Weak PRF Protocol: Pseudocode

Vivek Sharma

Jan 11, 2020

1 Fully Distributive Evaluation Protocol

The protocol is divided into three phases:

1.1 Phase 1:

Each server S_i holds replicated additive shares of key $k_i \in \mathbb{Z}_n^2$ and $x_i \in \mathbb{Z}_n^2$ and computes h, which is the multiplication of key and input over $\mathbb{Z}_2$. This computation is performed locally.

1.2 Phase 2:

1. Each server will

1.3 Phase 3:

Explanation: