본문에서 S는 coefficient ring의 extension입니다. 정확히는 차수 d인 Z_q-algebra로, cyclic galois group $\langle\sigma\rangle$을 갖는 extension입니다. 그래서 연산은

$$R'_S = S[X,Y,W]/\langle X^n - i, Y^n - i, \Phi_p(W)$$

에서 이뤄집니다. 즉, 계수만 S로 올렸고, 다변수 구조와 GL에서 사용한 인코딩은 그대로 유지될 수 있습니다.

GTA에서는 outer trace $Tr_{Z_q}^S(\cdot) = \sum_{t=0}^{d-1} \sigma^t(\cdot)$을 정의하고(계수별로 적용), inner trace $Tr_Z(\cdot)$ 위에 composite으로 사용합니다.

$$GTA_d(a,b) = Tr_{Z_q}^S\left(Tr_Z\left(a(X,Z,W)\cdot b(Y^{-1},Z^{-1},W^{-1})\right)\right) \in R'$$

이 때 trace는 σ는 계수를 서로 permutation으로 정합시키는 작용입니다.

예를 들어 toy example로 길이 $n = 4$ (인덱스 $\nu = 0,1,2,3$)의 내적 $\sum_{\nu=0}^{3} a_\nu b_\nu$일 때

$d = 2$로 잡고 $\{0,2\}$ 와 $\{1,3\}$ 두 개의 residue class로 나눔

Inner trace Tr_Z는 각 class 안에서 부분합을 만든다고 할 때

$S_{even} = a_0b_0 + a_2b_2,\ S_{odd} = a_1b_1 + a_3b_3$

이 toy example에서 coefficient extension ring S는 $Z_q \times Z_q$이므로,

Permutation authomorphism σ는 두 성분을 맞바꾸는 action $\sigma(x_0,x_1) = (x_1,x_0)$. 이 때 outer trace는 단순히 두 성분의 합이 됩니다.

$$Tr_Z^S(x_0,x_1) = x_0 + x_1$$

직관적으로 보면 σ가 성분을 순환시키고, trace는 그 순환된 각 orbit의 합을 구하는 과정입니다.

숫자로 예를 들면 Z_{17}에서

$a = [2,5,7,3],\ b = [11,4,6,8]$이라 하면,

짝수 클래스의 합

$a_0b_0 = 2\cdot 11 = 22 = 5,\ a_2b_2 = 7\cdot 6 = 42 = 8,\ S_{even} = 5 + 8 = 13$

홀수 클래스의 합

$a_1 b_1 = 5 \cdot 4 = 20 = 3,\ a_3 b_3 = 3 \cdot 8 = 24 = 7,\ S_{odd} = 3 + 7 = 10$

Inner trace가 만들어낸 클래스별 부분합을 S의 한 원소

$$x = (S_{even}, S_{odd}) \in S$$

라면 $\sigma(x) = (S_{odd}, S_{even})$으로 두 성분을 맞바꾸므로 outer trace

$$Tr_Z^S(x) = S_{even} + S_{odd} = 13 + 10 = 23 = 6$$

한편 직접 내적하면

$$\sum_{v=0}^{3} a_v b_v = 22 + 20 + 42 + 24 = 23 = 6$$

실제로는 다변수 다항/행렬 형태이지만 위의 toy example과 논리는 같습니다.

다른 예제로

행/열 크기 $n = 2$ $(j, k \in \{0,1\})$, 합산축 parameter $v \in \{0,1\}$

두 행렬

$A = \begin{bmatrix} 2 & 5 \\ 7 & 3 \end{bmatrix},\ B = \begin{bmatrix} 11 & 4 \\ 6 & 8 \end{bmatrix}$

GL에서의 인코딩

$$a(X, Z) = \sum_{j=0}^{1} \sum_{v=0}^{1} A_{j,v} X^j Z^v = (2 + 5Z) + X(7 + 3Z)$$

$$b(Y, Z) = \sum_{k=0}^{1} \sum_{v=0}^{1} B_{k,v} Y^k Z^v = (11 + 4Z) + Y(6 + 8Z)$$

다항식 곱은

$$P(X, Y, Z) = a(X, Z) \cdot b(Y^{-1}, Z^{-1})$$

전개하면 $X^j Y^{-k} Z^{(v-\mu)}$꼴인데 여기서 v는 a의 Z의 인덱스, μ는 b의 Z인ㄷ게스

다항 트레이스 Tr_Z는 Z의 인덱스가 0이 되는 항만 모아 합친다는 개념 (정확히는 보조변수 Z에 대한 적절한 합산/projection이나...

그러면 $v = \mu$인 항만 남아서 (j, k)에 대해

$$[X^j Y^{-k}] Tr_Z\big(P(X, Y, Z)\big) = \sum_{v=0}^{1} A_{j,v} B_{k,v}$$

이건 아직은 행렬 내적. 계수로 얻는 행렬은

$$C_{j,k} = \sum_{\nu} A_{j,\nu} B_{k,\nu} = (AB^T)_{j,k}$$

요컨데 $Tr_Z\big(a(X,Y)b(Y^{-1},Z^{-1})\big)$의 (j,k) 계수는 A의 j번째 행과 B의 k번째 행의 내적임

수치로 보면

$(j,k) = (0,0)$: $2 \cdot 11 + 5 \cdot 4 = 22 + 20 = 42$

$(j,k) = (0,1)$: $2 \cdot 6 + 5 \cdot 8 = 12 + 40 = 52$

$(j,k) = (1,0)$: $7 \cdot 11 + 3 \cdot 4 = 77 + 12 = 89$

$(j,k) = (1,1)$: $7 \cdot 6 + 3 \cdot 8 = 42 + 24 = 66$

즉

$$Tr_Z(P) = 42 + Y^{-1} \cdot 52 + X \cdot 89 + XY^{-1} \cdot 66$$

이 다항의 계수 배열은

$$C = \begin{bmatrix} 42 & 52 \\ 89 & 66 \end{bmatrix} = AB^T$$

GTA는 여기에서v를 d개의 residue class로 나누는 것임 (여기서는 n=2이라서 잘 보이지는 않네요.)

안쪽 트레이스: 각 클레스 부분합

바깥 트레이스: 그 d개의 부분합을 한 번에 합친다. 원래의 길이 n인 내적을 구하는 R&A를 n/d로 단축

추가 example n=4

행 인덱스 $j \in \{0,1\}$, 열 인덱스 $k \in \{0,1\}$ 합산축 $v \in \{0,1,2,3\}$

$A = \begin{bmatrix} 2 & 5 & 7 & 3 \\ 1 & 4 & 6 & 8 \end{bmatrix}$, $b = \begin{bmatrix} 11 & 4 & 6 & 8 \\ 9 & 10 & 12 & 5 \end{bmatrix}$

다항 인코딩

$$a(X,Z) = \sum_{j=0}^{1} \sum_{v=0}^{3} A_{j,v} X^j Z^v = (2 + 5Z + 7Z^2 + 3Z^3) + X(1 + 4Z + 6Z^2 + 8Z^3)$$

$$b(Y,Z)=\sum_{k=0}^{1}\sum_{\nu=0}^{3}B_{k,\nu}Y^kZ^\nu=(11+4Z+6Z^2+8Z^3)+Y(9+10Z+12Z^2+5Z^3)$$

$P(X,Y,Z)=a(X,Z)b(Y^{-1},Z^{-1})$를 전개하면 각 항은 $X^jY^{-k}Z^{\nu-\mu}$꼴

여기서 $Tr_Z(P)$는 Z인덱스가 0 (즉 $\mu=\nu$)인 항만 모으므로 (j,k)의 계수는

$$C_{j,k}=\sum_{\nu=0}^{3}A_{j,\nu}B_{k,\nu}$$

즉 계수 영역 행렬곱 $C=AB^T$와 1:1 대응

수치로 계산하면

$$C_{0,0}=2\cdot11+5\cdot4+7\cdot6+3\cdot8=108$$

$$C_{0,1}=2\cdot9+5\cdot10+7\cdot12+3\cdot5=167$$

$$C_{1,0}=1\cdot11+4\cdot4+6\cdot6+8\cdot8=127$$

$$C_{1,1}=1\cdot9+4\cdot10+6\cdot12+8\cdot5=161$$

GTD(d=2) 클래스 부분합 바깥 트레이스 한 번

$C_{even}=\{0,2\},\ C_{odd}=\{1,3\}$

각각 (j,k)에 대해 안쪽 Tr_Z가 만드는 클래스 부분합

$S_{even}^{(j,k)}=\sum_{\nu\in\{0,2\}}A_{j,\nu}B_{k,\nu},\ S_{odd}^{(j,k)}=\sum_{\nu\in\{1,3\}}A_{j,\nu}B_{k,\nu}$

그 다음 계수학장 S의 한 원소로 $(S_{even}^{(j,k)},S_{odd}^{(j,k)})$를 담아 두고 바깥 계수 트레이스 $Tr_Z^S(x_0,x_1)=x_0+x_1$를 적용하면

$$Tr_Z^S\left(S_{even}^{(j,k)},S_{odd}^{(j,k)}\right)=S_{even}^{(j,k)}+S_{odd}^{(j,k)}=\sum_{\nu}^{3}A_{j,\nu}B_{k,\nu}=C_{j,k}$$

일반론에서 차수 d의 Z_q-대수이고 σ가 d-순환을 만드는 Galois action, $Tr_Z^S=\sum_{t=0}^{d-1}\sigma^t$

중요한 것은 **여기서 sigma는 Y축에서의 재인덱싱이므로 이론상 CT-CT곱은 0임**. 하지만 실제 구현에 따라 조금 연산이 들어갈 수도. (GL/GTA에서 비밀키 $s(X,W)$는 Y에는 의존하지 않음. Y축에서의 재배열은 계수의 위치만 바꾸는 순수 인덱스 재배열이라 키스위칭이 필요없음. 이 부분이 outer를 만들었을 때 연산 gain이 생기는 지점이라 보입니다.)

GL에서는 $\nu=0,1,2,3$을 모두 rotation and accumulation 하면 길이 4의 체인이 필요하나

GTA(d=2)의 경우 $\{v=0,2\}$, $\{v=1,3\}$ 두 그룹(Y축 reindexing)으로 각각 2개씩만 누산 한 뒤 outer trace로 한 번으로 두 부분 합을 합침.

실질적인 R&A의 길이가 4/2로 줄어들게 됨

GTA($d=4$)

$d=4$로 v를 $\{0\},\{1\},\{2\},\{3\}$ 네 클래스로 둠.

안쪽 Tr_Z가 각 클래스 단일 항을 그대로 부분합으로 두고

바깥 Tr_Z^S가 차수 $d=4$로 한 번에 4개를 합함

실제 $C_{j,k}$의 각 항 $(A_{j,v}B_{k,v})$ 자체가 네 클래스의 부분합, Tr_Z^S가 $v=0,1,2,3$ 항을 한 번에 더한 것과 같음.

GL에서 내적은 rotation & accumulation 으로 $v=0,\dots,n-1$의 길이지만

GTA는 v를 d개의 클래스로 나눠 Tr_Z가 클래스 부분합을 만들고, d개만 모아서 Tr_Z^S로 한 번에 더합니다.

위의 예에서 $n=4,\ d=2$라면 기존에는 4단계가 필요했다면 GTA는 짝/홀 2단계+바깥 트레이스 1회입니다. 여기서 gain은 마지막 합을 coefficient trace로 키스위치 없이 처리한다는 점입니다.

그래서 Z축을 n에서 n/d로 줄였다는 것 보다는 인덱스 $v\in\{0,1,\dots,n-1\}$를 d개의 residue classes로 나누어서 Tr_Z가 각 class의 부분합을 만들고 Tr_Z^S가 그 d개의 부분합을 한 번에 합친다고 볼 수 있습니다. 이 때 클래스 내부의 재배열은 Y-축 계수의 재인덱싱(이 때는 키 스위칭이 필요 없음)으로 처리되어, 결과적으로 rotation&accumulation체인의 길이가 약 1/d로 단축됩니다. 내적의 길이가 달라진 것이 아니라 합치는 단계를 묶어서 줄였다는 의미.

Fused relinearization은

GL에서는 큰 키 스위치 2번이 필요

Free는 multi target 방식으로 한 번에 처리

$$Switch_{big}((d_2, d_3), (\mu_1, \mu_2))$$

이는 키 스위칭의 bi-liniearity 때문

입력 $ct(b, a)$는 단순화한 scalar RLWE 모형에서 $b \equiv -as_{old} + m + e$ mod q

복호는 $b + s_{old}a = m + e$

키 스위치 a를 가젯 기저 g로 분해. $a = \sum_i d_i g^i$. 각 i마다 평가키 (u_i, v_i)를 s_{new}를 써서 준비

$u_i + s_{new}v_i = g^i s_{old} + e_i$ mod q

그러면 $g^i s_{old}$를 s_{new}로 암호화 한 것으로 볼 수 있음

그러면 $c_0' = b + \sum_i d_i u_i$, $c_1' = \sum_i d_i v_i$에 대해 새 키로 복호화하면

$$c_0' + s_{new}c_1' = b + \sum_i d_i(u_i + s_{new}v_i) \equiv b + \sum_i d_i\left(g^i s_{old} + e_i\right) \equiv (m + e) + \sum_i d_i e_i$$

Free는 두 타킷 μ_1, μ_2에 대해 위 평가키를 두 묶음으로 갖고(같은 s_{new}), 한 번의 decomposition으로 공유하면

$\sum_i d_i^{(2)}\left(u_i^{(1)} + s_{new}v_i^{(1)}\right) + \sum_i d_i^{(3)}\left(u_i^{(2)} + s_{new}v_i^{(2)}\right)$ 를 한 번에 accumulate합. 이는 두 번 따로 한 합과 동일. (키 스위치의 bilinearity 때문)

참고로 garget decomposition에서 기저 g에 대해

$$a = \sum_{j=0}^{d_g - 1} h_j(a)g^j \leftrightarrow\ h(a) = \left(h_0(a), \dots, h_{d_g - 1}(a)\right)^T$$

타깃 μ마다 길이 d_g로 묶음

$EK(\mu) = \left(U(\mu), V(\mu)\right)$ with $U(\mu) + s_{new}V(\mu) = \left(g^0\mu, \dots, g^{d_g - 1}\mu\right)$

성분별로 $U_j(\mu) + s_{new}V_j(\mu) \approx g^j\mu$

키 스위치

$$Switch(a,\mu) = (c_0, c_1) = (< h(a), U(\mu) >, < h(a), V(\mu) >)$$

가젯 벡터 $h(a)$와 평가키 벡터 $U(\mu)$, $V(\mu)$의 내적

복호는

$$c_0 + s_{new}c_1 =< h(a), U(\mu) + s_{new}V(\mu) >\approx< h(a), \left(g^0\mu, \dots, g^{d_g-1}\mu\right) >= \left(\sum_j h_j(a)g^j\right)\mu = a\mu$$

여기에서 복호 후 평문 레벨에서 키 스위치는 곱 $a\mu$를 계산한 꼴, 곱의 본질적인 bilinearity 때문에

$$Dec\big(Switch\ (a_1 + a_2, \mu)\big) = (a_1 + a_2)\mu = a_1\mu + a_2\mu = Dec\big(Switch\ (a_1, \mu) + Switch\ (a_2, \mu)\big)$$

$$Dec\big(Switch\ (a, \mu_1 + \mu_2)\big) = a(\mu_1 + \mu_2) = a\mu_1 + a\mu_2 = Dec\big(Switch\ (a, \mu_1) + Switch\ (a, \mu_2)\big)$$

이 성립

FREE는 두 타깃 μ_1, μ_2에 대해 두 평가키 벡터를 한 번에 곱해서 더함

두 입력 a_3, a_2가 있고 $EK(\mu_1)$, $EK(\mu_2)$가 준비되어 있으면

$$(c_0, c_1) = (< h(a_2), U(\mu_1) > +< h(a_3), U(\mu_2) >, < h(a_2), V(\mu_1) > +< h(a_3), V(\mu_2) >)$$

$$Dec\big((c_0, c_1)\big) =< h(a_2), U + sV >_{\mu_1} +< h(a_3), U + sV >_{\mu_2}\approx< h(a_2), g^j\mu_1 > +< h(a_3), g^j\mu_2 > = a_2\mu_1 + a_3\mu_2$$

그래서

$$Switch(a_2, \mu_1) + Switch(a_3, \mu_2) = Free\ ((a_2, a_3), (\mu_1, \mu_2))$$

곱하고 더한다는 성질만 보인다는 점에서 키 스위치를 $Switch(x, \mu) = x \cdot \mu \pmod{17}$이라고 합시다.

GL의 경우

$d_2 = 5,\ d_3 = 9,\ \mu_1 = 4,\ \mu = 7$

인 경우

$$Switch\ (d_2, \mu_1) = 5 \cdot 4 = 3\ mod\ 17$$

$$Switch(d_3, \mu_2) = 9 \cdot 7 = 12\ mod\ 17$$

합은 $3 + 12 = 15$

Free의 경우

$$Switch\big((d_2, d_3), (\mu_1, \mu_2)\big) = d_2\mu_1 + d_3 mu_2 = 15$$

s