ZPN公链简介

密钥（sk）

256位随机对称密钥，在创建帐户时随机生成。

- Spending Key对Spend Authorization key（询问）：JubJub组标量字段的元素。通过在密钥（sk）后附加一个0字节，计算结果字节字符串上的Blake2b哈希值，并减少结果模数r（JubJub组的顺序）来生成。

授权密钥 （ak）

Nullifier密钥对：

- 证明授权密钥（nsk）：JubJub组标量字段的元素。通过在密钥（sk）后附加一个1字节，计算结果字节字符串上的Blake2b哈希值，并减少结果模数r（JubJub 组的顺序）来生成：

$$nsk = blake2b(sk \,||\, 1,\ personalization:\ "Money\ ",\ length:\ 512\ bits)$$

- Nullifier派生密钥（nk）：Jubjub曲线上的点。通过将证明授权密钥（nsk）乘以证明生成密钥生成器生成：

$$nk = nsk * PROOF\_GENERATION\_KEY\_GENERATOR$$