A Report on Seraphis

coinstudent2048

September 9, 2021

Abstract

This document contains a concise description of Seraphis [1], a novel privacy-preserving transaction protocol abstraction, and a security analysis for it.

1 Preliminaries

1.1 Public Parameters and Notations

Let $\mathbb{G}$ be a cyclic group of prime order $l > 3$ in which the Discrete Logarithm assumption (DL) and the Decisional Diffie-Hellman assumption (DDH) holds, and let $\mathbb{F}$ be its scalar field. Let G_0, G_1, H_0, H_1 be generators of $\mathbb{G}$ with unknown DL relationship to each other. Note that these generators may be produced using public randomness. Let $\mathcal{H} : \{0,1\}^* \to \mathbb{F}$ be a cryptographic hash function. We add a subscript to $\mathcal{H}$, such as $\mathcal{H}_1$, in lieu of domain-separating the hash function explicitly; any domain-separation method may be used in practice.

The notation $\leftarrow_R$ will be used to denote for a randomly chosen element, and $(1/x)$ for the modular inverse of $x \in \mathbb{F}$. Lastly, we use additive notation for group operations.

1.2 E-notes and E-note images

Definition 1.1. *An* **e-note** *for scalars $k_a^o, k_b^o, a \in \mathbb{F}$ is a tuple (C, K^o, m) such that $C = xH_0 + aH_1$ for $x \leftarrow_R \mathbb{F}$, $K^o = k_b^o G_0 + k_a^o G_1$, and m is an arbitrary data.*

C is called the **Amount Commitment** for the amount a with blinding factor x, K^o is called the **One-time Address** for (one-time) private keys k_a^o and k_b^o (the o superscript indicates "one-time"), and m is the **Memo field**. We say that someone *owns* an e-note if they know the corresponding scalars $k_a^o, k_b^o, a \in \mathbb{F}$.

Definition 1.2. *An* **e-note image** *for an e-note (C, K^o, m) is a tuple $(C', K'^o, \tilde{K})$ such that*

$$\begin{aligned} C' &= t_c H_o + C \\ &= (t_c + x)H_0 + aH_1 \\ &= v_c H_o + aH_1 \ , \\ K'^o &= t_k G_0 + K^o \\ &= (t_k + k_b^o)G_0 + k_a^o G_1 \\ &= v_k G_0 + k_a^o G_1 \ , \ \textit{and} \\ \tilde{K} &= (1/k_a^o)G_0 \end{aligned}$$

for $t_c, t_k \leftarrow_R \mathbb{F}$ and independent to each other.

C' is called the **Masked Amount Commitment**, K'^o is called the **Masked Address**, and $\tilde{K}$ is called the **Linking Tag**.

Definition 1.3. *A* **receiver address** *is a tuple (K^{DH}, K^v, K^s) such that $K^{DH} \in \mathbb{G}$, $K^v = k^v K^{DH}$, and $K^s = k_b^s G_0 + k_a^s G_1$.*

K^{DH} is called the **Diffie-Hellman Base Public Key**, the v superscript indicates "view", and the s superscript indicates "spend". The reason for the name of K^{DH} will be clear in the next section, while the reason for the names of superscipts is outside the scope of this document. We say that someone *owns* a receiver address if they know the corresponding scalars $k^v, k_a^s, k_b^s \in \mathbb{F}$.

2 A Seraphis Transaction

Suppose that Alice owns a set of e-notes $\{(C_i, K_i^o, m_i)\}_{i=1}^n$.

References

[1] UkoeHB. Seraphis: Privacy-focused tx protocol. `https://github.com/UkoeHB/Seraphis`.