A Survey of Three Atomic Swaps with Monero

F. Barbàra[1]

`me@fadibarbara.it`

Abstract. The abstract should briefly summarize the contents of the paper in 150–250 words.

Keywords: First keyword · Second keyword · Another keyword.

1 What is an Atomic Swap?

2 First Section

3 Building blocks

Three building blocks make atomic swaps from (respectively to Monero to (resp. from) other blockchain possible: a Discrete-Logarithm Equality Proof (DLEP), the use of Adaptor Signatures, and the use of view keys in the Monero blockchain. In the following we analyze these building blocks.

3.1 Discrete-Logarithm Equality Proof

All the presented atomic swaps methods leverage the use of the same private keys on both the Monero and the Bitcoin or Ethereum blockchain. On the one hand this is an efficient way to deal with the lack of scripts capabilities of Monero and it paves the way to the use of adaptor signatures (Section 3.2). On the other hand since Monero and Bitcoin (or Monero and Ethereum) do *not* share the same curve proving equality of priva keys on two curves requires some non trivial work.

All three atomic swap methods reference the technical note written by Noether [1] [2] as their base for the DLEP construction.

While the technical note presents all the computational information needed ot perform a succesful DLEP, the note does not provide any theoreticla information. A formalization of the content of the note ca be foun in Appendix I of this work. In this section we just highlight the foundational steps.

The Noether DLEP in [2] is a non-interactive zero-knowledge proof of knowledge between two actors: Peggy (acting as the prover) and Victor (acting as the verifier). We assume that Peggy and Victor share the parameters of the two

---

[1] As written on the note the credit for the first presentation of the DLEP goes to Andrew Poelstra

groups $\mathbb{G}$ and $\mathbb{H}$, with points $G, G' \in \mathbb{G}$ and $H, H' \in \mathbb{H}$ generators of the respective froups. We also assume $|G| = p$ and $|H| = q$, with p and q prime numbers and $p < q$. The goal of Peggy is to provide two points $xG' \in \mathbb{G}$ and $xH' \in \mathbb{H}$, and a proof that xG' and xH' share the same descrete logarithm $x < p^2$. The proof is built in a three steps process.

In the first step peggy splits x into a bit sequence, and creates as manny "blinders" as the number of bits of x, for each group. Formally:

1. $x = \sum_{i=0}^{n-1} 2^i b_i$
2. $r_0, \ldots, r_{n-2} \overset{\$}{\leftarrow} \mathbb{Z}_p, \quad s_0, \ldots, s_{n-2} \overset{\$}{\leftarrow} \mathbb{Z}_q$
3. $r_{n-1} = -(2^{n-1})^{-1} \sum_{i=0}^{n-2} 2^i r_i, \quad s_{n-1} = -(2^{n-1})^{-1} \sum_{i=0}^{n-2} 2^i s_i$

In the second step, Peggy creates Pedersen Commitments for each (b_i, r_i) and (b_i, s_i), for a total of $2n$ commitments:

$$C_i^{\mathbb{G}} = b_i G' + r_i G, \quad C_i^{\mathbb{H}} = b_i H' + r_i H, \quad \forall i = 0, \ldots, n-1$$

In the third step, Peggy creates $2n$ different Schnorr ring-signatures of the commitments: two signatures for each message $(C_i^{\mathbb{G}}, C_i^{\mathbb{H}})$, the first signed with r_i and the second with s_i. The signing procedure derives from the work of Abe, Okhubo and Suzuki [1], and since a complete treatment and a comparison between the work done in [2] and [1] is provided in Appendix I, we omit the details in this section. We just say that the proof π is so composed:

$$\pi = (xG', xH', \{\sigma_i^{\mathbb{G}}\}_{i=0}^{n-1}, \{\sigma_i^{\mathbb{H}}\}_{i=0}^{n-1}) \tag{1}$$

where $\{\sigma_i^{\mathbb{G}}\}_{i=0}^{n-1}$ are the n signatures of the commmitments using r_i.

3.2   Adaptor Signatures

3.3   View Keys

References

1. Abe, M., Ohkubo, M., Suzuki, K.: 1-out-of-n signatures from a variety of keys. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **87-A**(1), 131–140 (2004), https://link.springer.com/content/pdf/10.1007/3-540-36178-2_26.pdf
2. Noether, S.: Mrl-0010: Dirscrete logarithm equality across groups. Tech. rep., Monero Research Lab (2018)

---

[2] The definition of *same* requires some more formal definition, which can be found in Appendix **Iinsert reference**.

Appendix I

The goal of this post is the expansion of the MRL-0010 technical note by Sarang Noether in the Monero Research Lab [2] (the "report" from now on) into a more complete work. We will see why pieces of the report fit together.

The goal is to prove that two point $A \in \mathbb{G}$ and $B \in \mathbb{H}$ share the same (up to equivalence) discrete logarithm, i.e. if $A = aG$ where $G \in \mathbb{G}$ is the generator of $\mathbb{G}$ and if $B = bH$ where $H \in \mathbb{H}$ is the generator of $\mathbb{H}$ then $a = b$ (up to equivalence).

We proced in the following manner. Since this is actually a zero-knowledge proof of knowledge, we first explain how to *prove* the equality and then how to *verify* the proof. finally we see how to derive proofs of correctness and security.

As in Section 3.1, we assume Peggy (the prover) wants to prove to Victor (the verifier) the equality. We assume Peggy and Victor to have knowledge of the parameters of both curves. In particular they know of the generators $G, G' \in \mathbb{G}$ and $H, H' \in \mathbb{H}$ and of two statistically independent hash functions:

$$H_\mathbb{G} : \{0,1\}^* \to \mathbb{Z}_p, \qquad p = |G|, |G| := \min\{a \in \mathbb{N} | aG = 0\} \qquad (2)$$
$$H_\mathbb{H} : \{0,1\}^* \to \mathbb{Z}_q, \qquad q = |H|, \qquad (3)$$

Using the aforementioned notation, our goal is to give Peggy a way to contruct a proof for Victor showing the discrete logarithm equality of two points $xG' \in \mathbb{G}$ and $xH' \in \mathbb{H}$, withour revealing x. Also, without loss of generality, assume $p < q$.

3.4   Proof Construction

The proof construction is a three steps process. The bulk of the proof is built in the third steps, which as mentioned can be seen as deriving from the work on ring-signatures in Abe *et al.* [1]. The rest of this section is so composed. We first explain Steps 1 and 2, then we explain how a ring signature is composed under [1] and finally we use it to explain how to complete the proof π in the last part of this section.

Step 1 The first intuition is to see the discrete logarithm x as the sequence of bits in its bit representation. In other words, $x = b_{n-1}, \ldots, b_0$, or

$$x = \sum_{i=0}^{n-1} b_i 2^i \qquad (4)$$

Note that since $b_i \in \{0, 1\}$ then b_i can be easily mapped and used as element of either $\mathbb{Z}_p$ or $\mathbb{Z}_q$.

Step 2 Goal of this step is to create two sets of Pedersen Commitments, one set for xG' and one for xH'. In each set, each commitment is a commitment for one bit. Next paragraph explain the procedure in details.

give better definition AND insert use cases

are they?

Step 2.1 Create two sets of $n-1$ blinders

$$r_{n-2}, \dots, r_0 \xleftarrow{\$} \mathbb{Z}_p, \quad s_{n-2}, \dots, s_0 \xleftarrow{\$} \mathbb{Z}_q \tag{5}$$

Step 2.2 Create the n-th blinder as linear combianation of the previous ones (the reason will be clear in the next paragraph):

$$r_{n-1} = -(2^{n-1})^{-1} \sum_{i=0}^{n-2} r_i 2^i \in \mathbb{Z}_p \tag{6}$$

$$s_{n-1} = -(2^{n-1})^{-1} \sum_{i=0}^{n-2} s_i 2^i \in \mathbb{Z}_q$$

Note that

$$\begin{aligned}
\sum_{i=0}^{n-1} r_i 2^i &= \sum_{i=0}^{n-2} r_i 2^i + r_{n-1} 2^{n-1} \\
&= \sum_{i=0}^{n-2} r_i 2^i + (-(2^{n-1})^{-1} \sum_{i=0}^{n-2} r_i 2^i) 2^{n-1} \\
&= \sum_{i=0}^{n-2} r_i 2^i - (2^{n-1})^{-1} (2^{n-1}) (\sum_{i=0}^{n-2} r_i 2^i) \\
&= 0 \in \mathbb{Z}_p
\end{aligned} \tag{7}$$

and that the same works for $s_{n-1}, \dots, s_0$.

Step 2.3 For each $i \in 0, \dots, n-1$ Peggy creates two Pedersen Commitments:

$$C_i^{\mathbb{G}} := b_i G' + r_i G \in \mathbb{G} \tag{8}$$

$$C_i^{\mathbb{H}} := b_i G' + s_i G \in \mathbb{H}$$

Note that $\forall i \in 0, \dots, n-1$

$$\begin{aligned}
\sum_{i=0}^{n-1} 2^i C_i^{\mathbb{H}} &= \sum_{i=0}^{n-1} 2^i b_i G' + \sum_{i=0}^{n-1} 2^i r_i G \\
&= (\sum_{i=0}^{n-1} 2^i b_i) G' + (\sum_{i=0}^{n-1} 2^i r_i) G \\
&= x G' + 0 G = x G'
\end{aligned} \tag{9}$$

where xG' follows from Equation 4 and $0G$ is obtained from equality in Equation 7. Obviously the equality in Equation 9 holds for $C_i^{\mathbb{H}}$ and s_i too.

  The sets $C_i^{\mathbb{G}}{}_{i=0}^{n-1}$ and $C_i^{\mathbb{H}}{}_{i=0}^{n-1}$ are the Pedersen Commitments we mentioned at the beginning of this section.

Step 3

Signing in Abe et al. [1]

Signing in Noether [2]

3.5   Proof Verification

Verifying in Abe *et al.* [1]

Verifying in Noether [2]