Part. I

國立清華大學試卷

記分					
1	10	2	10		
3	10	4	10		
5	10	6	10		
7	10	8	10		
9	10	10	10		
11		12			
13		14			
15		16			
17		18			
19		20			
總分	100				

所系 資工 17

科目 Cryptography and Network Security

學號 10206 23172

姓名 張以詳

日期 DEC 21, 2015

1. (a) $1x^5+0x^4+0x^3+0x^2+0x^1+1x^0$

$= \underline{x^5+1}$

(b) $0x^4+0x^3+0x^2+1x^1+1x^0$

$= \underline{x+1}$ ✓

2. (a) $\begin{array}{|cccc} 0 & 1 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{array} \Rightarrow \underline{0101}$

(b) $\begin{array}{cccc||cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{array} \Rightarrow \underline{1000\ 0000}$ ✓

3. $P_m = x^2+x+1$

(a)

q	r_1	r_2	r	t_1	t_2	t
x	x^2+x+1	$x+1$	1	0	1	x
$x+1$	$x+1$	1	0	1	x	–
	1	0		(x)	–	

validation: $(x)(x+1) = x^2+x = 1$ ✓

$\underline{(x+1)^{-1} = x}$

(b)

q	r_1	r_2	r	t_1	t_2	t
$x+1$	x^2+x+1	x	1	0	1	$x+1$
x	x	1	0	1	$x+1$	$-$
	1	0		$x+1$	$-$	

validation: $(x+1)(x) = x^2+x = 1$ ✓

$(x)^{-1} = x+1$

4. (a)

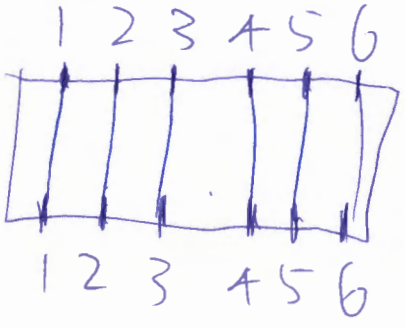


Figure: 6×6 P-box

$m \times n$ P-box:

(i) $m=n$: straight

(ii) $m>n$: compression

(iii) $m<n$: expansion

$m = 6 = n$, thus a straight P-box.

(b)

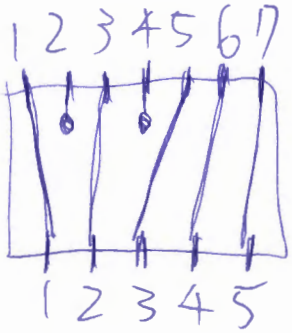
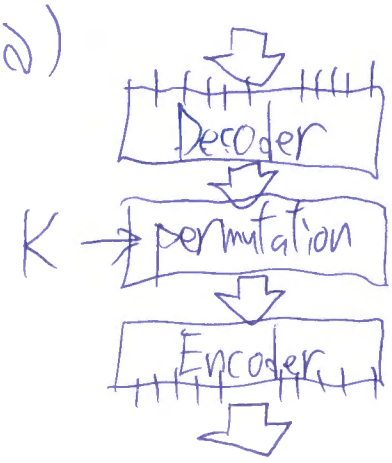


Figure: 7×5 P-box

$m = 7 > 5 = n$, thus a compression P-box.

5. (a)

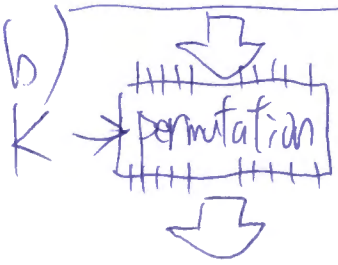


2^{10} possible input patterns

$\Rightarrow$ would need $\lceil \log_2((2^{10})!) \rceil$ bits to be able to fit any ID of the pattern.

The order: $(2^{10})!$

(b)



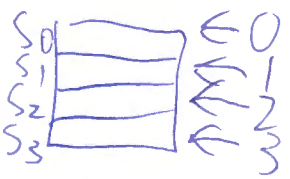
10! possible mappings

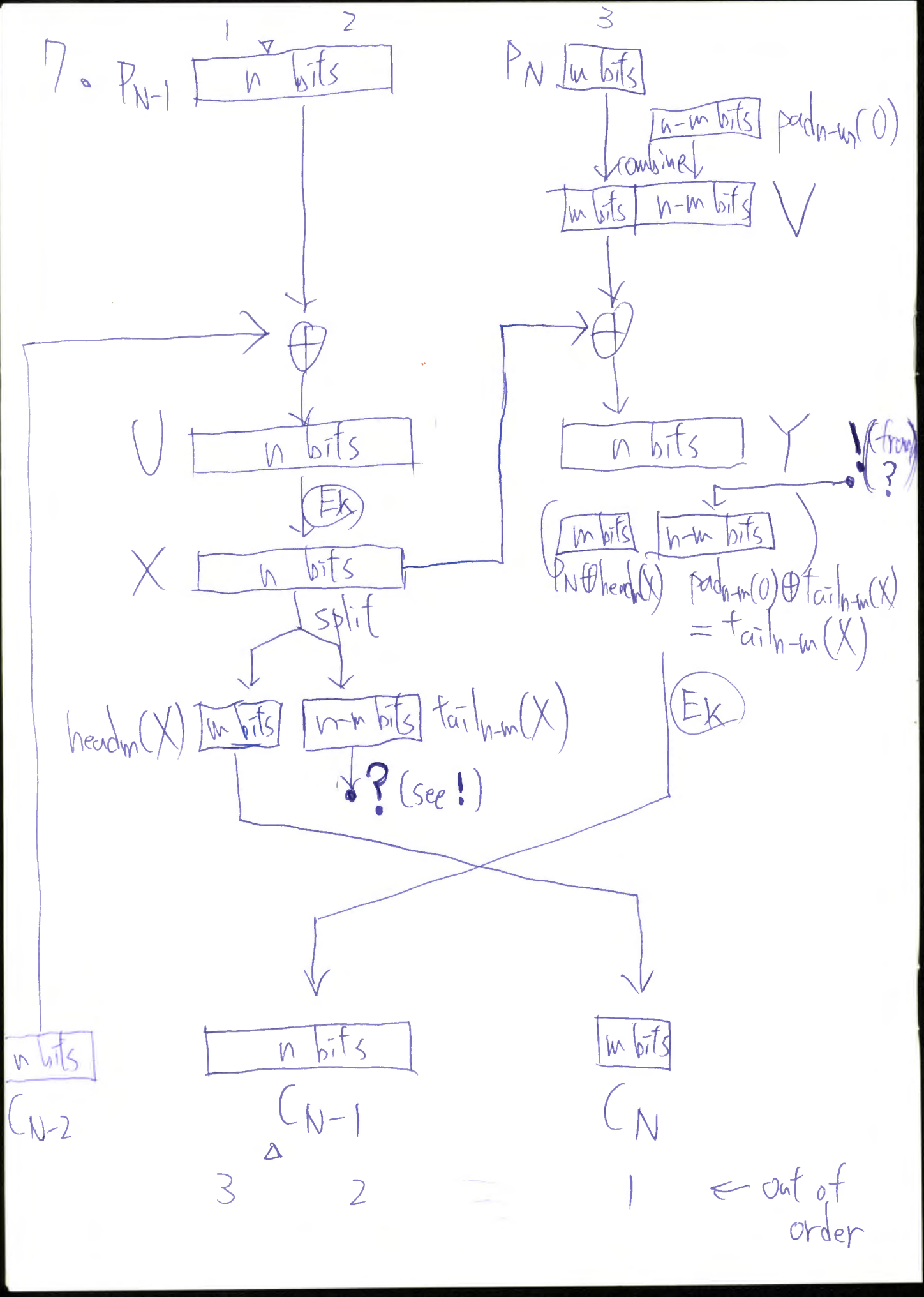
$\Rightarrow$ would need $\lceil \log_2(10!) \rceil$ bits to be able to fit any ID of the pattern

The order: 10!

6. (a) SubBytes $\rightarrow$ MixColumns $\rightarrow$ AddRoundKey

(b) ShiftRows




7.
P_{N-1}
1
2
n bits
P_N
3
m bits
n-m bits
$pad_{n-m}(0)$
combine
m bits
n-m bits
V
U
n bits
Ek
X
n bits
split
n bits
Y
(from ?)
m bits
n-m bits
$P_N \oplus head_m(X)$
$pad_{n-m}(0) \oplus tail_{n-m}(X)$
$= tail_{n-m}(X)$
$head_m(X)$
m bits
n-m bits
$tail_{n-m}(X)$
? (see !)
Ek
n bits
C_{N-2}
n bits
C_{N-1}
m bits
C_N
3
2
1
← out of order

$U = P_{N-1} \oplus C_{N-2}$

$V = P_N \mid pad_{n-m}(0)$

$X = E_k(U)$

$Y = X \oplus V$

$C_{N-1} = E_k(Y)$ ✓

$C_N = head_m(X)$

8.

$d_2 = S_5 \oplus S_3 \oplus S_1$

$d_1 = S_6 \oplus S_4 \oplus S_2$

Figure: 6x2 S-box

(i) $d_2 = 1 \oplus 0 \oplus 0 = 1$
$d_1 = 1 \oplus 1 \oplus 1 = 1$

(ii) $d_2 = 0 \oplus 0 \oplus 1 = 1$
$d_1 = 1 \oplus 1 \oplus 0 = 0$

If the input is 11 1010, the output is 11.

If the input is 10 1001, the output is 10.

Part. II

國立清華大學試卷

記					分
1		2			
3		4			
5		6			
7		8			
9		10			
11		12			
13		14			
15		16			
17		18			
19		20			
總 分					

所 系 資工 117

科 目 Cryptography and Network Security

學 號 10206 2372

姓 名 張以詩

日 期 DEC 21, 2015

9. q | r_1 | r_2 | r | t_1 | t_2 | t

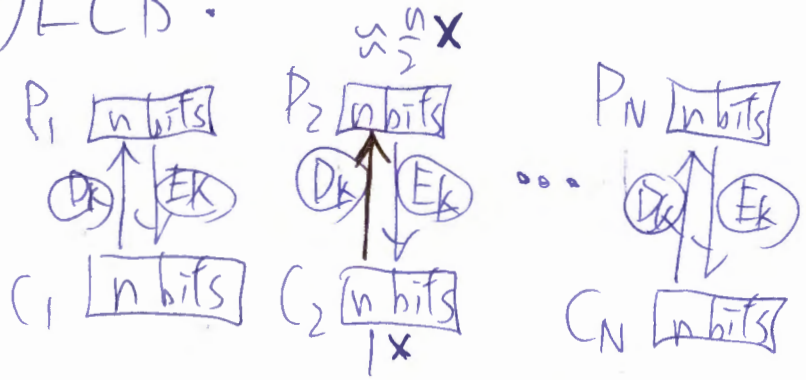
q	r_1	r_2	r	t_1	t_2	t
x	x^5+x^2+1	x^4+x^2+1	x^3+x^2+x+1	0	1	x
$x+1$	x^4+x^2+1	x^3+x^2+x+1	x^2	1	x	x^2+x+1
$x+1$	x^3+x^2+x+1	x^2	$x+1$	x	x^2+x+1	x^3+x+1
$x+1$	x^2	$x+1$	1	x^2+x+1	x^3+x+1	x^4+x^3+x
$x+1$	$x+1$	1	0	x^3+x+1	x^4+x^3+x	—
	1	0		x^4+x^3+x	—	

validation: $(x^4+x^3+x)(x^4+x^2+1)$

$= x^8+x^7+x^6+x^4+x$

$= 1$ ✓ $\quad (x^4+x^2+1)^{-1} = x^4+x^3+x$ ✓

10. (i) ECB:

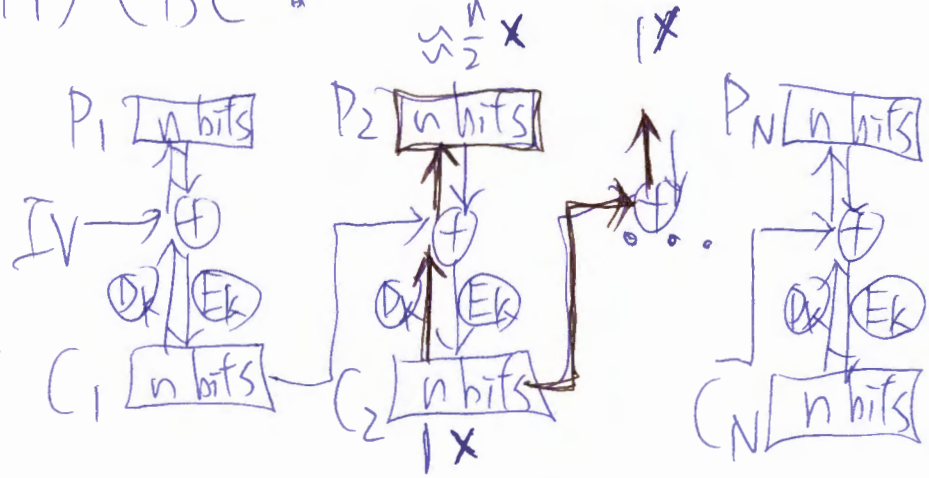


1 bit wrong in C_i

$\Rightarrow \approx \frac{n}{2}$ bits wrong in P_i,

other blocks are not affected. ✓

(ii) CBC:



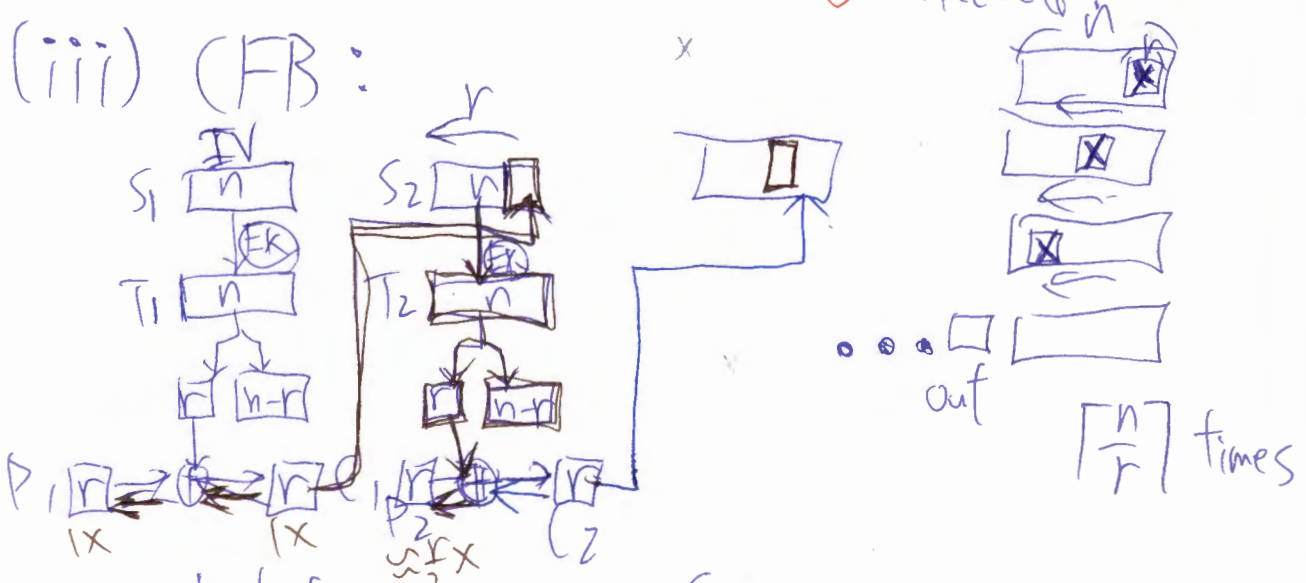
1 bit wrong in C_i

$\Rightarrow \approx \frac{n}{2}$ bits wrong in P_i,

1 bit wrong in P_{i+1},

other blocks are not affected.

(iii) CFB:



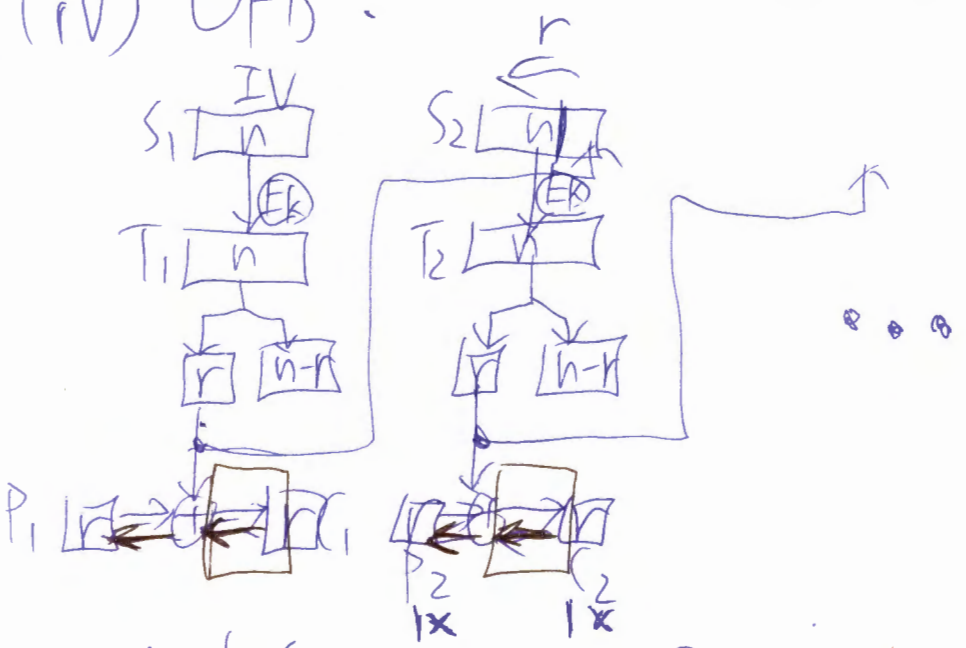
1 bit wrong in C_i

$\Rightarrow$ 1 bit wrong in P_i,

$\approx \frac{r}{2}$ bits wrong in P_{i+1} to $P_{i+\lceil \frac{n}{r} \rceil}$ (at most)

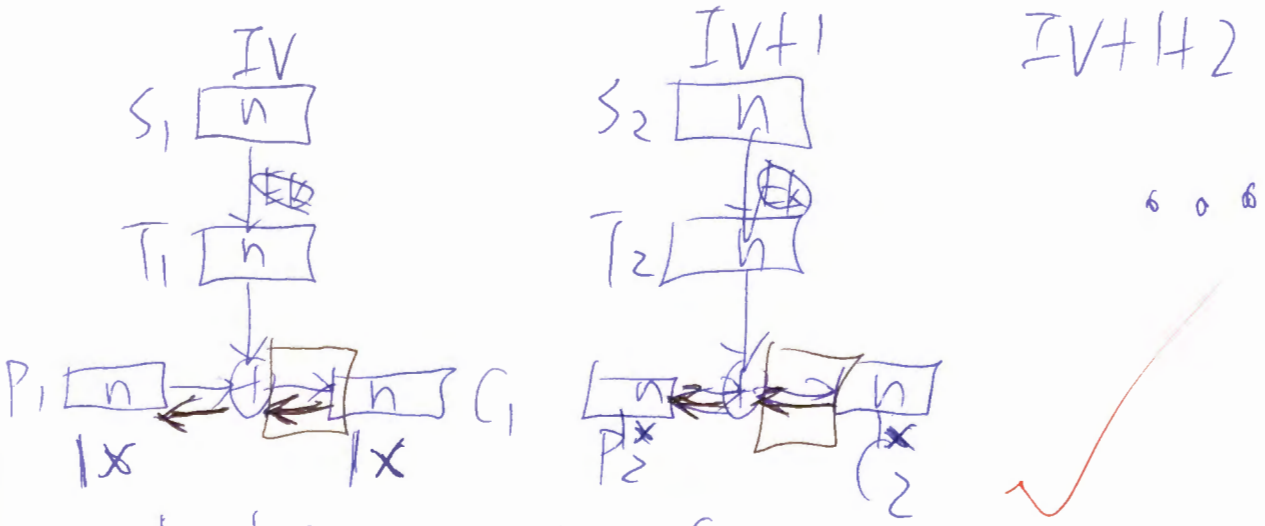
other blocks are not affected.

(iv) OFB:



1 bit wrong in C_i
$\Rightarrow$ 1 bit wrong in P_i ✓
other blocks are not affected.

(v) CTR:



1 bit wrong in C_i
$\Rightarrow$ 1 bit wrong in P_i ✓
other blocks are not affected.