10pt Bravo!

Cryptographic Protocols
Exercise 01

16-124-836
Marcel Zauder

4pt 1.1 Calculation in finite fields

Evaluate the following polynomials:

1.1.1 Evaluate the polynomial $r(X)$

$$
\begin{aligned}
r(X) &= 3 \cdot X^3 + 2 \cdot X^2 + X && \in GF(5)[X] \text{ at } X = 2 \\
r(X) &= (3 \cdot 2^3 + 2 \cdot 2^2 + 2) \text{ mod } 5 && \text{because } p = 5 \text{ is prime} \\
&= (24 + 8 + 2) \text{ mod } 5 \\
&= 34 \text{ mod } 5 \\
&= 4
\end{aligned}
$$

1.1.2 Evaluate the polynomial $s(X)$

$$
\begin{aligned}
s(X) &= (1+\alpha) \cdot X^3 + \alpha \cdot X^2 + X && \in GF(4)[X] \text{ at } X = \alpha \\
s(X) &= (1+\alpha) \cdot \alpha^3 + \alpha \cdot \alpha^2 + \alpha \\
&= (1+\alpha) \cdot \alpha \cdot \alpha \cdot \alpha + \alpha \cdot \alpha \cdot \alpha + \alpha \\
&= 1 \cdot \alpha \cdot \alpha + (1+\alpha) \cdot \alpha + \alpha && \text{,because } (1+\alpha) \cdot \alpha = 1 \text{ and } \alpha \cdot \alpha = 1 + \alpha \\
&= \alpha \cdot \alpha + 1 + \alpha && \text{,because } 1 \cdot \alpha = \alpha \text{ and } (1+\alpha) \cdot \alpha = 1 \\
&= (1+\alpha) + 1 + \alpha && \text{,because } \alpha \cdot \alpha = (1+\alpha) \\
&= \alpha + \alpha && \text{,because } (1+\alpha) + 1 = \alpha \\
&= 0
\end{aligned}
$$

3pt 1.2 Trivial functions for secure computation

a) is trivial

b) is non-trivial, because if the value of x is greater than the value of y, e.g. $x = 5$ in $\mathbb{GF}(5)$, we cannot determine whether y was, e.g. 2 or 3.

c) is non-trivial, because if the value of x is 0, then no matter which value was assigned to y, there is no way to determine that value after the computation, because f will return 0.

d) is trivial

e) is non-trivial, because there can be more than one value which is greater or less than the chosen value x in the finite field $\mathbb{GF}(5)$, e.g. $x = 3$ then y could be 2 or 1 to produce the output 1.

1.3 Non-trivial functions and an embedded OR

3pt

b) The corresponding table looks as follows:

$max(x, y)$	0	1	2	3	4
0	0	1	2	3	4
1	1	1	2	3	4
2	2	2	2	3	4
3	3	3	3	3	4
4	4	4	4	4	4

As one can see, when the value 4 is picked for x we cannot determine whether y was e.g. 2 or 3, because the output will always be 4.

c) The corresponding table looks as follows:

$x \cdot y$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

As one can see, when the value 0 is picked for x we cannot determine whether y was e.g. 2 or 3, because the output will always be 0.

e) The corresponding table looks as follows:

$e(x, y)$	0	1	2	3	4
0	1	1	1	1	1
1	0	1	1	1	1
2	0	0	1	1	1
3	0	0	0	1	1
4	0	0	0	0	1

As one can see, when the value 2 is picked for x and the output of the function is 1, we cannot determine whether the value y was 0 or 1 (or even 2).