ETH Zurich, Department of Computer Science
SS 2021

Prof. Ueli Maurer
Dr. Martin Hirt
Konstantin Gegier
Chen-Da Liu Zhang

Cryptographic Protocols
Exercise 8

8.1 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.

a) 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?

b) 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.

c) 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 $y = x \cdot r$.

d) 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.

8.2 Shamir Sharings

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

a) Let $s_1, \ldots, s_n$ 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).

b) 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.

c) Consider a 3-party setting with an adversary that passively corrupts P_2. Let $a \in \mathrm{GF}(5)$ be the input of P_1 and $b \in \mathrm{GF}(5)$ 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.

d) 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.