

Lecture 10: Worked Examples

The BFV Scheme

SEC 595: Encrypted Computing

Example 5: The instance

Given. $n = 4$, $t = 4$, $q = 2^{14} = 16384$, $\beta = 1$,

$$\text{SK} = 1 - X + X^3, \quad e = 1 - X^2 + X^3, \quad a = 7561 + 3002X + 15115X^2 + 8443X^3,$$

the messages $m_1 = 5$, $m_2 = 2$, and the encryption 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. The parameters, the public key, both ciphertexts, both decryptions and both noises.

Part A: Parameters

Step 1. *Scaling.* $\Delta = 16384/4 = 4096$; $t \mid q$, so $[q]_t = 0$.

Step 2. *Budget.* $q/(2t) = 16384/8 = 2048$.

Step 3. *Fresh noise.* $2n\beta + \beta = 8 + 1 = 9$.

Step 4. *Growth factor.* $G = 2tn^2\|\text{SK}\| = 2 \cdot 4 \cdot 16 \cdot 1 = 128$.

Step 5. *Depth.* After one multiplication the bound is $9 \cdot 128 = 1152 < 2048 \checkmark$; with the relinearization bound 112 of Example 7, $1264 < 2048 \checkmark$. After two, $1152 \cdot 128 = 147456 > 2048 \times$. One level is guaranteed.

Part B: Public key

Work with the centered form of a : $15115 - 16384 = -1269$ and $8443 - 16384 = -7941$, so $a = (7561, 3002, -1269, -7941)$.

Step 1. $a\text{SK}$ by $T\mathcal{3}$, rows a , $-Xa$, X^3a :

	X^0	X^1	X^2	X^3
a	7561	3002	-1269	-7941
$-X \cdot a$	-7941	-7561	-3002	1269
$X^3 \cdot a$	-3002	1269	7941	7561
$a\text{SK over } \mathbb{Z}$	-3382	-3290	3670	889

Step 2. Add e , negate, reduce:

	X^0	X^1	X^2	X^3
$a \text{ SK}$	-3382	-3290	3670	889
$+ e$	1	0	-1	1
$-(a\text{SK} + e)$	3381	3290	-3669	-890
$\text{PK}_0 = [\cdot]_q$	3381	3290	-3669	-890
in $[0, q)$	3381	3290	12715	15494

The handout prints the last row: $\text{PK}_0 = 3381 + 3290X + 12715X^2 + 15494X^3$, and $\text{PK}_1 = a$.

Step 3. Check the key identity (1).

	X^0	X^1	X^2	X^3
PK_0	3381	3290	-3669	-890
$+ a\text{SK}$	-3382	-3290	3670	889
sum over $\mathbb{Z}$	-1	0	1	-1
$[\cdot]_q$	-1	0	1	-1
$-e$	-1	0	1	-1

$$\text{PK}_0 + \text{PK}_1\text{SK} = -e. \checkmark$$

Part C: Encode and encrypt

Step 1. Encode in base 2: $5 = (101)_2$ gives $M^{(1)} = 1 + X^2$; $2 = (10)_2$ gives $M^{(2)} = X$. Then $\Delta M^{(1)} = 4096 + 4096X^2$ and $\Delta M^{(2)} = 4096X$.

Step 2. $c_0^{(1)} = [\text{PK}_0 u^{(1)} + e_1^{(1)} + \Delta M^{(1)}]_q$. With $u^{(1)} = 1 - X^2 + X^3$ the rows are PK_0 , $-X^2\text{PK}_0$, $X^3\text{PK}_0$:

	X^0	X^1	X^2	X^3
PK_0	3381	3290	-3669	-890
$-X^2 \cdot \text{PK}_0$	-3669	-890	-3381	-3290
$X^3 \cdot \text{PK}_0$	-3290	3669	890	3381
$\text{PK}_0 u^{(1)} \text{ over } \mathbb{Z}$	-3578	6069	-6160	-799
$+ e_1^{(1)}$	0	1	-1	0
$+ \Delta M^{(1)}$	4096	0	4096	0
sum over $\mathbb{Z}$	518	6070	-2065	-799
$[\cdot]_{16384} \text{ (centered)}$	518	6070	-2065	-799
in $[0, 16384)$	518	6070	14319	15585

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

	X^0	X^1	X^2	X^3
PK_1	7561	3002	-1269	-7941
$-X^2 \cdot \text{PK}_1$	-1269	-7941	-7561	-3002
$X^3 \cdot \text{PK}_1$	-3002	1269	7941	7561
$\text{PK}_1 u^{(1)} \text{ over } \mathbb{Z}$	3290	-3670	-889	-3382
$+ e_2^{(1)}$	1	-1	0	0
sum over $\mathbb{Z}$	3291	-3671	-889	-3382
$[\cdot]_{16384} \text{ (centered)}$	3291	-3671	-889	-3382
in $[0, 16384)$	3291	12713	15495	13002

Step 4. $c_0^{(2)}$, with $u^{(2)} = -1 + X + X^2$, rows $-\text{PK}_0, X\text{PK}_0, X^2\text{PK}_0$:

	X^0	X^1	X^2	X^3
$-\text{PK}_0$	-3381	-3290	3669	890
$X \cdot \text{PK}_0$	890	3381	3290	-3669
$X^2 \cdot \text{PK}_0$	3669	890	3381	3290
$\text{PK}_0 u^{(2)} \text{ over } \mathbb{Z}$	1178	981	10340	511
$+ e_1^{(2)}$	1	0	0	-1
$+ \Delta M^{(2)}$	0	4096	0	0
sum over $\mathbb{Z}$	1179	5077	10340	510
$[\cdot]_{16384}$ (centered)	1179	5077	-6044	510
in $[0, 16384)$	1179	5077	10340	510

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

	X^0	X^1	X^2	X^3
$-\text{PK}_1$	-7561	-3002	1269	7941
$X \cdot \text{PK}_1$	7941	7561	3002	-1269
$X^2 \cdot \text{PK}_1$	1269	7941	7561	3002
$\text{PK}_1 u^{(2)} \text{ over } \mathbb{Z}$	1649	12500	11832	9674
$+ e_2^{(2)}$	0	-1	1	1
sum over $\mathbb{Z}$	1649	12499	11833	9675
$[\cdot]_{16384}$ (centered)	1649	-3885	-4551	-6709
in $[0, 16384)$	1649	12499	11833	9675

The rows “in $[0, q)$ ” are the table of Example 5 in the handout.

Part D: Decrypt and read the noise

Step 1. *Decrypt* $\text{ct}^{(1)}$. Form $c_1\text{SK}$ by T3, add c_0 , reduce, scale by $t/q = 1/4096$, round, reduce modulo 4. The last two rows subtract ΔM to expose the noise:

	X^0	X^1	X^2	X^3
c_1	3291	-3671	-889	-3382
$-X \cdot c_1$	-3382	-3291	3671	889
$X^3 \cdot c_1$	3671	889	3382	3291
$c_1\text{SK}$	3580	-6073	6164	798
$+ c_0$	518	6070	-2065	-799
sum over $\mathbb{Z}$	4098	-3	4099	-1
$[\cdot]_q$	4098	-3	4099	-1
$\times t/q$	1.0005	-0.0007	1.0007	-0.0002
round	1	0	1	0
mod t	1	0	1	0
$-\Delta M^{(1)}$	-4096	0	-4096	0
v_1	2	-3	3	-1

Step 2. *Decrypt* $\text{ct}^{(2)}$ the same way:

	X^0	X^1	X^2	X^3
c_1	1649	-3885	-4551	-6709
$-X \cdot c_1$	-6709	-1649	3885	4551
$X^3 \cdot c_1$	3885	4551	6709	1649
$c_1 \text{SK}$	-1175	-983	6043	-509
$+c_0$	1179	5077	-6044	510
sum over $\mathbb{Z}$	4	4094	-1	1
$[\cdot]_q$	4	4094	-1	1
$\times t/q$	0.0010	0.9995	-0.0002	0.0002
round	0	1	0	0
mod t	0	1	0	0
$-\Delta M^{(2)}$	0	-4096	0	0
v_2	4	-2	-1	1

Step 3. *Decode.* $1 + X^2$ at $X = 2$ is 5; X at $X = 2$ is 2. ✓

Step 4. *Noise directly* from $v = -eu + e_1 + e_2 \text{SK}$ (Proposition 2):

	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

Both agree with Steps 1 and 2: $\|v_1\| = 3$, $\|v_2\| = 4$, both below the fresh bound 9 and the budget 2048.

What it shows. The mask $au\text{SK}$ is invisible in the final rows: only ΔM and a noise of size at most 4 remain.

Example 6: Add and multiply

Given. The ciphertexts and keys of Example 5 (centered coefficients).

Find. EvalAdd and EvalMult of $\text{ct}^{(1)}, \text{ct}^{(2)}$, their decryptions, and their noises.

Part A: EvalAdd

Step 1. *Add componentwise and reduce:*

	X^0	X^1	X^2	X^3
$c_0^{(1)}$	518	6070	-2065	-799
$+c_0^{(2)}$	1179	5077	-6044	510
$c_0^{(3)} = [\cdot]_q$	1697	-5237	-8109	-289
$c_1^{(1)}$	3291	-3671	-889	-3382
$+c_1^{(2)}$	1649	-3885	-4551	-6709
$c_1^{(3)} = [\cdot]_q$	4940	-7556	-5440	6293

Step 2. *Decrypt* as in Example 5, Part D:

	X^0	X^1	X^2	X^3
c_1	4940	-7556	-5440	6293
$-X \cdot c_1$	6293	-4940	7556	5440
$X^3 \cdot c_1$	7556	5440	-6293	4940
$c_1 \text{SK}$	18789	-7056	-4177	16673
$+ c_0$	1697	-5237	-8109	-289
sum over $\mathbb{Z}$	20486	-12293	-12286	16384
$[\cdot]_q$	4102	4091	4098	0
$\times t/q$	1.0015	0.9988	1.0005	0.0000
round	1	1	1	0
mod t	1	1	1	0
$-\Delta M^{(3)}$	-4096	-4096	-4096	0
v_3	6	-5	2	0

Step 3. *Decode.* $1 + X + X^2$ at $X = 2$ is $1 + 2 + 4 = 7 = 5 + 2$. ✓

Step 4. *Noise.* $v_1 + v_2 = (2 - 3X + 3X^2 - X^3) + (4 - 2X - X^2 + X^3) = 6 - 5X + 2X^2$, as in the last row. $\|v\| = 6 \leq \|v_1\| + \|v_2\| = 7$.

Part B: EvalMult

Step 1. *Lift.* Take the centered coefficients of Example 5 as integers. (Section 6.4: the tensor product is formed over $\mathbb{Z}$, not modulo q .)

Step 2. *Tensor over $\mathbb{Z}$.* The three components are the coefficients of S^0, S^1, S^2 in $(c_0^{(1)} + c_1^{(1)}S)(c_0^{(2)} + c_1^{(2)}S)$. Each is a product in $\mathbb{Z}[X]/(X^4 + 1)$. For example, the constant coefficient of $c_0^{(1)}c_0^{(2)}$ is

$$a_0b_0 - a_1b_3 - a_2b_2 - a_3b_1 = 610722 - 3095700 - (12480860) - (-4056523) = -10909315,$$

with $a = c_0^{(1)}$, $b = c_0^{(2)}$. The other coefficients follow the same pattern.

Step 3. *Scale by $t/q = 1/4096$ and round:*

	X^0	X^1	X^2	X^3
$c_0^{(1)}c_0^{(2)}$	-10909315	6010410	25659453	-47848926
$\times t/q$	-2663.407	1467.385	6264.515	-11681.867
round	-2663	1467	6265	-11682
$c_0^{(1)}c_1^{(2)} + c_1^{(1)}c_0^{(2)}$	46625479	-17100454	-72556826	-9029755
$\times t/q$	11383.174	-4174.916	-17714.069	-2204.530
round	11383	-4175	-17714	-2205
$c_1^{(1)}c_1^{(2)}$	-36386789	-40194797	-24871305	-7495751
$\times t/q$	-8883.493	-9813.183	-6072.096	-1830.017
round	-8883	-9813	-6072	-1830

Step 4. *Reduce modulo q :*

	X^0	X^1	X^2	X^3
c_0^*	-2663	1467	6265	4702
c_1^*	-5001	-4175	-1330	-2205
c_2^*	7501	6571	-6072	-1830
c_0^* in $[0, q)$	13721	1467	6265	4702
c_1^* in $[0, q)$	11383	12209	15054	14179
c_2^* in $[0, q)$	7501	6571	10312	14554

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

Step 5. SK^2 by T3:

	X^0	X^1	X^2	X^3
SK	1	-1	0	1
$-X \cdot SK$	1	-1	1	0
$X^3 \cdot SK$	1	0	-1	1
SK SK over $\mathbb{Z}$	3	-2	0	2

so $SK^2 = 3 - 2X + 2X^3$.

Step 6. c_1^*SK (rows $c_1^*, -Xc_1^*, X^3c_1^*$):

	X^0	X^1	X^2	X^3
c_1^*	-5001	-4175	-1330	-2205
$-X \cdot c_1^*$	-2205	5001	4175	1330
$X^3 \cdot c_1^*$	4175	1330	2205	-5001
c_1^*SK over $\mathbb{Z}$	-3031	2156	5050	-5876

Step 7. $c_2^*SK^2$ (rows $3c_2^*, -2Xc_2^*, 2X^3c_2^*$):

	X^0	X^1	X^2	X^3
$3 \cdot c_2^*$	22503	19713	-18216	-5490
$-2X \cdot c_2^*$	-3660	-15002	-13142	12144
$2X^3 \cdot c_2^*$	-13142	12144	3660	15002
$c_2^*SK^2$ over $\mathbb{Z}$	5701	16855	-27698	21656

Step 8. Decrypt $c_0^* + c_1^*SK + c_2^*SK^2$:

	X^0	X^1	X^2	X^3
c_0	-2663	1467	6265	4702
c_1SK	-3031	2156	5050	-5876
c_2SK^2	5701	16855	-27698	21656
sum over $\mathbb{Z}$	7	20478	-16383	20482
$[\cdot]_q$	7	4094	1	4098
$\times t/q$	0.0017	0.9995	0.0002	1.0005
round, mod t	0	1	0	1
$-\Delta M$	0	-4096	0	-4096
v_3	7	-2	1	2

Step 9. Decode. $M^{(3)} = X + X^3$ gives $2 + 8 = 10 = 5 \times 2$. ✓

Step 10. Compare with the bound. $\|v_3\| = 7$ against the worst case $\|v_2\| \cdot G = 4 \cdot 128 = 512$.

What it shows. Rounding after the t/q scaling removes one factor of Δ ; the noise grew from 4 to 7, far below the worst case.

Example 7: Relinearize, both ways

Given. ct^* of Example 6, $a' = 11923 + 604X + 9981X^2 + 14002X^3$, $e' = X - X^2$; for the gadget, $w = 4$.

Find. EK; the basic relinearization and why it fails; the gadget relinearization and its noise.

Part A: The evaluation key

Centered, $a' = -4461 + 604X - 6403X^2 - 2382X^3$.

Step 1. a' SK by T3:

	X^0	X^1	X^2	X^3
a'	-4461	604	-6403	-2382
$-X \cdot a'$	-2382	4461	-604	6403
$X^3 \cdot a'$	-604	6403	2382	-4461
a' SK over $\mathbb{Z}$	-7447	11468	-4625	-440

Step 2. $\text{EK}_0 = [-(a'\text{SK} + e') + \text{SK}^2]_q$:

	X^0	X^1	X^2	X^3
a' SK	-7447	11468	-4625	-440
$+ e'$	0	1	-1	0
$-(a'\text{SK} + e')$	7447	-11469	4626	440
$+ \text{SK}^2$	3	-2	0	2
$\text{EK}_0 = [\cdot]_q$	7450	4913	4626	442
in $[0, q)$	7450	4913	4626	442

Step 3. Check (5). $\text{EK}_0 + \text{EK}_1\text{SK} - \text{SK}^2$ reduces to $-X + X^2 = -e'$. ✓

Part B: Basic relinearization

Step 1. *Predicted noise.* By Proposition 7 the new noise is $[v_3 - c_2^*e']_q$. Compute c_2^*e' (rows Xc_2^* , $-X^2c_2^*$):

	X^0	X^1	X^2	X^3
$X \cdot c_2^*$	1830	7501	6571	-6072
$-X^2 \cdot c_2^*$	-6072	-1830	-7501	-6571
c_2^*e' over $\mathbb{Z}$	-4242	5671	-930	-12643

Step 2. *New noise and decryption:*

	X^0	X^1	X^2	X^3
v_3	7	-2	1	2
$-c_2^*e'$	4242	-5671	930	12643
new noise $[\cdot]_q$	4249	-5673	931	-3739
$\Delta M^{(3)} + v$, centered	4249	-1577	931	357
decrypts to	1	0	0	0

$\|v\| = 5673 > 2048$, and decryption returns 1 instead of $X + X^3$: the message is destroyed.

Step 3. *Why.* $\|c_2^*\| = 7501$, so the bound is $n\|c_2^*\|^\beta = 4 \cdot 7501 = 30004$, far above the budget.

Part C: Gadget relinearization, $w = 4$

Step 1. *Number of keys.* $\ell = \lceil \log_4 16384 \rceil = 7$, since $4^7 = 16384$.

Step 2. *Digits.* Write each coefficient of c_2^* (in $[0, q)$) in base 4, lowest digit first. For example $7501 = 1 + 3 \cdot 4 + 0 \cdot 16 + 1 \cdot 64 + 1 \cdot 256 + 3 \cdot 1024 + 1 \cdot 4096$. All four:

	X^0	X^1	X^2	X^3
c_2^* in $[0, q)$	7501	6571	10312	14554
d_0	1	3	0	2
d_1	3	2	2	2
d_2	0	2	0	1
d_3	1	2	1	3
d_4	1	1	0	0
d_5	3	2	2	2
d_6	1	1	2	3
$\sum_i 4^i d_i$	7501	6571	10312	14554
$D = \sum_i d_i$	10	13	7	13

Step 3. *Collapse the sum.* In this toy every key reuses a' and e' : $\text{EK}^{(i)} = ([-(a'\text{SK} + e') + 4^i \text{SK}^2]_q, a')$. (This is insecure; it only makes the arithmetic short.) Then, since $\sum_i 4^i d_i = c_2^*$,

$$\hat{c}_0 = c_0^* + c_2^* \text{SK}^2 - D(a'\text{SK} + e'), \quad \hat{c}_1 = c_1^* + D a'.$$

Step 4. $D a'$ by T3 with $D = 10 + 13X + 7X^2 + 13X^3$:

	X^0	X^1	X^2	X^3
$10 \cdot a'$	-44610	6040	-64030	-23820
$13X \cdot a'$	30966	-57993	7852	-83239
$7X^2 \cdot a'$	44821	16674	-31227	4228
$13X^3 \cdot a'$	-7852	83239	30966	-57993
$a' D$ over $\mathbb{Z}$	23325	47960	-56439	-160824

Step 5. *Assemble $\hat{c}_0$ and $\hat{c}_1$* ($c_2^* \text{SK}^2$ is from Example 6, $a'\text{SK} + e'$ from Part A):

	X^0	X^1	X^2	X^3
c_0^*	-2663	1467	6265	4702
$+ c_2^* \text{SK}^2$	5701	16855	-27698	21656
$- D(a'\text{SK} + e')$	185465	-81097	-56428	81066
$\hat{c}_0 = [\cdot]_q$	-8105	2761	4059	-7264
in $[0, q)$	8279	2761	4059	9120
c_1^*	-5001	-4175	-1330	-2205
$+ D a'$	23325	47960	-56439	-160824
$\hat{c}_1 = [\cdot]_q$	1940	-5367	7767	811
in $[0, q)$	1940	11017	7767	811

Step 6. *Decrypt $\hat{c}t$:*

	X^0	X^1	X^2	X^3
c_1	1940	-5367	7767	811
$-X \cdot c_1$	811	-1940	5367	-7767
$X^3 \cdot c_1$	5367	-7767	-811	1940
$c_1 \text{SK}$	8118	-15074	12323	-5016
$+c_0$	-8105	2761	4059	-7264
sum over $\mathbb{Z}$	13	-12313	16382	-12280
$[\cdot]_q$	13	4071	-2	4104
$\times t/q$	0.0032	0.9939	-0.0005	1.0020
round	0	1	0	1
mod t	0	1	0	1
$-\Delta M^{(3)}$	0	-4096	0	-4096
v	13	-25	-2	8

Step 7. *Noise from Proposition 8.* The added noise is $-\sum_i d_i e' = -De' = 6 - 23X - 3X^2 + 6X^3$, and $v_3 - De' = 13 - 25X - 2X^2 + 8X^3$, the last row. $\checkmark \|v\| = 25$, against the bound $\|v_3\| + n\ell w\beta = 7 + 4 \cdot 7 \cdot 4 = 119$.

What it shows. Decomposing c_2^* replaced a multiplier of size about $q/2$ by digits below 4: the added noise fell from thousands to 25.

Example 8: A second multiplication

Given. $\hat{\text{ct}}$ of Example 7 (encrypting $X + X^3$, i.e. 10) and $\text{ct}^{(2)}$ (encrypting X , i.e. 2).

Find. $\text{EvalMult}(\hat{\text{ct}}, \text{ct}^{(2)})$, its decryption and its decoding.

Step 1. *Tensor over $\mathbb{Z}$, scale, round, reduce* exactly as in Example 6, Part B:

	X^0	X^1	X^2	X^3
$\hat{c}_0 c_0^{(2)}$	50448019	-83867572	71494418	-87777747
$\times t/q$, round	12316	-20475	17455	-2143
$\hat{c}_0 c_1^{(2)} + \hat{c}_1 c_0^{(2)}$	43261004	34676382	-46111451	87880359
$\times t/q$, round	10562	8466	-11258	21455
$\hat{c}_1 c_1^{(2)}$	5690209	39412581	30270637	-17427699
$\times t/q$, round	1389	9622	7390	-4255
$c_0^{**} = [\cdot]_q$	-4068	-4091	1071	-2143
$c_1^{**} = [\cdot]_q$	-5822	-7918	5126	5071
$c_2^{**} = [\cdot]_q$	1389	-6762	7390	-4255

Step 2. *Decrypt* with SK and SK²:

	X^0	X^1	X^2	X^3
c_0	-4068	-4091	1071	-2143
$c_1 \text{SK}$	7167	-7222	7973	-5877
$c_2 \text{SK}^2$	9181	-37844	44204	-24767
sum over $\mathbb{Z}$	12280	-49157	53248	-32787
$[\cdot]_q$	-4104	-5	4096	-19
$\times t/q$	-1.0020	-0.0012	1.0000	-0.0046
round, mod t	3	0	1	0
$-\Delta M$	4096	0	-4096	0
v_4	-8	-5	0	-19

The rounded row is $-1, 0, 1, 0$, so the plaintext is $-1 + X^2 \equiv 3 + X^2 \pmod{4}$; the $-\Delta M$ row uses its centered form. The noise is $-8 - 5X - 19X^3$, of norm 19, far inside the budget 2048.

Step 3. *Check in R_4 .* $M^{(3)}M^{(2)} = (X + X^3) \cdot X = X^2 + X^4 = X^2 - 1 \equiv 3 + X^2 \pmod{4}$. BFV computed the product correctly.

Step 4. *Decode.* $(3 + X^2)(2) = 3 + 4 = 7$, but $5 \times 2 \times 2 = 20$.

Step 5. *Locate the failure.* $20 = (10100)_2$ needs X^4 , which $n = 4$ does not have (condition (b)). The wrap $X^4 = -1$ put $-1 \equiv 3$ in the constant term.

What it shows. Two independent failures: the noise budget and the plaintext geometry. Here the noise was fine and the encoding failed; neither announces itself.