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 $x_i \in \mathbb{Z}_n^2$

1.2 Phase 2:

1.3 Phase 3:

1. Start with random weight $w \in \mathbb{R}$ and $\triangledown J(w)^{'} = 0$
2. For each record i out of n records in dataset:
3. Compute $x_i^{'} = (1|x_i), y_i^{'} = 2 * y_i - 1$
4. Compute $z_i = x_i^{'}.y_i^{'}$ and transpose the result, z_i^T
5. $\triangledown J(w)^{'} = \triangledown J(w)^{'} + \sigma(z_i^T.w).z_i$
6. Compute $\triangledown J(w) = -\frac{1}{n}.\triangledown J(w)^{'}$ which is gradient of the loss function w.r.t. w
7. For limited number of rounds(as you told me, seven iteration for best value of w)
8. Compute $w^{(t+1)} = v^{(t)} + \alpha_t.\triangledown J(v^{(t)})$
9. Compute $v^{(t)} = (1 - \gamma_t).w^{(t+1)} + \gamma_{(t)}.w^{(t)}$
10. Recompute $\triangledown J(w)$

Explanation: