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

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

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:

insert reference

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

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), `http://search.ieice.org/bin/summary.php?id=e87-a_1_131&category=D&year=2004&lang=E&abst=`
2. Noether, S.: Mrl-0010: Dirscrete logarithm equality across groups. Tech. rep., Monero Research Lab (2018)

Appendix I

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