Gmail

Hao Ren <renhao.szu@gmail.com>

（无主题）

Hao Ren <renhao.szu@gmail.com>
2017年11月21日 下午12:30
草稿

multisig

n~n

GIVEN: a account (p,P), 3 user (x_1,X_1), (x_2,X_2), (x_3,X_3). Where $X=(A,B)$ and $x=(a,b)$.

1. Compute $X'=X_1+X_2+X_3$ and $x'=x_1+x_2+x_3$, a' is shared to the 3 user.
2. Send P to (X'), the new account is $P'=H_s(rA')G+B'$, where r is a random scalar and R is published to all. This new account can be spent iff p', which is $p'=H_s(rA')+b'$ or $p'=H_s(a'R)+b'$.
3. Every user computes a partial key image $J_1=b_1H_p(P')$, J_2, J_3, the key image is $J=H_s(a'R)H_p(P')+J_1+J_2+J_3$.
4. Set P' the s-th account of P_N, such that $P'=P_s$.
5. Every user picks a random scalar u_1, u_2, u_3, compute $u=u_1+u_2+u_3$.
6. Randomly choose scalar s_i for $i\neq s$, compute:

$$L_s=uG,R_s=uH_p(P_s),c_{s+1}=H_s(m,L_s,R_s)$$

$$L_{s+1}=s_{s+1}G+c_{s+1}P_{s+1},R_{s+1}=s_{s+1}H_p(P_{s+1}),c_{s+2}=H_s(m,L_{s+1},R_{s+1})$$

…

$$L_{s-1},R_{s-1},c_s$$

1. Every user computes $s_{s,1}=u_1-c_sb_1$, $s_{s,2}$ and $s_{s,3}$, which are shared.
2. Compute $s_s=s_{s,1}+s_{s,2}+s_{s,3}-c_sH_s(a'R)=u-c_s(b'+H_s(a'R))$.

n-1~n

1. Compute x_1X_2,x_1X_3,x_2X_3…
2. Set $xx_1=H_s(x_1X_2)$…
3. Do same as before.