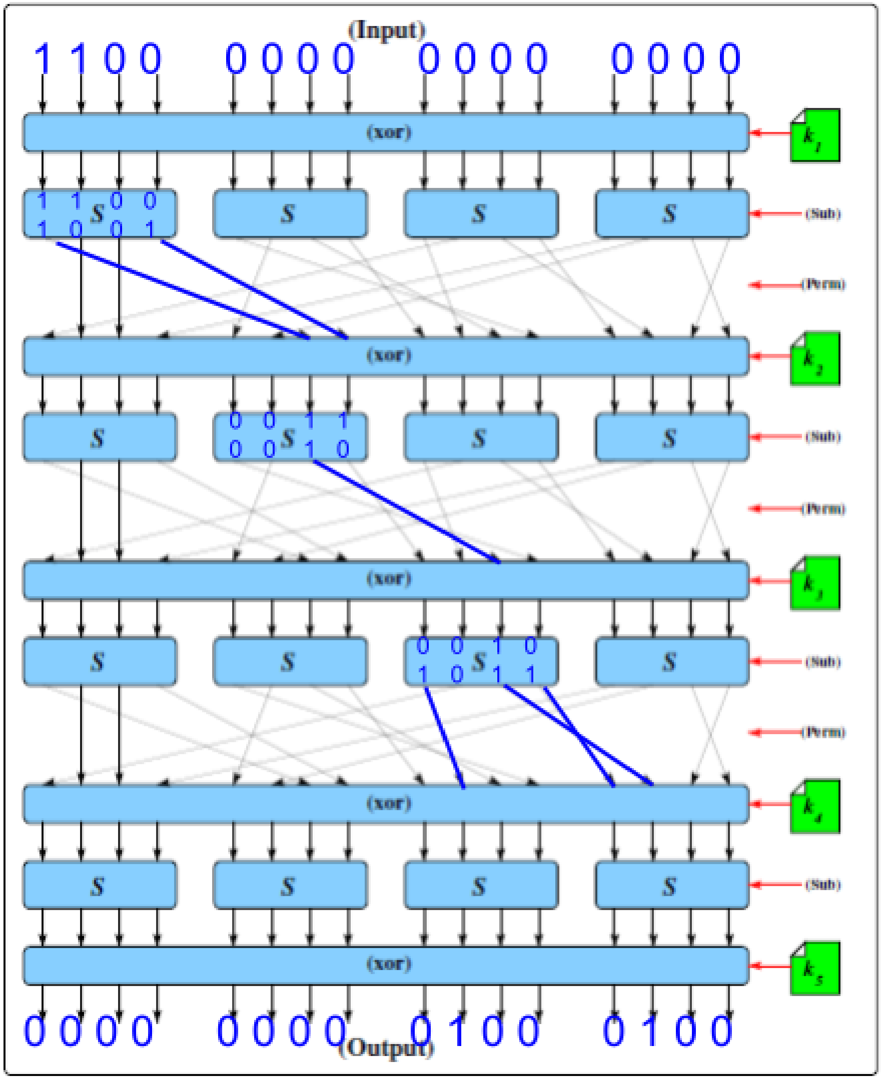
A0216695U Ng Jong Ray, Edward

Question 1



a)

b) $\frac{4}{16} \cdot \frac{2}{16} \cdot \frac{4}{16} = 2^{-7}$

<u>Question 2</u>

X_1	$\oplus$	Y_1	$\oplus$	Y_0		$Z_{2,3}$
0	$\oplus$	0	$\oplus$	0	→	0
0	$\oplus$	1	$\oplus$	1	→	0
1	$\oplus$	0	$\oplus$	1	→	0
1	$\oplus$	0	$\oplus$	1	→	0
0	$\oplus$	1	$\oplus$	0	→	1
0	$\oplus$	0	$\oplus$	0	→	0
1	$\oplus$	0	$\oplus$	1	→	0
1	$\oplus$	0	$\oplus$	0	→	1
0	$\oplus$	1	$\oplus$	1	→	0
0	$\oplus$	1	$\oplus$	1	→	0
1	$\oplus$	1	$\oplus$	0	→	0
1	$\oplus$	0	$\oplus$	0	→	1
0	$\oplus$	0	$\oplus$	1	→	1
0	$\oplus$	1	$\oplus$	1	→	0
1	$\oplus$	1	$\oplus$	0	→	0
1	$\oplus$	1	$\oplus$	0	→	0

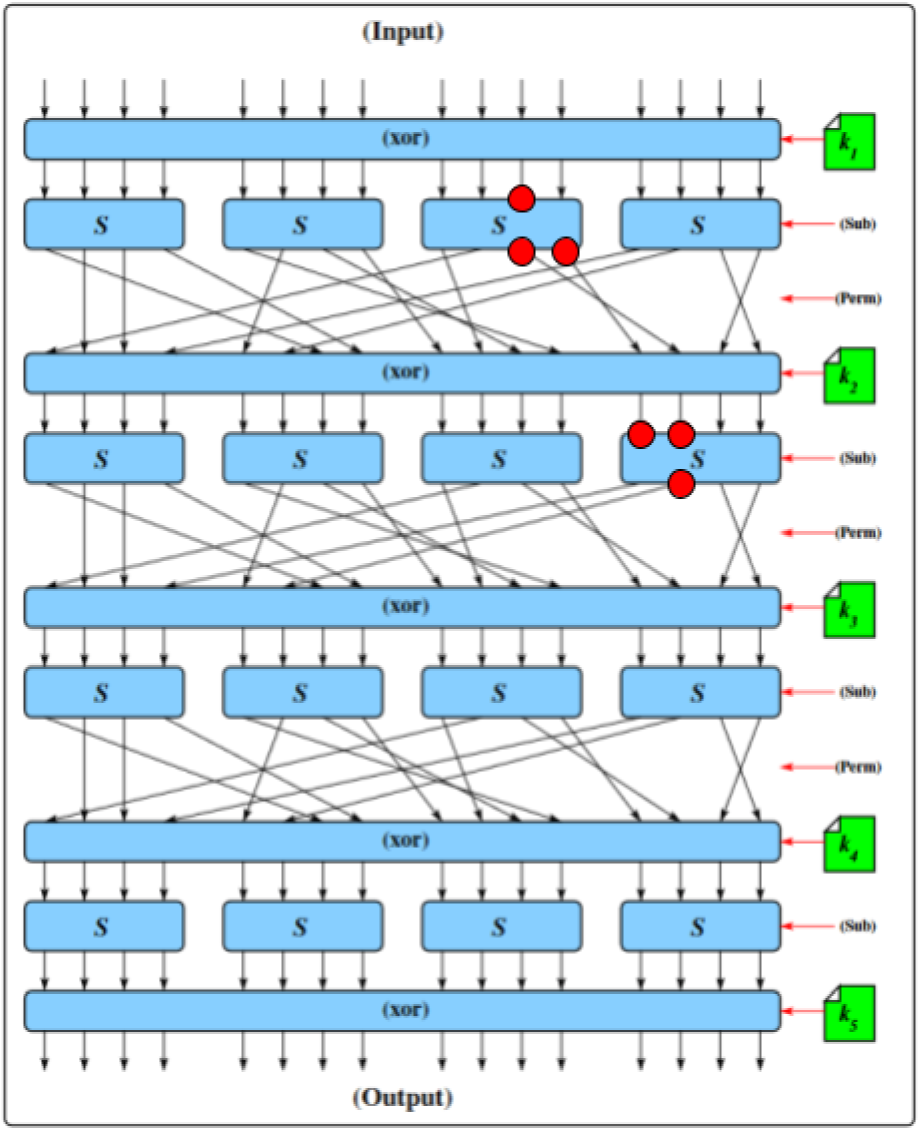
a) Bias of $Z_{2,3}$: $\varepsilon(Z_{2,3}) = \frac{12}{16} - \frac{1}{2} \ =+ \frac{1}{4}$

X_3	$\oplus$	X_2	$\oplus$	Y_2		$Z_{c,4}$	$Z_{2,3}$	$\oplus$	$Z_{c,4}$		$Z_{c,4} \oplus Z_{2,3}$
0	$\oplus$	0	$\oplus$	0	→	0	0	$\oplus$	0	→	0
0	$\oplus$	0	$\oplus$	0	→	0	0	$\oplus$	0	→	0
0	$\oplus$	0	$\oplus$	1	→	1	0	$\oplus$	1	→	1
0	$\oplus$	0	$\oplus$	0	→	0	0	$\oplus$	0	→	0
0	$\oplus$	1	$\oplus$	1	→	0	1	$\oplus$	0	→	1
0	$\oplus$	1	$\oplus$	0	→	1	0	$\oplus$	1	→	1
0	$\oplus$	1	$\oplus$	1	→	0	0	$\oplus$	0	→	0
0	$\oplus$	1	$\oplus$	1	→	0	1	$\oplus$	0	→	1
1	$\oplus$	0	$\oplus$	1	→	0	0	$\oplus$	0	→	0
1	$\oplus$	0	$\oplus$	1	→	0	0	$\oplus$	0	→	0
1	$\oplus$	0	$\oplus$	0	→	1	0	$\oplus$	1	→	1
1	$\oplus$	0	$\oplus$	1	→	0	1	$\oplus$	0	→	1
1	$\oplus$	1	$\oplus$	0	→	0	1	$\oplus$	0	→	1
1	$\oplus$	1	$\oplus$	0	→	0	0	$\oplus$	0	→	0
1	$\oplus$	1	$\oplus$	1	→	1	0	$\oplus$	1	→	1
1	$\oplus$	1	$\oplus$	0	→	0	0	$\oplus$	0	→	0

b)

Bias of $Z_{2,3} \oplus Z_{c,4}$: $\varepsilon(Z_{2,3} \oplus Z_{c,4}) = \frac{8}{16} - \frac{1}{2} \ = \ +\ 0$

First there was a need to find what $Z_{c,4}$ is. Then XOR $Z_{2,3}$ and $Z_{c,4}$ and calculate the bias after.



c)

This pair of S-Box is interesting as we can see how one specific input bit will directly affect one other specific bit in the SPN.

<u>Question 3</u>

$\langle c_1, c_2 \rangle \leftarrow \langle m + kh,\ kg \rangle$

Calculating c_1: $(4, 21)\ +_{E_{31}(1,1)} (22, 21)\ +_{E_{31}(1,1)} (22, 21)$

Calculating $2h\ = (22, 21)\ +_{E_{31}(1,1)} (22, 21)$:

Gradient $\Delta = \frac{3x_h^2 + 1}{2y_h}\ mod\ 31\ = (2 \cdot 21)^{-1} \cdot (3 \cdot 22^2 + 1) \equiv 42^{-1} \cdot 27 \equiv 459 \equiv 25\ mod\ 31$

x coordinate for $2h$: $x_{2h} = 25^2 - (2 \cdot 22) \equiv 23\ mod\ 31$

y coordinate for $2h$: $y_{2h} = 25(22 - 23) - 21 \equiv\ - 46 \equiv 16\ mod\ 31$

Therefore $2h\ = (23, 16)$

Calculating $c_1 = (4, 21)\ +_{E_{31}(1,1)} (23, 16)$:

Gradient $\Delta_{c_1} = \frac{16-21}{23-4} \equiv \frac{-5}{19} \equiv 19^{-1} \cdot\ - 5 \equiv\ - 90 \equiv 3\ mod\ 31$

x coordinate for R: $x_{c_1} = 3^2 - 4 - 23 \equiv 13\ mod\ 31$

y coordinate for R: $y_{c_1} = 3(4 -- 18) - 21 \equiv 45 \equiv 14\ mod\ 31$

There $c_1 = (13, 14)$

Calculating $c_2\ = (0, 1)\ +_{E_{31}(1,1)} (0, 1)$:

Gradient $\Delta = \frac{3x_h^2 + 1}{2y_h}\ mod\ 31\ = (2 \cdot 1)^{-1} \cdot (3 \cdot 0 + 1) \equiv 2^{-1} \cdot 1 \equiv 16\ mod\ 31$

x coordinate for c_2: $x_{c_2} = 16^2 - (2 \cdot 0) \equiv 8\ mod\ 31$

y coordinate for c_2: $y_{c_2} = 16(0 - 8) - 1 \equiv\ - 129 \equiv\ 26\ mod\ 31$

Therefore $c_2 = (8, 26)$

Therefore the message Alice will send to Bob is $\langle (13, 14), (8, 26) \rangle$

Question 4

4. (Exam) Show/prove that there exists a MAC that is secure (existentially unforgeable) but that is not strongly secure. (4 marks)

Let $\Pi = (Gen, Mac, Vrfy)$ be a strongly secure MAC. A different scheme where $\Pi' = (Gen', Mac', Vrfy')$ where $Mac'_k(m) = Mac_k(m)$ || 0 and $Vrfy'_k(m, t||b) = Vrfy_k(m, t)$ where b is the bit added in Mac'. Thus this would mean that Π' is secured as an adversary is unable to forge a correct tag with a message not seen before but not strongly secured since an adversary is able to create a new tag t' for the same message m. This can be done by flipping the last bit of $Mac'_k(m)$ from 0 to 1.

Question 5

In the Hiding experiment, the poly-time adversary A and Challenger will establish common parameters using $Setup(1^n)$. A then outputs a pair of messages $m_0, m_1 \in \{0, 1\}^n$. The challenger will choose a uniform bit $b \in \{0, 1\}$ and computes c_A using $Commit(m_b) \rightarrow c_A$. A is then given com and outputs a bit b' and wins iff $b' = b$.

Under the random-oracle model, following the first property, if x has not been queried to H, then the value of $H(x)$ is uniform. Else, if x has been queried before, then $H(x)$ will be consistent. However, considering here that $x = m \mathbin{+\!\!+} r$ where r is a randomly generated string, c_A will always appear uniform to A no matter the input m because the probability that r repeats $\frac{1}{2^n}$. Therefore, this commitment scheme will be secure for all PPT adversary A where $Pr[Hiding_{A, Com}(n) = 1] \leq \frac{1}{2} + negl(n)$.