표 => 공격량, □ 이상 되어야 견딜수 있음.

128일때 공격이 '''이면 성공하지 못함

h = 차원

ie $N = 2^{14}$ ~~log Q~~ < 440

$N = 2^{15}$ log Q < 880

가끔 key change 에서 더 높은 q 필요한 경우는

다음 q 나 level 더 올려 key 잡는다.

* N이 작을수록 한다.

또는 bootstrap 횟수를 더 줄인다. ( N이 커지면 오래 걸리기 때문에, 표보고 잘 setting 한다 )

ternary 많이 씀. => bootstraping 쓰고 때문에

Cta max 고려해서 => table 참조

T 차이 => ( Encoding, / (depth. q) → bootstraping )

=> Key switchg 하면 $q = 2^x$ q를 더 올리게 되는데 (2배정도)

이를 고려해서 table을 참조해서 parameter를 잡는다.

=> 같은 skeme 이지만 시간차이나는 이유?

Msg Encoding, bootstraping depth 설정 최적화 등등

=> parameter 참조하다 안맞는 경우 log q 가 2배더 올려야

하는 상황이면, (bootstraping depth 줄이거나, security level 낮춘다)