

Math 259: Spring 2019
Quiz 5

NAME: SOLUTIONS

Are you taking this class for graduate credit?

Time: 30 minutes

Problem	Value	Score
1	4	
2	3	
3	7	
4	6	
TOTAL	20	

Problem 1 : (4 points) Let

$$F: \mathbb{F}_2^4 \rightarrow \mathbb{F}_2^3$$
$$x \mapsto (f_1(x), f_2(x), f_3(x))$$

be a public key given by the quadratic polynomials

$$f_1(x_1, x_2, x_3, x_4) = x_1x_2 + x_2x_3 + x_1 + x_4,$$
$$f_2(x_1, x_2, x_3, x_4) = x_2x_4 + x_3x_4 + x_1 + x_2 + x_3,$$
$$f_3(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_3 + x_3x_4 + 1.$$

Is

$$x = (1, 0, 1, 1)$$

a valid signature for the message digest

$$y = (0, 1, 1)?$$

Please justify your answer with some computations and a short sentence.

$$f_1(1, 0, 1, 1) = 0 + 0 + 1 + 1 = 0$$

$$f_2(1, 0, 1, 1) = 0 + 1 + 1 + 0 + 1 = 1$$

$$f_3(1, 0, 1, 1) = 1 + 0 + 1 + 1 = 1$$

Yes it is valid since $F(1, 0, 1, 1) = (0, 1, 1)$.

Problem 2 : (3 points) This problem presents a series of statements. For each, please indicate if the statement is true or false.

The question will be graded in such a way as to reward **self-consistency** over correctness. In other words, you can earn a point for answering a question in a manner consistent with your previous answers, even if it is wrong. You can also lose a point for answering a question in a manner inconsistent with your previous answers, even if it is right.

- a) In an “oil and vinegar” multivariate polynomial, “oil” variables may be multiplied together but “vinegar” variables may not.

FALSE

- b) The following system of multivariate quadratic polynomials is an oil and vinegar system, with x_1 and x_2 “oil” variables and x_3 and x_4 “vinegar” variables:

$$P: \mathbb{F}_2^4 \rightarrow \mathbb{F}_2^2 \\ x \mapsto (p_1(x), p_2(x)),$$

where

$$p_1(x_1, x_2, x_3, x_4) = x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 + x_2, \\ p_2(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_4 + x_3x_4 + x_3 + 1.$$

TRUE

- c) To solve an oil and vinegar system where x_1 and x_2 are “oil” variables and x_3 and x_4 are “vinegar” variables, you should first fix random values of x_1 and x_2 . This will give you a linear system in x_3 and x_4 which can then be solved using linear algebra (if a solution exists).

FALSE

Problem 3 : (7 points) Let β be a root of the irreducible polynomial $f(x) = x^2 + x + 1$ over \mathbb{F}_2 . According to the theory we have developed in class, this means that $\mathbb{F}_4 = \mathbb{F}_2[\beta]$.

a) (4 points) Write down a multiplication table for $\mathbb{F}_2[\beta]$.

	0	1	β	$\beta+1$
0	0	0	0	0
1	0	1	β	$\beta+1$
β	0	β	$\beta+1$	1
$\beta+1$	0	$\beta+1$	1	β

$$\beta^2 = \beta + 1 \quad (\text{minimal polynomial of } \beta)$$

$$\beta(\beta+1) = \beta^2 + \beta = (\beta+1) + \beta = 1$$

$$(\beta+1)^2 = \beta^2 + 1^2 = (\beta+1) + 1 = \beta$$

↑
(Freshman's Dream identity)

This is still part of the same problem, where β is a root of $f(x) = x^2 + x + 1$ and $\mathbb{F}_4 = \mathbb{F}_2[\beta]$.

b) (3 points) Compute the following quantities:

i. β^{-1}

$$\text{Since } \beta(\beta+1)=1, \quad \beta^{-1} = \beta+1.$$

ii. β^4

Since $\beta \in \mathbb{F}_4$, by the field equation

$$\beta^4 = \beta.$$

iii. $(\beta+1)^5 = (\beta+1)^4(\beta+1)$

$$= (\beta+1)(\beta+1)$$

$$= (\beta+1)^2$$

$$= \beta$$

since $\beta+1 \in \mathbb{F}_4$, we can use the field equation

looked up in the table

Problem 4 : (6 points) Consider the HFE polynomial

$$G(X) = X^9 \in \mathbb{F}_4[X].$$

Give the associated multivariate quadratic polynomial $G: (\mathbb{F}_2)^2 \rightarrow (\mathbb{F}_2)^2$. Throughout, use the field structure $\mathbb{F}_4 = \mathbb{F}_2[\beta]$, where β is a root of $x^2 + x + 1$.

$$\begin{aligned} G(x_0 + x_1, \beta) &= (x_0 + x_1, \beta)^9 \\ &= (x_0 + x_1, \beta)^8 (x_0 + x_1, \beta) \\ &= (x_0^8 + x_1^8 \beta^8) (x_0 + x_1, \beta) \\ &= (x_0 + x_1, (\beta + 1)) (x_0 + x_1, \beta) \\ &= x_0^2 + x_0 x_1 \beta + x_0 x_1 (\beta + 1) + x_1^2 \beta (\beta + 1) \\ &= x_0 + x_0 x_1 \beta + x_0 x_1 \beta + x_0 x_1 + x_1 \\ &= x_0 x_1 + x_0 + x_1 \end{aligned}$$

$$\begin{aligned} x_i^8 &= \left((x_i^2)^2 \right)^2 = x_i \\ \beta^8 &= (\beta^4)^2 = \beta^2 \\ &= \beta + 1 \\ \beta(\beta + 1) &= \beta^2 + \beta \\ &= \beta + 1 + \beta = 1 \end{aligned}$$

$$\text{So } G(x_0, x_1) = (x_0 x_1 + x_0 + x_1, 0)$$