appendix1

1. The generation process of rK in MN-SC mechanism

The generation process of rK in MN-SC mechanism is as follows:

(1)Initialization stage

Distributor $KGC_C, NP_i = \{NP_1, NP_2, \ldots, NP_n\}$, master key is r_k. The distributor KGC_C randomly selects n points $K_1, K_2, \ldots, K_n$, on the elliptic curve $E_p(a, b)$, and makes its vertical coordinate $r_{k_1}, r_{k_2}, \ldots, r_{k_n}$ as the subkey of NP_i, G is the base point selected on $E_p(a, b)$. KGC_C distributes its subkeys to $NP_i, i \in [1, n]$ over a secure channel. KGC_C calculates $G_i' = k_i G, i \in [1, n]$. Then, parameters $(E, G, n, H(x), G^{'})$ is disclosed.

(2)Key distribution

a. Distributor KGC_C randomly selects a point Q on $E_p(a, b)$ and a $t-1$ degree polynomial $f(x) = a_0 + \sum_{i=1}^{t-1} a_i x^i$, where $f(0) = \mathsf{a}_0 = r_K$ and Q is the public parametlates and $f(x)$ is retained by the distributor.

b. Distributor KGC_C calculates $f(i) = r_{k_i}$, $A_l = a_l G$, $1 \leq l \leq t-1$, $D_i = (i, f(i)) - K_i Q$. The parameters A_l and D_i are disclosed.

c. Distributor KGC_C calculates $F_i = H(K_i Q)$, which is used to verify the authenticity of the subkeys interacted by the NP_i.

(3)Verification of subkeys

After receiving the subkey distributed by $KGC_C, NP_i (1 \leq i \leq n)$ first verifies the authenticity of the subkey. Then it calculates $C_i = K_i Q$ and $(i, r_{k_i}) = (D_i + C_i)$. If the equation $r_{k_i} G = \sum_{k=0}^{t-1} A_l i_i^l$ holds, then the subkey is true. If the equation $F_i = H(C_i)$ holds, it means that the identity between NP_i is true.

(4)Master key reconstruction:

When the number l of participants satisfies $l \geq t$, allow the participants be $NP_{i_1}, NP_{i_2}, \ldots NP_{i_l}$, and the master key r_K can be reconstructed by Lagrange interpolation. For the subkeys $r_{k_i}, i \in [1, t]$ of t different NP_i, a unique Lagrange interpolation polynomial $L(x) = \sum_{i=0}^{t-1} r_{k_i} l_i(x)$ can be constructed by (x_i, r_{k_i}), where $l_i(x) = \prod_{0 \leq j \leq t-1} \frac{x - x_i}{x_i - x_j}, 0 \leq i \leq t-1$. Because $L(x)$ is a polynomial of degree $t-1$ and corresponds to different values, there is $L(0)=f(0)=r_k$. Get the master key and send r_k to NP_1.