Gmail

Hao Ren <renhao.szu@gmail.com>

（无主题）

Hao Ren <renhao.szu@gmail.com> 2017年10月16日 下午10:03
草稿

MRL’s paper is confusing, it’s better to read the source code.

There is a new output we want to make a “range proof”.

$$C = aG + 10H$$

10 is the amount, a is the secret key. G and H are different base point.

We split it in four, we get:

$$C_0 = a_0 G + 0 \times 1H$$

$$C_1 = a_1 G + 1 \times 2H$$

$$C_2 = a_2 G + 0 \times 4H$$

$$C_3 = a_3 G + 1 \times 8H$$

because $2 + 8 = 10$. a_i is random.

For the first line, we get $(C_0, C_0 - 1 \times 1H)$ these two points.

We know:

1. The first point’s secret key is a_0.
2. We can’t compute the second point’s secret key.
3. The difference between the tow points is $1H$.

We sign a ring signature on these two points, a ring contains only two points.

$$L_0 = \alpha G$$

α is random.

$$q_1 = H(L_0)$$

$H()$ is a hash function to covert a point to scalar.

$$L_1 = s_1 G + q_1 P_1$$

s_1 is random, P_1 is the second point.

$$q_0 = H(L_1)$$

$s_0 = \alpha - q_0 a_0$ since $L_0 = \alpha G = s_0 G + q_0 P_0 = (\alpha G - q_0 a_0) G + q_0 P_0$

It’s easy to verify this signature because:

$$L_0 + L_1 = (s_0 + s_1) G + (q_0 + q_1) H$$

The second line is similar but we should change the order of (P_0, P_1) because we only know the second point's secret key.

At last we make four range proof.

In practice, the code is a little different for space-saving.