CS4236 Assignment 4 feedback

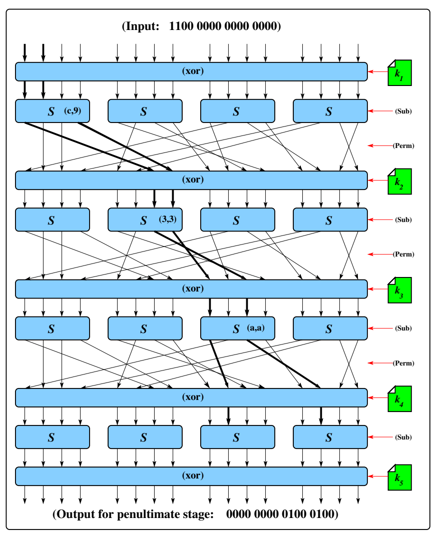
November 18, 2022

1 Questions

1. (Differential) Assume the SPN given in the slides (Session9, and graphic given on the next page). Find a trail which significantly affects some of the least-significant 8-bits of the output: perhaps $\Delta_{\text{in}} = 1100\ 0000\ 0000\ 0000$ and $\Delta_{\text{out}} = 0000\ 0000\ 0100\ 0100$ (have I worked that out correctly this time?).

1. Show the complete trail on the SPN diagram. (2 marks)
2. Calculate $\Pr[\langle \Delta_{\text{in}}, \Delta_{\text{out}} \rangle]$. Show and explain your working. (2 marks)

Possible Answer: *(a) Perhaps:*



(b) *In the first row we choose* $\Pr[\langle 1100, 1001 \rangle] = \Pr[\langle c, 9 \rangle] = \frac{1}{4}$. *The second row has* $\Pr[\langle 0011, 0011 \rangle] = \Pr[\langle 3, 3 \rangle] = \frac{1}{4}$. *The third row has* $\Pr[\langle 1010, 1010 \rangle] = \Pr[\langle a, a \rangle] = \frac{1}{8}$. *As a result, the penultimate row of S-boxes has a high likelihood of affecting the low 8-bits of the SPN:* $\Pr[\langle \Delta_x, \Delta_y \rangle] = \frac{1}{4} \times \frac{1}{4} \times \frac{1}{8} = \frac{1}{128}$. *Some of you did multi-trails, and worked out the probabilities for these.*

Marking schedule: *The section weighting*

(a) *a clear marked trail* *(2 marks)*

(b) *Final result should be* $\frac{1}{128}$ *I think, and there should be a coherent calculation of it. Note that a Pr of* $\frac{1}{256}$ *is probably not useful, so marks removed here.* *(2 marks)*

2. (Linear) Assume the SPN given in the slides (Session9, and graphic given on the next page). A worked example shows the bias of $Z_{1,7} = X_0 \oplus Y_2 \oplus Y_1 \oplus Y_0$. It is $\varepsilon(Z_{1,7}) = +\frac{1}{8}$.

(a) Using a worked example, show the bias of $Z_{2,3} = X_1 \oplus Y_1 \oplus Y_0$. (1 mark)

(b) Calculate the bias of $Z_{2,3} \oplus Z_{c,4}$. Show and explain your working. (2 marks)

(c) The bias of $Z_{2,3} \oplus Z_{c,4}$ is of interest in a pair of the S-Boxes from the SPN. Show on a diagram a relevant pair of S-Boxes, highlighting why they are interesting. (1 mark)

Possible Answer: *Perhaps:*

(a) *Should be $+\frac{1}{4}$, but I expected to see you describe how you worked it out. Either by*

(i) *using the table ($N_L(2,3) = 12$, and so $\varepsilon(Z_{2,3}) = +\frac{1}{4}$), or by*

(ii) *the bitwise technique from class:*

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

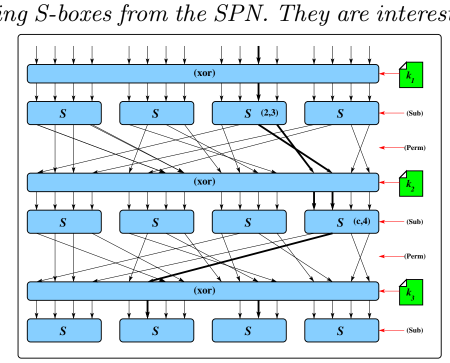
(b) *The bias of X is*

$$\varepsilon(X) = \Pr[X = 0] - \frac{1}{2}$$

So, from the tables, $\varepsilon(Z_{2,3}) = \frac{12}{16} - \frac{1}{2} = +\frac{1}{4}$, and $\varepsilon(Z_{c,4}) = \frac{12}{16} - \frac{1}{2} = +\frac{1}{4}$. The bias of $Z_{2,3} \oplus Z_{c,4}$ is then calculated using the piling up lemma:

$$\begin{aligned} \varepsilon(Z_{2,3} \oplus Z_{c,4}) &= 2^{2-1} \times \tfrac{1}{4} \times \tfrac{1}{4} \\ &= \tfrac{1}{8} \end{aligned}$$

(c) *I was expecting to see two matching S-boxes from the SPN. They are interesting because they connect together.*



Marking schedule: *The section weighting*

(a) *Correct answer and working out (even if it is just using the table).* *(1 mark)*

(b) *Final result should be $\frac{1}{8}$ I think, but there should be a coherent calculation of it.* *(2 marks)*

(c) *Correct.* *(1 mark)*

3. (Like exam) Alice is going to send a message to Bob using ECC *encryption*. Bob has a private/secret key $K_S = \langle \mathcal{G}, g, x \rangle = \langle E_{31}(1,1), (0,1), 4 \rangle$, and public key $K_P = \langle \mathcal{G}, g, h \rangle = \langle E_{31}(1,1), (0,1), (22,21) \rangle$. If Alice encoded her message as the point $(4,21)$, and chooses a random value $k = 2$, what message does she send to Bob? Show your working. (4 marks)

Feedback: *I expected a detailed answer for each part of this.*

Possible Answer: *Perhaps:*

Ciphertext should be

$$\begin{aligned}
\langle c_1, c_2 \rangle &= \langle m + kP_A, kg \rangle \\
&= \langle (4,21) + 2(22,21), 2(0,1) \rangle \\
&= \langle (4,21) + (22,21) + (22,21), (0,1) + (0,1) \rangle \\
&= \langle (4,21) + (23,16), (8,26) \rangle \\
&= \langle (13,14), (8,26) \rangle
\end{aligned}$$

There are a total of three additions. For c_1 where $P = (22,21), Q = (22,21)$, then for $P + Q$:

$$\begin{array}{lclcl}
\Delta &=& \frac{3x_P^2+a}{2y_P} \bmod p = \frac{3(22^2)+1}{2\times 21} \bmod 31 = \frac{27}{11} \bmod 31 = 27 \times 17 \bmod 31 &=& 25 \\
x_R &=& \Delta^2 - 2x_P \bmod p = 25^2 - 2 \times 22 \bmod 31 &=& 23 \\
y_R &=& \Delta(x_P - x_R) - y_P \bmod p = 25(22-23) - 21 \bmod 31 &=& 16 \\
R &=& (x_R, y_R) &=& (23,16)
\end{array}$$

For c_1, where $P = (4,21), Q = (23,16)$ then for $P + Q$:

$$\begin{array}{lclcl}
\Delta &=& \frac{y_Q-y_P}{x_Q-x_P} \bmod p = \frac{16-21}{23-4} \bmod 31 = \frac{26}{19} \bmod 31 = 26 \times 18 \bmod 31 &=& 3 \\
x_R &=& \Delta^2 - x_P - x_Q \bmod p = 9 - 4 - 23 \bmod 31 = -18 \bmod 31 = 13 &=& 13 \\
y_R &=& \Delta(x_P - x_R) - y_P \bmod p = 3(4-13) - 21 \bmod 31 = 3 \times 22 - 21 \bmod 31 = 45 \bmod 31 &=& 14 \\
R &=& (x_R, y_R) &=& (13,14)
\end{array}$$

For c_2, where $P = (0,1), Q = (0,1)$ then for $P + Q$:

$$\begin{array}{lclcl}
\Delta &=& \frac{3x_P^2+a}{2y_P} \bmod p = \frac{1}{2} \bmod 31 = 16 \bmod 31 &=& 16 \\
x_R &=& \Delta^2 - 2x_P \bmod p = 16^2 \bmod 31 &=& 8 \\
y_R &=& \Delta(x_P - x_R) - y_P \bmod p = 16(-8) - 1 \bmod 31 &=& 26 \\
R &=& (x_R, y_R) &=& (8,26)
\end{array}$$

The steps are quite long-winded, but the final result should be $\langle (13,14), (8,26) \rangle$, with clear working.

Marking schedule: *The assessment weighting*

(a) *Correct answer.* *(2 marks)*

(b) *Working shown.* *(2 marks)*

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

Feedback: *I expected an example (there exists...) or clear argument/discussion of some sort.*

Possible Answer: The secure MAC game pays attention to the previous message(s) m, whereas the strongly secure game is recording the previous (m, t) pairs. There were several construction ideas possible here - a proof-by-example:

(i) A MAC that is secure, but probabilistic, will not be strongly secure. There can be multiple (m, t^*) pairs for a message.

(ii) It is also possible to imagine, or construct a MAC with extra bits that are ignored by the verifier. This may be secure, but since you can change these bits at will, it will not be strongly secure.

Marking schedule: *The assessment weighting*

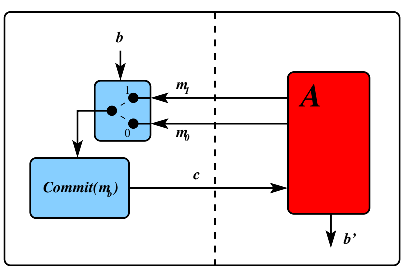
(a) *Understanding of the question.* *(1 mark)*

(b) *Proof, argument, or a good example.* *(3 marks)*

5. In Session8, and in the textbook in Section 5.6.5, a commitment scheme is described, whereby the sender (Alice) commits to a message m, by sending $c_A = \mathcal{H}(m + r)$, where $\mathcal{H}$ is a collision resistant hash, $+$ is string concatenation, and r is a randomly generated string. Prove that this scheme is secure in terms of the Hiding experiment (only). (4 marks)

Feedback: *I expected a proof or clear argument/discussion of some sort. One of you pointed out that as stated in the question above, this scheme is NOT secure! Interpreting the hash under the standard model, you gave a counter-example which showed that it was possible to construct a collision resistant hash which was not hiding-secure. Good work.*

Possible Answer: *Perhaps as mentioned in class, an argument based on the random oracle. The hiding game involves this game:*



where the adversary wins (i.e. result is 1) if $b = b'$. In the question, the commitment is replaced by a hash function of the message concatenated with a random string. For hiding to work, the hash function must be interpreted under a random oracle model. If the hash is a random oracle, the commitment reveals nothing about any of the bits of $m_b + r$, and so does not reveal m_b. At the bottom of page 188 this is discussed.

Marking schedule: *The assessment weighting*

(a) *Understanding of the question.* *(1 mark)*

(b) *Full marks if you showed that it was NOT hiding-secure. Alternatively, your proof mentioned the random oracle model for the hash.* *(3 marks)*