AND and OR gate FSS scheme

May 30, 2020

Let there are n parties, denoted by p_i, and each party has a bit b_i, where $i \in \{1, 2, ..., n\}$. They want to evaluate AND or OR of $b_i`s$. So, each party p_i generates a random bit r_i to mask b_i by XORing with r_i. Parties calculate $m_i = b_i \oplus r_i$ and pass m_i to gate.

1 AND gate

Let $r = r_1|r_2|...|r_n$ and $\mathbf{1} = 11...1(ntimes)$. Consider a DPF $f : \{0, 1\}^n \to 0, 1$ be given as

$$f(x) = \begin{cases} 1, & \text{if } x = r \oplus \mathbf{1} \\ 0, & \text{otherwise} \end{cases}$$

DPF $f(x)$ corresponds to AND gate where $x = m_1|m_2|...|m_n$ and m_i is masked input from party p_i for $i \in \{1, 2, ..., n\}$.

2 OR gate

Let $r = r_1|r_2|...|r_n$. Consider a DPF $g : \{0, 1\}^n \to 0, 1$ be given as

$$g(x) = \begin{cases} 1, & \text{if x = r} \\ 0, & \text{otherwise} \end{cases}$$

Consider function $f : \{0, 1\}^n \to \{0, 1\}$ given by

$$f(x) = 1 - g(x)$$

Function $f(x)$ corresponds to OR gate where $x = m_1|m_2|...|m_n$ and m_i is masked input from party p_i for $i \in \{1, 2, ..., n\}$.