ETH Zurich, Department of Computer Science
SS 2021

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

Cryptographic Protocols
Solution to Exercise 8

8.1 Trusted Party Operations

a) To generate a random secret value, the trusted party receives a random value r_i from each player P_i and computes $\sum_i r_i$.

b) Since the order of the multiplicative group of $\mathbb{F}$ is $p-1$, $x^{p-1} = 1$, which implies that $x^{p-2} \cdot x = 1$, we have that $x^{-1} = x^{p-2}$. Then, to compute the inverse x^{-1}, the trusted party can do $p-2$ consecutive multiplications. Note that when $x = 0$, then the computed "inverse" equals 0. Using the square-and-multiply method, it is enough to compute $O(\log(p))$ multiplications.

c) The trusted party can generate a secret random value r. Then, using a single multiplication gate it computes $y := x \cdot r$ and sends this value to each party P_i. Then, each party computes y^{-1} and sends it to the trusted party. Finally, the trusted party computes $r \cdot y^{-1} = r \cdot (x \cdot r)^{-1} = x^{-1}$. Observe that when $r = 0$, the inverse is not defined. One can choose the size of the field large enough so that this happens with negligible probability.

When $x = 0$, then the players obtain the value $y = 0$. In this case, the players learn that the value that is shared is 0.

d) Let $c \in \{0, 1\}$. To execute the "if"-statement, compute

$$z := (1 - c) \cdot x + c \cdot y.$$

For an arbitrary $c \in \mathbb{F}$, compute

$$z := (1 - c^{p-1}) \cdot x + c^{p-1} \cdot y.$$

This results in the correct value z since $c^{p-1} = 1$ if $c \neq 0$ and $c^{p-1} = 0$ if $c = 0$.

8.2 Shamir Sharings

a) Suppose there is another polynomial f' of degree at most $n-1$ with the property that $f'(\alpha_i) = s_i$ for all $i = 1, \ldots, n$. Then, the polynomial $h := f - f'$ has n roots (namely $\alpha_1, \ldots, \alpha_n$). Since it has degree at most $n-1$, h must be the all-zero polynomial. Thus, $f = f'$.

b) For $T \subseteq \{1, \ldots, n\}$ and $s \in \mathbb{F}$, denote by $S^{T,s}$ the distribution sampled as follows: Choose random coefficients $R_1, \ldots, R_t$, compute $S_i := p(\alpha_i)$ for $p(x) := s + R_1 x + R_2 x^2 + \ldots + R_t x^t$ and set $S^{T,s} := (S_i)_{i \in T}$. That is, $S^{T,s}$ denotes the random variable corresponding to the vector of shares of the players P_i with $i \in T$ when $s \in \mathbb{F}$ is shared.

A sharing scheme reveals no information about s to up to t players if for every $T \subseteq \{1, \ldots, n\}$ with $|T| \leq t$,

$$S^{T,s} \equiv S^{T,s'} \tag{1}$$

for all $s, s' \in \mathbb{F}$.

Consider now a second distribution $\tilde{S}^{T,s}$, which is defined as $S^{T,s}$ except that the sharing polynomial $\tilde{p}(x)$ is obtained by choosing random values $\tilde{s}_1, \ldots, \tilde{s}_t$ of $\tilde{p}(x)$ and interpolating the unique polynomial $\tilde{p}(x)$ through the points $(\alpha_i, \tilde{s}_i)$ and $(0, s)$. It is easily seen that $S^{T,s} \equiv \tilde{S}^{T,s}$ for all T and s, since every choice of coefficients $R_i = r_i$ uniquely determines a polynomial $p(x)$, which in turn uniquely determines the values at the t positions α_i and vice-versa.

Also, $\tilde{S}^{T,s} \equiv \tilde{S}^{T,s'}$ because both distributions are simply $|T|$ uniformly random and independent field elements. This implies (1).

c) Denote by $f(X) = a'X + a$ and $g(X) = b'X + b$ the sharing polynomials of a and b, respectively. In the following we create a system of equations that will allow P_2 to compute a and b from the values which he sees in the protocol:

$$f(2) = a_2 \iff 2a' + a = a_2 \tag{2}$$

$$g(2) = b_2 \iff 2b' + b = b_2 \tag{3}$$

Using the announced shares c_i, one can compute the *unique* polynomial h of degree at most 2 that goes through these points, i.e., $h(1) = c_1$, $h(2) = c_2$ and $h(3) = c_3$:

$$h(X) = h_1 + h_2 X + h_3 X^2 \tag{4}$$

for some coefficients h_1, h_2,and h_3, which can be computed, e.g., using Lagrange's interpolation formula.

Because h corresponds to the polynomial resulting from the multiplication of f and g, it should have the following form:

$$\begin{aligned} h(X) &= f(X) \cdot g(X) \\ &= (a + a'X) \cdot (b + b'X) \\ &= ab + (ab' + a'b)X + a'b'X^2 \end{aligned} \tag{5}$$

Because the coefficients in (4) and (5) should be the same

$$\begin{aligned} ab &= h_1 \\ ab' + a'b &= h_2 \\ a'b' &= h_3 \end{aligned}$$

The above three equations, together with (2) and (3), form a system of 5 equations over GF(5) with 4 unknowns. Solving these equations P_2 can compute the factors a and b.

d) The adversary can use its shares to interpolate a degree-$(t-1)$ polynomial $g' \neq g$, since the degree of the sharing polynomial g is exactly t. Because $g(\alpha_i) = g'(\alpha_i)$ for t indices $i \in \{1, \ldots, n\}$, $g(0) \neq g'(0)$ (since otherwise $g' = g$). Thus, the adversary can exclude $g'(0)$ as the secret, which violates privacy.