# CT Using Aggregate Range Proof

Shen Noether - MRL

October 20, 2015

**Abstract**

In this experimental note, I present a scheme for "confidential transactions" which equals the optimization given by the Borromean signatures. The idea is to use an aggregate schnorr signature. I must stress this is experimental and should be checked carefully!

**Definition 1.** Schnorr1 Signatures

**Generation** Let $(x, xG = P)$ be a secret / public key pair. Let $\alpha \leftarrow$ random and $L = \alpha G$ . Let $s = \alpha + xH(L)$. Output $(L, s)$

**Verification** Check if $sG = L + H(L)P$

**Definition 2.** Aggregate Schnorr1 Signatures

**Generation**: Given $(L_i, s_i)$ signed by $(x_i, x_i G = P_i)$ for $i = 1, ..., n$ compute $s = \sum s_i \ mod\ q$. Output $(L_1, ..., L_n, s)$

**Verification**: Check that $sG = \sum_i (L_i + H(L_i) P_i)$

**Definition 3.** Schnorr non-linkable ring signatures

**Generation** Let $(x, xG = P_1)$ and $P_2$ be two keys. Let $\alpha \leftarrow$random, $L_1 = \alpha G$, $s_2 \leftarrow$random, $L_2 = s_2 G + H(L_1) P_2$, $L_1 = s_1 G + H(L_2) P_1$ and then solve for $s_1$ , and shuffle the indices. Output $(L_1, s_1, s_2)$ (after an index shuffle).

**Verification** Compute $L_2 = s_2 G + H(L_1) P_2$, $L_1' = s_1 G + H(L_2) P_1$, and verify that $L_1 = L_1'$.

**Definition 4.** Aggregate schnorr non-linkable ring signatures

**Generation** Let $\left\{\left(x_1^j, P_1^j\right), P_2^j\right\}$ a set of keys for $j = 1, ..., n$ with signatures $\left(L_1^j, s_1^j, s_2^j\right)$ for all $j$. $s = \sum s_1$, output $\left(L_1^j, s_2^j\right)$ for all $i$ and $s$.

**Verification** Recompute $L_2^j$ for all $j$, and then compute $\sum L_1^j \stackrel{?}{=} sG + \sum H\left(L_2^j\right) P_1$

**Definition 5.** Borromean Confidential Transactions Range Proof algorithm

Let $C = \sum_{i=1}^{n} C_i$ be the decomposition of $C$, which is a commitment to some value, into the commitments to the binary decomposition of $C$. In other words, $C = \alpha G + bH$ and $b = b_0 2^0 + b_1 2^1 + ... + b_n 2^n$ so that $C_i = \alpha_i G + b_i 2^i H$. Now compute ring signatures on $\left\{C_i, C_i - 2^i H\right\}$ for all $i$, and combine these into one Borromean signature of size $2 \cdot n + 1$.

**Definition 6.** Confidential Transactions using Aggregate Range Proof Algorithm

Let $C = \sum_{i=1}^{n} C_i$ be the decomposition of $C$, which is a commitment to some value, into the commitments to the binary decomposition of $C$. In other words, $C = \alpha G + bH$ and $b = b_0 2^0 + b_1 2^1 + ... + b_n 2^n$ so that $C_i = \alpha_i G + b_i 2^i H$. Now use the aggregate schnorr algorithm to compute a signature of size $2 \cdot n + 1$.