CS4236 Individual Assignment 4

November 1, 2022

1 The rules...

Assignment deadline is 5pm, 11th November 2022 Uploaded to the Luminus assignment submission folder in pdf format. The file name should be like A91234567X.A4.pdf (Your student id and ".A4.pdf") .

2 Questions - 5 assignment questions, due 11th November.

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?).

   (a) Show the complete trail on the SPN diagram. (2 marks)

   (b) Calculate $\Pr[\langle\Delta_{\text{in}}, \Delta_{\text{out}}\rangle]$. Show and explain your working. (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)

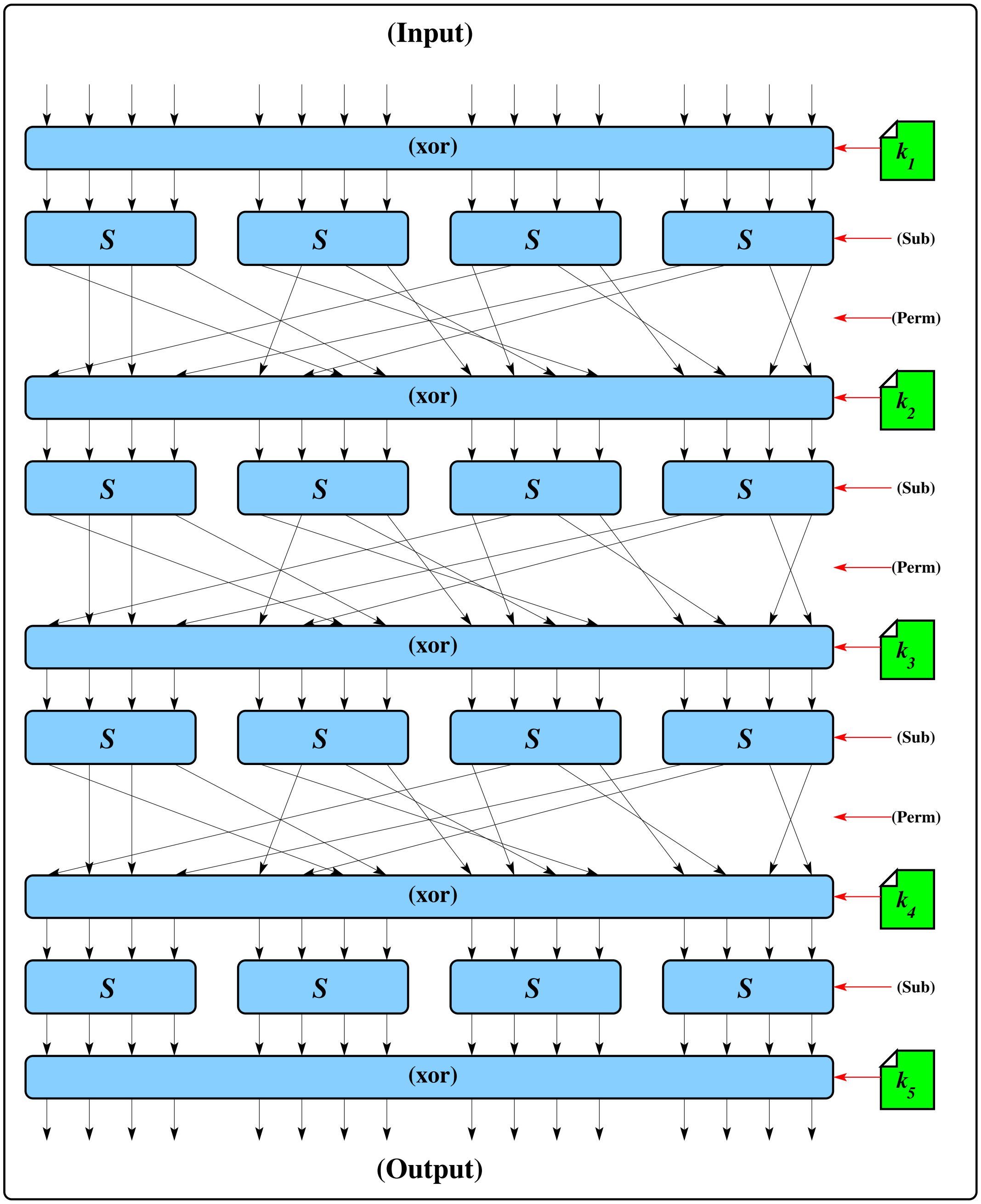
   (b) Calculate the bias of $Z_{2,3} \oplus Z_{c,4}$. Show and explain your working. (2 marks)

   (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)

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)

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


(Input)
(xor)
k_1
S
S
S
S
(Sub)
(Perm)
(xor)
k_2
(Sub)
(Perm)
(xor)
k_3
(Sub)
(Perm)
(xor)
k_4
(Sub)
(xor)
k_5
(Output)