Weak PRF Protocol: Pseudocode

Vivek Sharma

Jan 11, 2020

1 Fully Distributive Evaluation Protocol

The key is structured as a vector in $\mathbb{Z}_2$

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, at this point have locally computed their shares, which was the multiplication of two vectors.
2. Server 1 randomly chooses a value $c \in \mathbb{Z}_3^m$ and each bit of value is converted to it's 2-bit representation to form $c_0 and c_1$ respectively.
3. Meanwhile, Server 1, 2 and 3 runs sub-protocol for m instances(m is the length of additive share and also the value of c, which is with server 1.

   For $1 \leq j \leq m$:

   Each server $s_i, i \in 1, 2, 3$ share their input $h_{i,j}$ [Note: $h_{i,j}$ is the input of server s_i in j^{th} iteration]

   Compute combined XOR of their input: $comb := h_1 \oplus h_2 \oplus h_{13}$

1.3 Phase 3:

Explanation: