5/9

- h = hint (0, -1) 개수

  p = 몇개다 내려갔다 하는 module 값

- $m = \lfloor \langle ct, sk \rangle_q \rfloor_t = [t]_q$

  $\Delta m + e$ 로 e 제거 감

↳ 줄이다보면 더이상 못줄임

($q_t \to q_{t-1}$ 한계가 있음)

BGV, BFV 는

$m = \lfloor [\langle ct, sk \rangle]_q \rfloor_t$

$[m + te]_t$

$= m$

e가 커지면 e를 줄이는 다

- $t = \langle ct, sk \rangle$ 인데 이것의 최대 범위를 ↳ New def

  ↳ (ct 내적 sk 한 값 = t = 정수) K_q 보다 작다

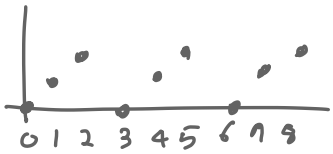
$\to \quad t \in (\mathbb{Z} \cap -K_q, K_q)$

$ct' \to \langle ct', sk \rangle \approx m$ 를 만족하는 ct' 를 찾고 싶다!

$\langle ct, sk \rangle = m$

- 우리는 +, × 만 할수 있다. $10 \bmod 3 = 1$ 하기 위해서는

mod 또는 나눗셈 해야 하는데 힘들어서 조금 손봐줄것!

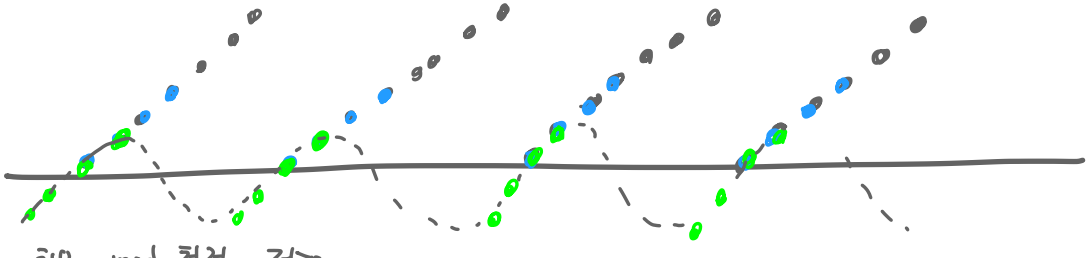


=> not continuous

↳ 이를 sin function 으로 표현

$t = \langle ct, sk \rangle = qI + m$ 으로 표현 (큰 q, msg) ↳ 이때 이거 쓰면 할수록 error가 작다.

그리고 $\sin F \to S(t) = \frac{q}{2\pi} \sin\left(\frac{2\pi t}{q}\right)$



0. 처음 mod 처럼 접근함
1. 이것을 전부 보는 게 아니라 일부 앞부분만 사용함
2. 범위를 $0 \sim q$ 이따금 $-\frac{q}{2} \sim \frac{q}{2}$ 로 가짐
3. 그 이후 sin 으로 근사할수 였고 error bound 가 보였다

$(s^2 \to as+b)$

$\times$ Mult → 곱함 → relinear → rescaling

sin 으로 근사했으니 Taylor polynomial 사용해서 근사 함

=> 0 근처에서는 잘 작동하지만 뒤에서는 error 커지고 복잡도 지수적 증가

=> 배각공식 써보자!

-> $\cos 2\theta =$

$\sin 2\theta =$

$e^{i\theta} = \cos\theta + i\sin\theta$

$e^{2i\theta} =$

점점 큰 영역에서 가능

$e^{i\theta}$ 에서 근사 -> $e^{2i\theta}$ 에서 -> $e^{4i\theta}$ -> $e^{8i\theta}$

$\theta < M$ $2\theta < 2M$ $4\theta < 4M$ 8θ ...

$2\sin\theta = e^{i\theta} - e^{-i\theta}$ 로 $\sin\theta$ 구하고, $\cos\theta$ 구하고 2θ 구함.

→ mod 연산 원한다

$\langle ct, sk \rangle \bmod q$ => sin 으로 근사해보자 => Taylor eval 별로

=> 2배각 공식을 써보자.

$P(r)$

$P_i(t) - E(t) = (\quad)$

└> 스털링 근사 $n! \sim \sqrt{2\pi n}(n/e)^n$ 사용해 E 바꿔보자

-> Taylor remain = f 실제값 − 몇번 expand f = ...

* △가 공간에 나오는데 sin 최대 1이니, 늘려주는 것

- Rotation / Conjugate → 동일

⇒ Taylor, 2θ, Post-E, Conju, ConCv Check

5/16

1. $q \to Q$로 올리기 $\quad m(x) = qI + m = \langle sk, ct \rangle_q$

$t(x) = \langle \ \rangle_Q \quad Q > q$

2. 계수를 slot에 넣기 ⇒ 곱셈인 enc 형태 2개로 만들기

OE

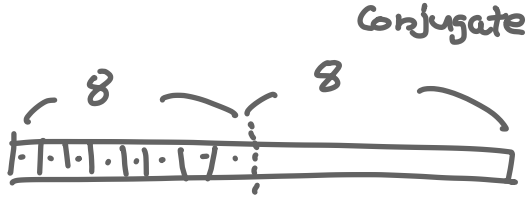
3. Evaluation of the complex exponential Func

4. imaginary part

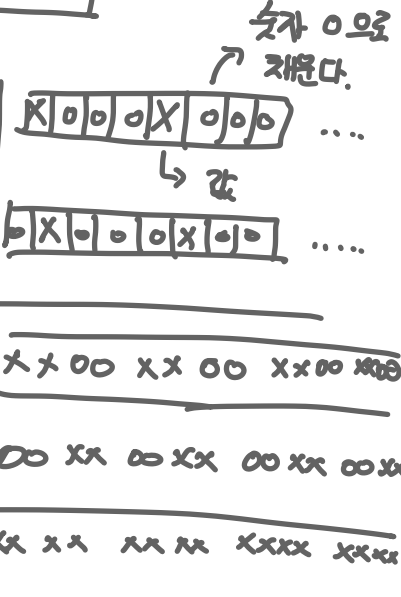
5 / 23

Recryption

If $N = 16$



↳ 8개 사용 안 해도 $N = 2$ 이면



* [fully packed ctx ⇒ 값 다들어 간것
Sparsely packed ctx ⇒ 값비어 있는것

↳ shift 하면서 채워 준다.

이렇게 값들로 채워진것을 Boot alg 에 넣는다.

* Encoding 법 여러가지가 있다

- $z_0\ z_1\ z_2\ z_3\ \bar{z}_0\ \bar{z}_1\ \bar{z}_2\ \bar{z}_3$
- $z_0\ \bar{z}_0\ z_1\ \bar{z}_1\ \cdots$
- $z_0\ z_1\ z_2\ z_3\ \bar{z}_3\ \bar{z}_2\ \bar{z}_1\ \bar{z}_0$
- ⋮