ECE 3170 Cryptographic Hardware for Embedded Systems

Fall 2025

Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology

Homework 10, 105 pts.

Due Monday Nov. 3 prior to 11:55pm

(please turn in homework electronically on Canvas)

As always this semester, you are required to solve this homework alone.

1) (5 pts.) Read the paper by L. Goubin and J. Patarin, "DES and Differential Power Analysis: The 'Duplication' Method," Cryptographic Hardware for Embedded Systems (CHES) conference, 1999. Please indicate that you have read the article by writing an appropriate sentence, e.g., "I hereby certify under the Georgia Tech Honor Code that I have read the CHES 1999 article assigned in this homework for problem 1."

2) (10 pts.) One approach to masking is to replace a multi-bit variable V (e.g., V could have 8 bits) with k variables $V_1,\ldots,V_k$. Condition 1 as described in lecture discusses V_i, $1 \le i \le k$. Why does Condition 1 stress that V_i should have no discernable relationship to V?

3) (15 pts.) Consider DES. In this question we are going to focus on the S-box.

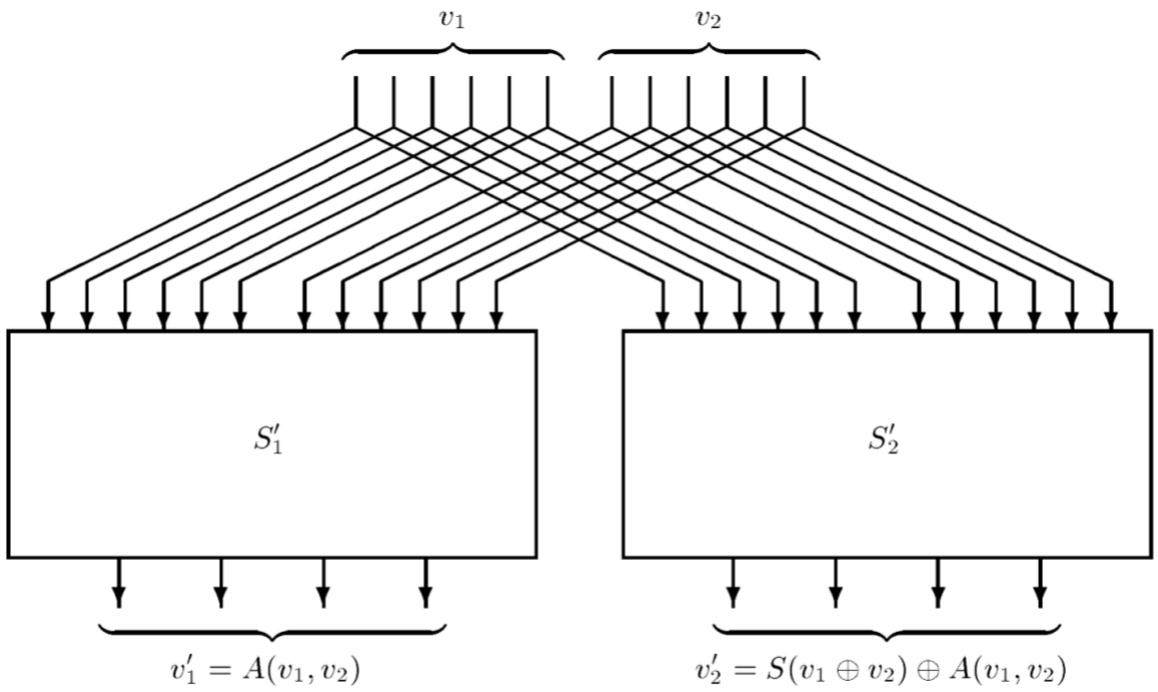
Table 12.6
S-Boxes

S-box 1:

14,	4,	13,	1,	2,	15,	11,	8,	3,	10,	6,	12,	5,	9,	0,	7,
0,	15,	7,	4,	14,	2,	13,	1,	10,	6,	12,	11,	9,	5,	3,	8,
4,	1,	14,	8,	13,	6,	2,	11,	15,	12,	9,	7,	3,	10,	5,	0,
15,	12,	8,	2,	4,	9,	1,	7,	5,	11,	3,	14,	10,	0,	6,	13,

S Box																
	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10	4	1	14	8	12	6	2	11	15	12	9	7	3	10	5	0
11	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

a. (5 pts.) For S-box 1 (shown above in two different formats) calculate the following quantities: S(0x13), S(0x31) and S(0x13 $\oplus$ 0x31). Give your answers in hexadecimal format.
b. (5 pts.) Give a proper definition of linearity of a function.
c. (5 pts.) Is S-box 1 a linear function? If so, why? If not, why not?



Modified implementation: the values $v = v_1 \oplus v_2$ and $v' = v_1' \oplus v_2'$ never explicitely appear in RAM

4) (20 pts.) Consider S_2' in the figure above. Recall from lecture that S_2' is used in a masked implementation of DES.
   a. (5 pts.) Suppose S_2' above is implemented in a memory look-up table. How many kilobits (Kb) of memory are required to implement the look-up table for S_2'? Please give your answer kilobits (Kb). For example, 64 KB (kilobytes) is equal to 64*8 Kb = 512 Kb = 512*1024 bits = 524,288 bits. A correct answer in KB or any units other than Kb (= 2^{10} bits) will receive zero points. (NOTE: an alternative definition for 2^{10} bits is Kibibits or Kib.)
   b. (5 pts.) You are asked to give your estimate of the time it will take to calculate (i.e., look up) S_1' and S_2' in parallel in the masked DES implementation as compared to a standard S-Box calculation (look-up) in the standard (non-masked) DES implementation in an Application-Specific Integrated Circuit (ASIC)? Is the time needed (i) approximately the same, (ii) between 50% and 2X larger or (iii) greater than 2X longer? Please explain the reason(s) for your answer clearly and unambiguously. You may assume a standard SRAM design for the look-up table implementation in the ASIC. Please assume that the ASIC clock is as fast as possible.
   c. (5 pts.) In order to calculate S_2' off-line (i.e., prior to implementing S_2' in the masked DES implementation), is it necessary to calculate $v = v_1 \oplus v_2$? Why or why not? Please explain the reason(s) for your answer clearly and unambiguously.
   d. (5 pts.) In order to calculate A, S_1' or S_2' off-line (i.e., prior to implementing the masked DES implementation), is it necessary to calculate $v' = v_1' \oplus v_2'$? Why or why not? Please explain the reason(s) for your answer clearly and unambiguously.

5) (5 pts.) Read the paper by T. Popp and S. Mangard, "Masked Dual-Rail Pre-charge Logic: Differential Power Analysis Resistance Without Routing Constraints," Cryptographic Hardware for Embedded Systems (CHES) conference, 2005. Please indicate that you have read the article by writing an appropriate sentence, e.g., "I hereby certify under the Georgia Tech Honor Code that I have read the CHES 2005 article assigned in this homework for problem 5."

Table 2. Transitions of the value d_m of a masked node

Line no.	d_{t-1}	m_{t-1}	$d_{m_{t-1}}$	d_t	m_t	d_{m_t}	Energy	Probability
1	0	0	0	0	0	0	E_{00}	$\frac{1}{4}p_{00}$
2	0	0	0	1	1	0	E_{00}	$\frac{1}{4}p_{01}$
3	1	1	0	0	0	0	E_{00}	$\frac{1}{4}p_{10}$
4	1	1	0	1	1	0	E_{00}	$\frac{1}{4}p_{11}$
5	0	0	0	0	1	1	E_{01}	$\frac{1}{4}p_{00}$
6	0	0	0	1	0	1	E_{01}	$\frac{1}{4}p_{01}$
7	1	1	0	0	1	1	E_{01}	$\frac{1}{4}p_{10}$
8	1	1	0	1	0	1	E_{01}	$\frac{1}{4}p_{11}$
9	0	1	1	0	0	0	E_{10}	$\frac{1}{4}p_{00}$
10	0	1	1	1	1	0	E_{10}	$\frac{1}{4}p_{01}$
11	1	0	1	0	0	0	E_{10}	$\frac{1}{4}p_{10}$
12	1	0	1	1	1	0	E_{10}	$\frac{1}{4}p_{11}$
13	0	1	1	0	1	1	E_{11}	$\frac{1}{4}p_{00}$
14	0	1	1	1	0	1	E_{11}	$\frac{1}{4}p_{01}$
15	1	0	1	0	1	1	E_{11}	$\frac{1}{4}p_{10}$
16	1	0	1	1	0	1	E_{11}	$\frac{1}{4}p_{11}$

6) (10) Consider Table 2 shown above. Why does the first row have probability $\frac{1}{4}p_{00}$?

Table 3. Truth table of an MDPL AND gate

Line no.	a_m	b_m	m	q_m	$\overline{a_m}$	$\overline{b_m}$	$\overline{m}$	$\overline{q_m}$
1	0	0	0	0	1	1	1	1
2	0	0	1	0	1	1	0	1
3	0	1	0	0	1	0	1	1
4	0	1	1	1	1	0	0	0
5	1	0	0	0	0	1	1	1
6	1	0	1	1	0	1	0	0
7	1	1	0	1	0	0	1	0
8	1	1	1	1	0	0	0	0

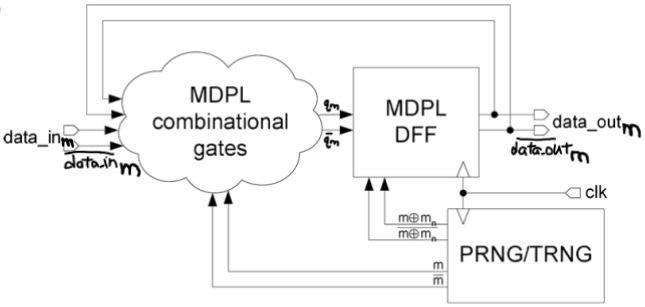


Fig. 5. Architecture of an MDPL circuit

7) (20 pts.) Suppose that "MDPL combinational gates" shown above in Fig. 5 consists of a single AND gate implemented in MDPL. We are going to consider specific cases. Note that $data\_in_m$ and $\overline{data\_in_m}$ come from an MDPL flip-flop not shown where the MDPL flip-flop not shown has inputs $data\_in$, $\overline{data\_in}$, mask bit m and complemented mask bit $\overline{m}$.

   a. (5 pts.) Suppose $data\_in = 0$, $\overline{data\_in} = 1$, $data\_out = 0$, $\overline{data\_out} = 1$, mask bit $m = 1$ and complemented mask bit $\overline{m} = 0$. Given these input values, what are the values of the "MDPL combinational gates" outputs q_m and $\overline{q_m}$?

   b. (5 pts.) Recalling that $q_m = q \oplus m$, what are the values of q and $\bar{q}$?

c. (5 pts.) Now instead suppose $data\_in = 1$, $\overline{data\_in} = 0$, $data\_out = 1$, $\overline{data\_out} = 0$, mask bit $m = 0$ and complemented mask bit $\overline{m} = 1$. Given these input values, what are the values of the "MDPL combinational gates" outputs q_m and $\overline{q_m}$?

d. (5 pts.) Given these newly calculated values (see part c above), and recalling that $q_m = q \oplus m$, what now are the values of q and $\bar{q}$?

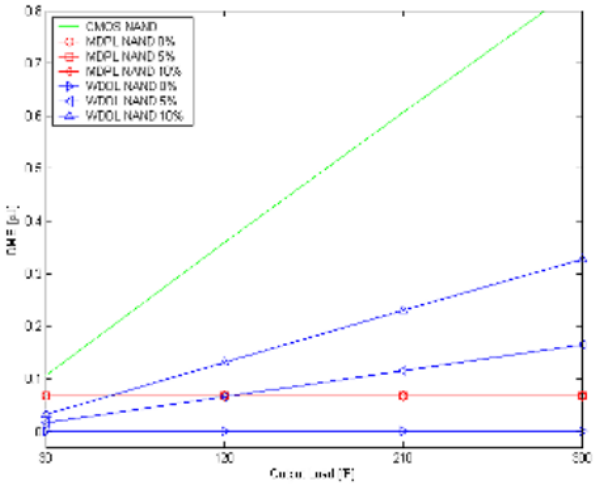


Fig. 6. Comparison of the DME of CMOS, WDDL and MDPL implementations NAND gate

8) (20 pts.) Consider Figure 6 above.

a. (5 pts.) What does the green line represent? Please explain the reason for its

b. (5 pts.) The top blue line is labeled "WDDL NAND 10%." Why is the slope not flat?

c. (5 pts.) The bottom blue line is labeled "WDDL NAND 0%" and is flat. Is this line realistic? Why or why not? Please explain the reason(s) for your answer clearly and unambiguously.

d. (5 pts.) Why are all three red lines on top of each other? What does the slope tell you about MDPL?

YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES. ALL LABORATORY SUBMISSIONS MUST INCLUDE YOUR NAME, COURSE NUMBER, SECTION, AND THE HOMEWORK SET NUMBER. ALL SHEETS MUST BE STAPLED TOGETHER. ALL WRITING MUST BE EASY TO READ (FOR EXAMPLE, YOU MAY HAVE TO WRITE ONLY ON ONE SIDE OF EACH SHEET OF PAPER THAT YOU SUBMIT AND MAY NOT BE ABLE TO USE RECYCLED PAPER). FAILURE TO FOLLOW INSTRUCTIONS MAY RESULT IN ZERO POINTS. ALL WORK MUST BE YOUR OWN. NO PLAGIARISM IS ALLOWED, AND YOU MUST PROPERLY REFERENCE ALL SOURCES OF YOUR INFORMATION – ALTHOUGH YOU SHOULD NOT LOOK FOR AND MAY NOT CONSULT "SOLUTIONS" AVAILABLE FROM OTHER SOURCES (TO REPEAT, YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES!).