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 13

13.1 Adversaries in the Player Elimination Framework

Observe that after player elimination in one block the communication among honest parties is reduced in the following block executions, if an honest party is eliminated (since there are fewer honest parties).

Also, eliminating two corrupted parties in one player elimination step reduces the total communication among honest parties, as there are fewer possible block repetitions.

These observations result on the following strategy for the adversary:

The adversary corrupting t parties plays the first $t-1$ blocks honestly. During the tth block, the adversary cheats t times, each time with one party P_i towards an honest party P_j, resulting in t repititions of the last block. The other corrupted parties behave honestly, even when chosen as the referee in the *Fault Localization* step. P_i does not accuse the referee in step 3.5, resulting in $E = \{P_i, P_j\}$ being eliminated.

13.2 Berlekamp-Welch-Decoding

a) We have two cases:
Case $j \in A$: Then we have $e(\alpha_j) = 0$. Thus, $p(\alpha_j) = g(\alpha_j) \cdot e(\alpha_j) = g(\alpha_j) \cdot 0 = s_j \cdot 0$.
Case $j \notin A$: Then we have $s_j = g(\alpha_j)$, since s_j was sent by an honest party. Thus, $p(\alpha_j) = g(\alpha_j) \cdot e(\alpha_j) = s_j \cdot e(\alpha_j)$.

b) Note that $g(x) = \frac{p(x)}{e(x)}$. Thus, P_i can compute g, if it can determine p and e.
We have $\deg(e) \leq t$ and $\deg(p) = \deg(g) + \deg(e) \leq d + t$. Since e is a monic polynomial of degree at most t, there are t unknown coefficients of e and $d + t + 1$ unknown coefficients of p.
Subtask a) yields n linear equations in these at most $d + 2t + 1$ unknown coefficients. This system of equations can be solved (in $\mathcal{O}(n^3)$ using e.g. Gaussian elimination) if $n \geq d + 2t + 1$, which is equivalent to $d < n - 2t$.

13.3 Sharings of Zero

In the following, denote by $\mathbb{F}$ the field used in the sharing.

a) The protocol proceeds similarly to the passively-secure protocol that allows the players to create $n - t$ double-sharings of random values.

1. Each player P_i t-shares $s_i = 0$ among all players, resulting in sharings $[s_1], \ldots, [s_n]$.

2. The players (by local computation) compute the sharings

$$([r_1], \ldots, [r_{n-t}]) = M([s_1], \ldots, [s_n]),$$

where M is some hyper-invertible $(n-t) \times n$-matrix over $\mathbb{F}$.

3. The players use $[r_1], \ldots, [r_{n-t}]$ as sharings of zero.

We show that the outputted sharings are random, correct degree-t sharings of 0.

Essentially, we use the fact that the 0-sharing property "survives" applying a hyper-invertible matrix.[1]

Let f be the hyper-invertible function induced by the matrix M. Denote the indices of the honest players by $H \subseteq \{1, \ldots, n\}$, $|H| = n - t$. By hyper-invertibility of f, for any t fixed sharings $\{[s_i]\}_{i \notin H}$, there exists a bijective linear function $f' : \{[s_i]\}_{i \notin H} \to \{[r_j]\}_j$. Hence, the outputted sharings are the result of applying a bijective linear function f' (chosen by the adversary) to random, correct degree-t sharings of 0. Since any linear combination of degree-t sharings of 0 is again a degree-t sharing of 0, the outputted sharings are correct and random.

b) The protocol proceeds similarly to the actively-secure (with abort) protocol for generating $T = n - 2t$ random double-sharings.

In particular,

1. Each player P_i shares $s_i = 0$ among all players, resulting in sharings $[s_1], \ldots, [s_n]$.
2. The players (by local computation) compute the sharings

$$([r_1], \ldots, [r_n]) = M([s_1], \ldots, [s_n]),$$

where M is some hyper-invertible $(n \times n)$-matrix over $\mathbb{F}$.

3. For $i = T+1, \ldots, n$, every player P_j sends his share of $[r_i]$ to P_i, who checks that all shares lie on a polynomial g of degree at most t and that $g(0) = 0$. If any of these conditions does not hold, P_i broadcasts a complaint and the protocol *aborts*.
4. The players use $[r_1], \ldots, [r_T]$ as sharings of zero.

It is easily seen that the protocol succeeds if all players follow the instructions (that is, the protocol is *complete*).

It remains to show that if the protocol does not abort, then the resulting sharings $[r_1], \ldots, [r_T]$ are indeed random degree-t sharings of zero. Indeed, if the protocol does not abort, then at least t of the sharings $[r_i]$ opened in Step 3 are correct degree-t sharings of zero. Moreover, $n - t$ of the sharings $[s_i]$ were created by honest players and thus are degree-t sharings of zero as well. Since M induces a hyper-invertible function, there exists a bijective linear function f mapping these n correct sharings of zero to the remaining sharings. Hence, all sharings are correct degree-t sharings of zero.

Given this, one can argue about the randomness of the sharings in the same fashion as in part a).

[1] Actually, the sharings of zero form a vector space.