周报-向嘉豪 (2025 年 1 月 19 日)

1 Coding reading

On the last weekly, we had to read the paper and do some coding, we had figured out the SPHINCS+ all the compent, we will use the SPX to repalce the SPHINCS+, for the SPX, it have the three compent.

on the top level see, the SPX have the arithy length mssage msg for it inupt, then on the signer have it own sercurity key sk_{seed}, and public key pk_{seed}. So the auth message, it like $SPX_{sign} : (msg, sk_{seed}) \mapsto (pk_{root}, auth)$. then we will by the detial to saw the signature proposs.

first the msg to the hash function, i.e. which function can chose differen sercurity level, by the hash fucntion it will out put the one have value hm, $tree_{index}$, for the FORS sign and HT sign (muti XMSS tree) respectily.

then we have the n bytes lenght of the hm, this is the hash function output the fix value, for the specific verison SPX. So we will do the FORS singture, first spilt the $8 \times n$ bit hm dividel by the FORS tree height t, where the tree leaf node number is 2^t. here $t|(8 \times n)$. the $k \times t = (8 \times n)$, the k is the number of FORS tree. on the FORS leaf node is the random creat the sk by the sk_{seed} and other field. all the leaf node by the $sk_{1...k}$ by the hash function for the low height level node, then the k tree will split to compute the different root node. finally use the all the root node hash to the $FORS_{pk}$. on the FORS the $auth$, is the aside the node by the hm spilt to k index. we use the figure to show the FORS auth node and pulic node.