

Cryptographic Protocols

Exercise 7

7.1 Trusted Party Operations

In the lecture we consider a trusted party who can receive inputs, give outputs, and perform addition and multiplication over a field \mathbb{F} . In this exercise, we investigate how the trusted party can perform further operations. Consider a field \mathbb{F} with $|\mathbb{F}| = p$ for a prime p .

- An instruction we would like the trusted party to be able to do is to generate a secret random value. How can this be achieved?
- Given a value $x \in \mathbb{F}$, how can the trusted party compute x^{-1} ? What happens when $x = 0$? How many multiplications are evaluated?
HINT: Use Fermat's Little theorem.
- Consider a trusted party who can also generate secret random values. Design a more efficient way to compute the inverse operation. What happens when $x = 0$?
HINT: Generate a random value r , compute and reveal $y = x \cdot r$.
- Let $x, y, c \in \mathbb{F}$. Consider the following instruction:

$$z = \begin{cases} x & \text{if } c = 0 \\ y & \text{otherwise} \end{cases}$$

How can the trusted party compute this instruction?

HINT: First, find a solution that works for $c \in \{0, 1\}$. Then, solve the general case.

7.2 Shamir Sharings

Let \mathbb{F} be a finite field and $\alpha_1, \dots, \alpha_n$ be fixed, distinct values in $\mathbb{F} \setminus \{0\}$.

- Let s_1, \dots, s_n be arbitrary values in \mathbb{F} . Show that there exists a *unique* polynomial $f \in \mathbb{F}[X]$ of degree at most $n - 1$ that goes through the points (α_i, s_i) .
- Show that any subset of at most t players have no information about a secret that is Shamir-shared with a polynomial of degree at most t .
- Consider a 3-party setting with an adversary that passively corrupts P_2 . Let $a \in \text{GF}(5)$ be the input of P_1 and $b \in \text{GF}(5)$ that of P_3 . Assume a and b are shared via polynomials of degree at most $t = 1$ with $\alpha_1 = 1$, $\alpha_2 = 2$, and $\alpha_3 = 3$ as evaluation points.
Suppose that the players, to compute $c = ab$, locally multiply their shares and then open the product. Show that, given the shares of c (obtained when c was reconstructed) and the shares of player P_2 , the adversary can determine a and b .
- In an alternative sharing protocol, the dealer chooses a random sharing polynomial g with degree *exactly* t . Show that the alternative sharing protocol is not private, i.e., that it gives away information about the secret to the adversary.
Hint: Consider the case where the adversary corrupts t players.