathsf{SpendingKey}$, and asset id, $\mathsf{id} : \mathsf{AssetId}$, we are given a balance state, $\mathcal{B} : \mathsf{FinSet}\,(\mathsf{Bool} \times \mathbb{F} \times \mathsf{AssetValue})$, a set of transparenct-blinder-balance triples for unspent assets, a total balance to withdraw, $\mathsf{total} : \mathsf{AssetValue}$, and a receiving key $\mathsf{pk} : \mathsf{zkAddress}$. We can then compute

$$\textsc{BuildBatch}(\mathsf{sk}, \mathcal{B}, \mathsf{total}, \mathsf{pk})$$

to receive a $\mathsf{List}(\mathsf{TransferPost})$ to send to the ledger, representing the transfer of total to pk.

If all of the Transfers are accepted by the ledger, the balance state $\mathcal{B}$ should be updated accordingly, removing all of the pairs which were used in the Transfer. Wallets should also handle the more complex case when only some of the Transfers succeed in which case they need to be able to continue retrying the transaction until they are finally resolved. Since the only Transfer which sends zkAssets out of the control of the user is the last one (and it recursively depends on the previous Transfers), then it is safe to continue from a partially resolved state with a simple retry of the BuildBatch algorithm.

5 Concrete Protocol

We define the instantiation of the abstract protocol in this section, but first some preliminary notes.

5.1 Poseidon Permutation and Poseidon Hash

The **Poseidon** Permutation (**Poseidon**$^\pi$) [2] is a finite field cryptographic primitive that can be used to build many cryptographic primitives, like hash functions, commitment schemes, and symmetric encryption schemes. **Poseidon** plays a fundamental role in simplifying the Transfer protocol and reducing the overall cost of the Zero-Knowledge circuits. **Poseidon**$^\pi$ is a family of permutation functions with the following type:

$$\mathbf{Poseidon}_k^\pi : \mathbb{F} \times \mathbb{F}^k \to \mathbb{F}^k$$

over some sufficiently large finite field $\mathbb{F}$. The first distinguished field element is used as a domain separation element. For this purpose, we use the following hashing function to generate domain strings:

$$\mathsf{HashToScalar}(m) := \mathbb{F}.\mathsf{truncate}(\mathsf{Blake2s}(m))$$

The **Poseidon** hash function (without sponges) with the following type:

$$\mathbf{Poseidon}_k : \mathbb{F} \times \mathbb{F}^k \to \mathbb{F}$$

is defined as extracting the first finite field element out of $\mathbf{Poseidon}_k^\pi$.

We make use of **Poseidon** for a few values of k in the concrete protocol below.

5.2 Elliptic Curve Cryptography

Because our protocol relies on a cryptographic group which should be efficient in a Zero-Knowledge Proving System we choose an elliptic curve defined over the finite field $\mathbb{F}$ of the proving system. To use group elements in affine form we also define the projections:

$$\mathcal{X} : \mathbb{G} \to \mathbb{F} \text{ and } \mathcal{Y} : \mathbb{G} \to \mathbb{F}$$

which we use below to insert group elements into field-only hash functions.

For this protocol, we use `BN254` as our outer (pairing-friendly) curve with scalar field $\mathbb{F}$ and `BabyJubJub` [4] as our inner curve with scalar field $\mathbb{S}$. For this protocol, we call the inner curve $\mathbb{G}$.

5.3 Concrete Cryptographic Schemes

Definition 5.3.1 (Commitment Schemes)**.** The protocol features two different commitment schemes: $\mathsf{COM}^{\mathsf{U}}$ the UTXO Commitment Scheme and $\mathsf{COM}^{\mathsf{N}}$ the Nullifier Commitment Scheme. Both commitment schemes use **Poseidon** as the underlying cryptographic primitive. The UTXO uses an arity-5 **Poseidon** with the following mapping:

$$\mathsf{COM}^{\mathsf{U}}(r, \mathsf{pk}, \mathsf{asset}) := \mathbf{Poseidon}_5(d, r, \mathcal{X}(\mathsf{pk}), \mathcal{Y}(\mathsf{pk}), \mathsf{asset.id}, \mathsf{asset.value})$$

where $d = \mathsf{HashToScalar}(\text{“}\texttt{manta-pay/1.0.0/com-utxo}\text{”})$ the domain separation element. For the Nullifier Commitment Scheme we use an arity-3 **Poseidon** with the following mapping:

$$\mathsf{COM}^{\mathsf{N}}(\mathsf{ak}, h) := \mathbf{Poseidon}_3(d, \mathcal{X}(\mathsf{ak}), \mathcal{Y}(\mathsf{ak}), h)$$

where $d = \mathsf{HashToScalar}(\text{“}\texttt{manta-pay/1.0.0/com-vn}\text{”})$ the domain separation element.

Definition 5.3.2 (Hash Functions)**.** The protocol features two additional hash functions: H^{vk} the viewing key derivation function and H^{U} the UTXO hash function. Both hash functions use **Poseidon** as the underlying cryptographic primitive. The viewing key derivation function uses an arity-2 **Poseidon**

$$\mathsf{H}^{\mathsf{vk}}(\mathsf{ak}) := \mathbf{Poseidon}_2(d, \mathcal{X}(\mathsf{ak}), \mathcal{Y}(\mathsf{ak}))$$

where $d = \mathsf{HashToScalar}(\text{“}\texttt{manta-pay/1.0.0/kdf-vk}\text{”})$ the domain separation element. Since the target type of this hash function is the scalar field $\mathbb{S}$ instead of $\mathbb{F}$, we reduce the result modulo the order of $\mathbb{S}$. For the UTXO hash function we use an arity-4 **Poseidon**

$$H^{\mathsf{U}}(t, \mathsf{pa}, \mathsf{cm}) := \mathbf{Poseidon}_4(d, t, \mathsf{pa.id}, \mathsf{pa.value}, \mathsf{cm})$$

where $d = \mathsf{HashToScalar}(\text{“}\texttt{manta-pay/1.0.0/utxo-hash}\text{”})$ the domain separation element.

Definition 5.3.3 (Signature Scheme)**.** For the signature scheme we use Schnorr signature over the inner curve, $\mathbb{G}$.

Definition 5.3.4 (Authenticated Encryption Scheme)**.** For $\mathsf{AUTH}^{\mathsf{in}}$ and $\mathsf{AUTH}^{\mathsf{out}}$ we use the **Poseidon** permutation as the permutation of a duplex sponge encryption protocol.

Definition 5.3.5 (Dynamic Cryptographic Accumulator)**.** For DCA, we use a Merkle Tree with $\mathbf{Poseidon}_2$ as the inner node combining hash function and no leaf hash function. It is safe to omit the leaf hash function in this case because the leaf values are already the outputs of a hash function and cannot be directly controlled.

Definition 5.3.6 (Non-Interactive Zero-Knowledge Proving System)**.** For NIZK, the protocol can use any non-interactive zero-knowledge proving system like Groth16 [2] and/or PLONK/PLONKUP [1, 3].

5.4 AssetValue Bounds Check

In order to implement the balanced transfer relation one needs to ensure that the amount of input value is equal to the amount of output value. However, since we're working over finite fields, the naïve arithmetic wraps past zero and is vulnerable to range-based attacks. Instead we constrain every $\mathsf{AssetValue}$ to be less than some bound $\mathcal{V}$ and that every sum over those values is also less than $\mathcal{V}$. Since we're using `BN254` we are safe to use $\mathcal{V} = 2^{128}$.

6 Acknowledgements

We would like to thank Luke Pearson and Toghrul Maharramov for our insightful discussions on reusable shielded addresses.

References

[1] Ariel Gabizon, Zachary J. Williamson, and Oana Ciobotaru. PLONK: permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge. *IACR Cryptol. ePrint Arch.*, page 953, 2019.

[2] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. Poseidon: A new hash function for zero-knowledge proof systems. In *USENIX Security Symposium*, pages 519–535. USENIX Association, 2021.

[3] Luke Pearson, Joshua Fitzgerald, Héctor Masip, Marta Bellés-Muñoz, and Jose Luis Muñoz-Tapia. Plonkup: Reconciling plonk with plookup. *IACR Cryptol. ePrint Arch.*, page 86, 2022.

[4] Barry WhiteHat, Marta Bellés, and Jordi Baylina. EIP-2494: Baby Jubjub Elliptic Curve . Eip, Ethereum Foundation, 2020.