ETH Zurich, Department of Computer Science
SS 2021

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

Cryptographic Protocols
Exercise 13

13.1 Adversaries in the Player Elimination Framework

Consider any non-robust but detectable protocol run in the Player Elemination Framework with t corrupted parties. Find a strategy for the adversary that maximizes the communicated bits among honest parties.

13.2 Berlekamp-Welch-Decoding

Consider the local reconstruction protocol from the lecture where party P_i receives shares s_i of a degree-d-sharing (a polynomial g with $\deg(g) \leq d$) of some secret s. Let $A \subseteq \{1, \ldots, n\}$ (where $|A| \leq t < \frac{n}{3}$) be the indices of corrupted parties P_j, which sent values with $s_j \neq g(\alpha_j)$.

Consider the polynomials $e(x) = \prod_{i \in A}(x - \alpha_i)$ and $p(x) = g(x) \cdot e(x)$.

a) Show that for all $j \in \{1, \ldots n\}$ we have $p(\alpha_j) = s_j \cdot e(\alpha_j)$.

b) Show that for $d < n - 2t$ party P_i can efficiently recover $g(x)$.

13.3 Sharings of Zero

a) Describe a passively secure protocol that allows n players to jointly generate $\Omega(n)$ random sharings of 0 and prove its security.

b) Modify your protocol such that it becomes actively-secure with abort, and prove its security.