

Lecture 11: Worked Examples

The BGV Scheme

SEC 595: Encrypted Computing

This companion works every example of Lecture 11 in full. Each example states what is given and what is asked, then proceeds in numbered steps. Example numbers match the handout.

Toolkit

T1. Centred reduction. $[x]_q$ is the representative of x in $(-q/2, q/2]$. With $q_1 = 97873$ the range is $(-48936.5, 48936.5]$; for example $[51750]_{q_1} = 51750 - 97873 = -46123$. Messages are read with $[x]_8 \in \{-3, \dots, 4\}$.

T2. Multiplying by X^k in $\mathbb{Z}[X]/(X^4 + 1)$. For $p = (p_0, p_1, p_2, p_3)$,

$$Xp = (-p_3, p_0, p_1, p_2), \quad X^2p = (-p_2, -p_3, p_0, p_1), \quad X^3p = (-p_1, -p_2, -p_3, p_0).$$

T3. Multiplying by a small polynomial. To form $p \cdot s$, write one row $s_k X^k p$ for each nonzero coefficient of s and add the columns. With $SK = 1 - X + X^3$ the rows are $p, -Xp, X^3p$; with $SK^2 = 3 - 2X + 2X^3$ they are $3p, -2Xp, 2X^3p$.

T4. BGV decryption in two reductions. Compute $c_0 + c_1 SK$ over $\mathbb{Z}$, reduce it centred modulo q_ℓ , then reduce modulo t . The noise is read off as $v = ([c_0 + c_1 SK]_{q_\ell} - M)/t$.

Tables list the coefficients of $X^0, \dots, X^3$ from left to right.

Example 1: One failure, in BGV and in BFV

Given. $t = 8$; BGV with prime $q = 1009$ and $M = 5$; BFV with $q = 1024$ and $m = 5$; noise $v = 30$ and $v = 70$.

Find. Both bounds and all four decryptions.

BGV.

Step 1. *Bound.* $q/(2t) = 1009/16 = 63.06$.

Step 2. $v = 30$: *form $M + tv$.* $5 + 8 \cdot 30 = 245$.

Step 3. *Reduce centred modulo 1009.* The range is $(-504.5, 504.5]$ and 245 is inside, so $[245]_{1009} = 245$.

Step 4. *Reduce modulo 8.* $245 = 30 \cdot 8 + 5$, so the result is 5. ✓

Step 5. $v = 70$: *form $M + tv$.* $5 + 560 = 565$.

Step 6. *Reduce centred.* $565 > 504.5$, so $[565]_{1009} = 565 - 1009 = -444$: one extra multiple of q is subtracted ($j = 1$).

Step 7. *Reduce modulo 8.* $-444 = -56 \cdot 8 + 4$, so the result is 4. $\times$

Step 8. *Explain the 4.* The output is $[M - jq]_8 = [5 - 1009]_8$. Since $1009 = 126 \cdot 8 + 1$, $[1009]_8 = 1$ and the output is $5 - 1 = 4$.

BFV.

Step 1. *Bound.* $\Delta = 1024/8 = 128$, $\Delta m = 640$, and $q/(2t) = 64$.

Step 2. $v = 30$. $\frac{8}{1024}(640 + 30) = 5.2344$, which rounds to 5. $\checkmark$

Step 3. $v = 70$. $\frac{8}{1024}(640 + 70) = 5.5469$, which rounds to 6. $\times$

What it shows. The thresholds agree to within one unit (63.06 against 64). BGV returns $5 - 1$, BFV returns $5 + 1$: mirror images, both valid plaintexts, both silent.

Example 2: Checking a chain

Given. $p_0 = 17$, $p_1 = 41$, $p_2 = 97$; $t = 8, 16, 2$.

Find. Which switches $q_2 \rightarrow q_1 \rightarrow q_0$ satisfy $p_i \equiv 1 \pmod{t}$.

Step 1. *The rule.* Switching from q_ℓ to $q_{\ell-1}$ divides by p_ℓ , and needs $p_\ell \equiv 1 \pmod{t}$ (Proposition 5). The bottom prime p_0 is never divided out, so it is not checked.

Step 2. $t = 8$. $41 = 5 \cdot 8 + 1$ and $97 = 12 \cdot 8 + 1$: both $\equiv 1$. Both switches are legal.

Step 3. $t = 16$. $97 = 6 \cdot 16 + 1 \equiv 1$, so $q_2 \rightarrow q_1$ is legal. $41 = 2 \cdot 16 + 9 \equiv 9$, so $q_1 \rightarrow q_0$ is not. The ladder stops at level 1.

Step 4. $t = 2$. $p \equiv 1 \pmod{2}$ means p is odd; every prime but 2 qualifies.

Example 3: Budgets and keys

Given. The instance of Section 8: $n = 4$, $t = 8$, $p_0 = 1009$, $p_1 = 97$, $q_1 = 97873$, $q_0 = 1009$, $\beta = 1$, $\text{SK} = 1 - X + X^3$, $e = 1 - X^2 + X^3$, $a = 42445 + 19772X + 51750X^2 + 85319X^3$.

Find. The budgets, the fresh bound, whether one multiplication fits, and PK with its identity.

Step 1. *Chain.* $q_1 = 1009 \cdot 97 = 97873$. Both primes are $\equiv 1 \pmod{8}$: $1009 = 126 \cdot 8 + 1$, $97 = 12 \cdot 8 + 1$.

Step 2. *Budgets.* Level 1: $q_1/(2t) = 97873/16 = 6117.06$. Level 0: $q_0/(2t) = 1009/16 = 63.06$.

Step 3. *Fresh noise.* $2n\beta + \beta = 2 \cdot 4 \cdot 1 + 1 = 9$.

Step 4. *One multiplication.* With $V = 9$, Proposition 3 gives $ntV(1 + V) = 4 \cdot 8 \cdot 9 \cdot 10 = 2880$. Compare: $2880 < 6117.06$ (fits at level 1) but $2880 > 63.06$ (does not fit at level 0). So multiply at level 1 and switch down before decrypting.

Step 5. Centre a . $51750 - 97873 = -46123$ and $85319 - 97873 = -12554$, so $a = 42445 + 19772X - 46123X^2 - 12554X^3$.

Step 6. a SK by T3:

	X^0	X^1	X^2	X^3
a	42445	19772	-46123	-12554
$-X \cdot a$	-12554	-42445	-19772	46123
$X^3 \cdot a$	-19772	46123	12554	42445
a SK over $\mathbb{Z}$	10119	23450	-53341	76014

Step 7. $PK_0 = [-(aSK + te)]_{q_1}$ with $te = 8 - 8X^2 + 8X^3$:

	X^0	X^1	X^2	X^3
a SK	10119	23450	-53341	76014
$+ te$	8	0	-8	8
$-(aSK + te)$	-10127	-23450	53349	-76022
$PK_0 = [\cdot]_{q_1}$	-10127	-23450	-44524	21851
in $[0, q_1)$	87746	74423	53349	21851

The last row is the handout's PK_0 ; $PK_1 = a$.

Step 8. Check (2).

	X^0	X^1	X^2	X^3
PK_0	-10127	-23450	-44524	21851
$+ a$ SK	10119	23450	-53341	76014
sum over $\mathbb{Z}$	-8	0	-97865	97865
$[\cdot]_{q_1}$	-8	0	8	-8
$-te$	-8	0	8	-8

$PK_0 + PK_1SK = -8 + 8X^2 - 8X^3 = -te$: small, and every coefficient a multiple of 8. ✓

Example 4: Encrypt and decrypt

Given. The keys of Example 3; $m_1 = 5$, $m_2 = 2$; the randomness

$$\begin{aligned} u^{(1)} &= 1 - X^2 + X^3, & e_1^{(1)} &= X - X^2, & e_2^{(1)} &= 1 - X, \\ u^{(2)} &= -1 + X + X^2, & e_1^{(2)} &= 1 - X^3, & e_2^{(2)} &= -X + X^2 + X^3. \end{aligned}$$

Find. Both ciphertexts, both decryptions and both noises.

Step 1. Encode in base 2: $M^{(1)} = 1 + X^2$ ($5 = (101)_2$), $M^{(2)} = X$ ($2 = (10)_2$). Unlike BFV, M is *not* scaled.

Step 2. $c_0^{(1)} = [PK_0 u^{(1)} + te_1^{(1)} + M^{(1)}]_{q_1}$, rows PK_0 , $-X^2PK_0$, X^3PK_0 :

	X^0	X^1	X^2	X^3
PK_0	-10127	-23450	-44524	21851
$-X^2 \cdot \text{PK}_0$	-44524	21851	10127	23450
$X^3 \cdot \text{PK}_0$	23450	44524	-21851	-10127
$\text{PK}_0 u^{(1)} \text{ over } \mathbb{Z}$	-31201	42925	-56248	35174
$+ t e_1^{(1)}$	0	8	-8	0
$+ M^{(1)}$	1	0	1	0
sum over $\mathbb{Z}$	-31200	42933	-56255	35174
$[\cdot]_{97873}$ (centred)	-31200	42933	41618	35174
in $[0, 97873)$	66673	42933	41618	35174

Step 3. $c_1^{(1)} = [\text{PK}_1 u^{(1)} + t e_2^{(1)}]_{q_1}$:

	X^0	X^1	X^2	X^3
PK_1	42445	19772	-46123	-12554
$-X^2 \cdot \text{PK}_1$	-46123	-12554	-42445	-19772
$X^3 \cdot \text{PK}_1$	-19772	46123	12554	42445
$\text{PK}_1 u^{(1)} \text{ over } \mathbb{Z}$	-23450	53341	-76014	10119
$+ t e_2^{(1)}$	8	-8	0	0
sum over $\mathbb{Z}$	-23442	53333	-76014	10119
$[\cdot]_{97873}$ (centred)	-23442	-44540	21859	10119
in $[0, 97873)$	74431	53333	21859	10119

Step 4. $c_0^{(2)}$, rows $-\text{PK}_0$, $X\text{PK}_0$, $X^2\text{PK}_0$:

	X^0	X^1	X^2	X^3
$-\text{PK}_0$	10127	23450	44524	-21851
$X \cdot \text{PK}_0$	-21851	-10127	-23450	-44524
$X^2 \cdot \text{PK}_0$	44524	-21851	-10127	-23450
$\text{PK}_0 u^{(2)} \text{ over } \mathbb{Z}$	32800	-8528	10947	-89825
$+ t e_1^{(2)}$	8	0	0	-8
$+ M^{(2)}$	0	1	0	0
sum over $\mathbb{Z}$	32808	-8527	10947	-89833
$[\cdot]_{97873}$ (centred)	32808	-8527	10947	8040
in $[0, 97873)$	32808	89346	10947	8040

Step 5. $c_1^{(2)}$:

	X^0	X^1	X^2	X^3
$-\text{PK}_1$	-42445	-19772	46123	12554
$X \cdot \text{PK}_1$	12554	42445	19772	-46123
$X^2 \cdot \text{PK}_1$	46123	12554	42445	19772
$\text{PK}_1 u^{(2)} \text{ over } \mathbb{Z}$	16232	35227	108340	-13797
$+ t e_2^{(2)}$	0	-8	8	8
sum over $\mathbb{Z}$	16232	35219	108348	-13789
$[\cdot]_{97873}$ (centred)	16232	35219	10475	-13789
in $[0, 97873)$	16232	35219	10475	84084

The rows “in $[0, q_1)$ ” are the handout’s table.

Step 6. *Decrypt* $\text{ct}^{(1)}$ by T4:

	X^0	X^1	X^2	X^3
c_1	-23442	-44540	21859	10119
$-X \cdot c_1$	10119	23442	44540	-21859
$X^3 \cdot c_1$	44540	-21859	-10119	-23442
$c_1\text{SK}$	31217	-42957	56280	-35182
$+c_0$	-31200	42933	41618	35174
sum over $\mathbb{Z}$	17	-24	97898	-8
$[\cdot]_{q_1}$	17	-24	25	-8
$[\cdot]_8$	1	0	1	0
$-M$	-1	0	-1	0
$\div t: v_1$	2	-3	3	-1

Step 7. Decrypt $\text{ct}^{(2)}$:

	X^0	X^1	X^2	X^3
c_1	16232	35219	10475	-13789
$-X \cdot c_1$	-13789	-16232	-35219	-10475
$X^3 \cdot c_1$	-35219	-10475	13789	16232
$c_1\text{SK}$	-32776	8512	-10955	-8032
$+c_0$	32808	-8527	10947	8040
sum over $\mathbb{Z}$	32	-15	-8	8
$[\cdot]_{q_1}$	32	-15	-8	8
$[\cdot]_8$	0	1	0	0
$-M$	0	-1	0	0
$\div t: v_2$	4	-2	-1	1

Step 8. Decode. $1 + X^2 \mapsto 5$ and $X \mapsto 2$. ✓

Step 9. Noise directly from $v = -eu + e_1 + e_2\text{SK}$:

	X^0	X^1	X^2	X^3
$-e u^{(1)}$	0	-2	3	-2
$+e_1^{(1)}$	0	1	-1	0
$+e_2^{(1)}\text{SK}$	2	-2	1	1
v_1	2	-3	3	-1

	X^0	X^1	X^2	X^3
$-e u^{(2)}$	1	0	-2	2
$+e_1^{(2)}$	1	0	0	-1
$+e_2^{(2)}\text{SK}$	2	-2	1	0
v_2	4	-2	-1	1

These match Steps 6 and 7, and they are the BFV noises of Lecture 10: v does not involve q , t or a .

What it shows. Every error carries the factor t , so the last reduction modulo 8 deletes the noise outright; no division or rounding is needed.

Example 5: Add and multiply

Given. $\text{ct}^{(1)}, \text{ct}^{(2)}$ of Example 4 (centred), v_1, v_2 .

Find. EvalAdd and EvalMult, their decryptions, and the three parts of the product noise.

Part A: EvalAdd

Step 1. *Add componentwise and reduce:*

	X^0	X^1	X^2	X^3
$c_0^{(1)}$	-31200	42933	41618	35174
$+ c_0^{(2)}$	32808	-8527	10947	8040
$c_0^{(3)} = [\cdot]_{q_1}$	1608	34406	-45308	43214
$c_1^{(1)}$	-23442	-44540	21859	10119
$+ c_1^{(2)}$	16232	35219	10475	-13789
$c_1^{(3)} = [\cdot]_{q_1}$	-7210	-9321	32334	-3670

Step 2. *Decrypt by T4:*

	X^0	X^1	X^2	X^3
c_1	-7210	-9321	32334	-3670
$-X \cdot c_1$	-3670	7210	9321	-32334
$X^3 \cdot c_1$	9321	-32334	3670	-7210
$c_1 \text{SK}$	-1559	-34445	45325	-43214
$+ c_0$	1608	34406	-45308	43214
sum over $\mathbb{Z}$	49	-39	17	0
$[\cdot]_{q_1}$	49	-39	17	0
$[\cdot]_8$	1	1	1	0
$-M$	-1	-1	-1	0
$\div t: v$	6	-5	2	0

Step 3. *Read off.* $M = 1+X+X^2$, decoding to $1+2+4 = 7$. ✓ The noise is $v_1+v_2 = 6-5X+2X^2$, with $\|v\| = 6 < \|v_1\| + \|v_2\| = 7$: coefficients partly cancel.

Part B: EvalMult

Step 1. *No rescaling.* BGV has no Δ , so EvalMult is the bare tensor product reduced modulo q_1 . Any representatives may be used: the result is reduced modulo q_1 anyway.

Step 2. *One coefficient by hand.* With $a = c_0^{(1)}$, $b = c_0^{(2)}$, the constant coefficient of ab is

$$\begin{aligned} a_0b_0 - a_1b_3 - a_2b_2 - a_3b_1 &= -1023609600 - 345181320 - 455592246 - (-299928698) \\ &= -1524454468. \end{aligned}$$

Step 3. *All three components:*

	X^0	X^1	X^2	X^3
$c_0^{(1)}c_0^{(2)}$ over $\mathbb{Z}$	-1524454468	954929766	374968293	1018251457
$c_0^* = [\cdot]_{q_1}$	15380	-17095	16830	-19235
$c_0^{(1)}c_1^{(2)} + c_1^{(1)}c_0^{(2)}$	-2153166215	-1744418831	3104761307	2386168084
$c_1^* = [\cdot]_{q_1}$	39785	-28352	34001	24344
$c_1^{(1)}c_1^{(2)}$ over $\mathbb{Z}$	-1580026690	-1353159852	-1319863031	790788967
$c_2^* = [\cdot]_{q_1}$	35022	32246	-45626	-24873
c_0^* in $[0, q_1)$	15380	80778	16830	78638
c_1^* in $[0, q_1)$	39785	69521	34001	24344
c_2^* in $[0, q_1)$	35022	32246	52247	73000

The $[0, q_1)$ rows are the handout's c_0^*, c_1^*, c_2^* .

Step 4. *Decrypt* with SK and $SK^2 = 3 - 2X + 2X^3$, forming c_1^*SK and $c_2^*SK^2$ by T3:

	X^0	X^1	X^2	X^3
c_0^*	15380	-17095	16830	-19235
c_1^*SK	92481	-102138	38009	30128
$c_2^*SK^2$	-9172	117946	-151624	86677
sum over $\mathbb{Z}$	98689	-1287	-96785	97570
$[\cdot]_{q_1}$	816	-1287	1088	-303
$[\cdot]_8$	0	1	0	1
$-M^{(3)}$	0	-1	0	-1
$\div t: v_3$	102	-161	136	-38

Step 5. *Decode.* $M^{(3)} = X + X^3 \mapsto 2 + 8 = 10 = 5 \times 2$. $\checkmark$ $\|v_3\| = 161$.

Step 6. *The product v_1v_2 by T3 (rows $2v_2, -3Xv_2, 3X^2v_2, -X^3v_2$):*

	X^0	X^1	X^2	X^3
$2 \cdot v_2$	8	-4	-2	2
$-3X \cdot v_2$	3	-12	6	3
$3X^2 \cdot v_2$	3	-3	12	-6
$-X^3 \cdot v_2$	-2	-1	1	-4
$v_2 v_1$ over $\mathbb{Z}$	12	-20	17	-5

Step 7. *Split v_3 by Proposition 3:*

	X^0	X^1	X^2	X^3
$M^{(1)}v_2$	5	-3	3	-1
$M^{(2)}v_1$	1	2	-3	3
$t v_1 v_2$	96	-160	136	-40
sum = v_3	102	-161	136	-38

The two linear parts contribute at most 5; the quadratic part $t v_1 v_2$ contributes 160.

Step 8. *Compare with the bound.* With $V = 4$: $ntV(1 + V) = 4 \cdot 8 \cdot 4 \cdot 5 = 640 \geq 161$. $\checkmark$

What it shows. The noise jumped from 4 to 161, almost all of it from $t v_1 v_2$: BGV noise growth is quadratic in the noise.

Example 6: Relinearize

Given. ct^* of Example 5; base $w = 4$; nine evaluation keys $EK^{(i)} = ([-(a_i SK + t e_i) + 4^i SK^2]_{q_1}, a_i)$ with fresh random a_i and $\|e_i\| \leq 1$.

Find. The number of keys, the noise bound, the digits of c_2^* , and the noise of the relinearized ciphertext.

Step 1. *Number of keys.* $4^8 = 65536 < 97873 \leq 262144 = 4^9$, so $\ell_w = \lceil \log_4 97873 \rceil = 9$.

Step 2. *Bound.* $n\ell_w(w - 1)\beta = 4 \cdot 9 \cdot 3 \cdot 1 = 108$.

Step 3. *Digits.* Write each coefficient of c_2^* in base 4, lowest digit first; for example $35022 = 2 + 3 \cdot 4 + 0 \cdot 4^2 + 3 \cdot 4^3 + 0 \cdot 4^4 + 2 \cdot 4^5 + 0 \cdot 4^6 + 2 \cdot 4^7 + 0 \cdot 4^8$:

	X^0	X^1	X^2	X^3
c_2^* in $[0, q_1)$	35022	32246	52247	73000
d_0	2	2	3	0
d_1	3	1	1	2
d_2	0	3	1	2
d_3	3	3	0	0
d_4	0	1	0	1
d_5	2	3	3	3
d_6	0	3	0	1
d_7	2	1	3	0
d_8	0	0	0	1
$\sum_i 4^i d_i$	35022	32246	52247	73000

Step 4. *Combine.* $\hat{c}_0 = [c_0^* + \sum_i d_i \text{EK}_0^{(i)}]_{q_1}$ and $\hat{c}_1 = [c_1^* + \sum_i d_i \text{EK}_1^{(i)}]_{q_1}$. Since $\text{EK}_0^{(i)} + \text{EK}_1^{(i)} \text{SK} = 4^i \text{SK}^2 - t e_i$ and $\sum_i 4^i d_i = c_2^*$,

$$\hat{c}_0 + \hat{c}_1 \text{SK} = c_0^* + c_1^* \text{SK} + c_2^* \text{SK}^2 - t \sum_i d_i e_i.$$

The added noise is $-\sum_i d_i e_i$, at most $n \cdot 9 \cdot 3 \cdot 1 = 108$. The keys a_i, e_i are random and are not printed, so the next step checks the result instead of rebuilding it.

Step 5. *Decrypt the result* $\hat{c}_0 = 2831 + 18002X + 61140X^2 + 85983X^3$, $\hat{c}_1 = 32787 + 81132X + 67514X^2 + 46330X^3$, centred:

	X^0	X^1	X^2	X^3
c_1	32787	-16741	-30359	46330
$-X \cdot c_1$	46330	-32787	16741	30359
$X^3 \cdot c_1$	16741	30359	-46330	32787
$c_1 \text{SK}$	95858	-19169	-59948	109476
$+ c_0$	2831	18002	-36733	-11890
sum over $\mathbb{Z}$	98689	-1167	-96681	97586
$[\cdot]_{q_1}$	816	-1167	1192	-287
$[\cdot]_8$	0	1	0	1
$-M$	0	-1	0	-1
$\div t: v$	102	-146	149	-36

Step 6. *Increment.* $v - v_3 = 15X + 13X^2 + 2X^3$, so $\|v - v_3\| = 15 \leq 108$. ✓ Decryption still returns $X + X^3 = 10$.

What it shows. The key errors carry t like every other error, so relinearization only adds a small term to v ; base decomposition keeps it of order w .

Example 7: One modulus switch

Given. $\hat{c}t$ of Example 6 at level 1; switch to $q_0 = 1009$ by dropping $p_1 = 97$.

Find. $\hat{c}t'$, its decryption, and its noise against the bound.

Step 1. *Centre the input* (T1): $\hat{c}_0 = 2831 + 18002X - 36733X^2 - 11890X^3$, $\hat{c}_1 = 32787 - 16741X - 30359X^2 + 46330X^3$.

Step 2. *The rule.* For each coefficient c : compute $c/97$ (that is, $(q_0/q_1)c$), then pick the integer congruent to c modulo 8 that is nearest to $c/97$. The two candidates are the multiples-of-8 shifts of $c \bmod 8$ just below and just above $c/97$.

Step 3. *Apply it* (first four rows $\hat{c}_0$, last four $\hat{c}_1$):

c	$c \bmod 8$	$c/97$	nearest	candidates $\equiv c$	c'
2831	7	29.186	29	23, 31	31
18002	2	185.588	186	178, 186	186
-36733	3	-378.691	-379	-381, -373	-381
-11890	6	-122.577	-123	-130, -122	-122
32787	3	338.010	338	331, 339	339
-16741	3	-172.588	-173	-173, -165	-173
-30359	1	-312.979	-313	-319, -311	-311
46330	2	477.629	478	474, 482	474

In most rows the choice differs from plain rounding. For -36733: plain rounding gives $-379 \equiv 5$, but residue 3 is needed; the candidates are -381 and -373, and -381 is nearer to -378.691. The move is never more than $t/2 = 4$.

Step 4. *Read modulo q_0 .* In $[0, 1009)$: $c'_0 = 31 + 186X + 628X^2 + 887X^3$, $c'_1 = 339 + 836X + 698X^2 + 474X^3$ (the handout's form).

Step 5. *Decrypt at level 0* by T4 with q_0 :

	X^0	X^1	X^2	X^3
c_1	339	-173	-311	474
$-X \cdot c_1$	474	-339	173	311
$X^3 \cdot c_1$	173	311	-474	339
$c_1 \text{SK}$	986	-201	-612	1124
$+ c_0$	31	186	-381	-122
sum over $\mathbb{Z}$	1017	-15	-993	1002
$[\cdot]_{q_0}$	8	-15	16	-7
$[\cdot]_8$	0	1	0	1
$-M$	0	-1	0	-1
$\div t: v'$	1	-2	2	-1

Step 6. *Read off.* $M = X + X^3 \mapsto 10$. ✓ The noise fell from 149 to $\|v'\| = 2$.

Step 7. *Bound (4).* $\frac{q_0}{q_1}\|v\| + \frac{1}{2}(1 + n\|\text{SK}\|) + \frac{\|M\|}{t} = \frac{149}{97} + \frac{5}{2} + \frac{1}{8} = 4.16 \geq 2$. ✓

Step 8. *Why switch.* $149 > 63.06$: decrypting $\hat{c}_t$ at level 0 without switching would fail. After the switch, $2 < 63.06$.

What it shows. Dividing by $p_1 \equiv 1 \pmod{8}$ leaves M unchanged modulo 8 while the noise shrinks by about 97.