Direct Extension of RR17b PSI Protocol to Multiparty Setting

November 14, 2020

Protocol $\Pi_{M-RRPSI}$

Parameters:
n - a bound on the size of the input set of each party; $\mathcal{D}$ – a domain of input items;
σ - computational security parameter; λ - statistical security parameter;
N_{BF} - size of the Bloom filter; $N_{\mathrm{OT}} > N_{\mathrm{BF}}$ - number of random OTs to perform;
N^1_{OT}, N_{cc}, $N_{maxones}$ – parameters for Π_{AppROT} computed as in Sec. **??**.
Inputs: Each party P_i, $i \in \{0,...,t\}$, inputs its set of items $X_i = \{x_{i1}, x_{i2}, ..., x_{in_i}\}$, $n_i \leq n$, $x_{ij} \in \mathcal{D}$.

Offline-phase $\Pi^{Offline}_{MPSI}$

1. **[hash seeds agreement]**
Parties run a coin-tossing protocol to agree on random hash-functions h_1, h_2, ... ,h_k: $\{0,1\} \to [N_{\mathrm{BF}}]$.
2. **[approximate ROT-offline]** Parties perform in parallel (with parameters N_{OT}, N^1_{OT}, N_{cc}, and $N_{maxones}$):
   - P_0 as a receiver performs $\Pi^{Offline}_{AppROT}$ with each P_i, $i \in [t]$.
3. **[random shares]** Each P_i, $i \in [t]$, sends $S^{il} = (s^{il}_1, ..., s^{il}_{N_{\mathrm{BF}}})$ to any P_l, $l \in [t] \setminus \{i\}$, where $s^{il}_r \xleftarrow{R} \{0,1\}^\sigma$, $r \in [N_{\mathrm{BF}}]$.

Online-phase Π^{Online}_{MPSI}:

4. **[compute Bloom filters]** Each party P_i, $i \in [t] \cup \{0\}$, locally computes the Bloom filter BF_i of its input set X_i. If $n_0 < n$, then P_0 computes the Bloom filter of the joint set X_0 with $(n - n_0)$ random dummy items.
5. **[approximate ROT-online]**
   - Using BF_0 as its input, P_0 performs Π^{Online}_{AppROT} with every other party to finish Π_{AppROT}s started on Step 2. As a result, it receives t arrays M^i_*, P_i learns M^i, where M^i_* and M^i are N_{BF}-size arrays of σ-bit values.
   - P_0 computes $\mathrm{GBF}^0 = \bigoplus_{i \in [t]} M^i_*$.
6. **[secret-sharing of GBFs and sending codewords]** Each P_i, $i \in [t]$, locally computes
$$\mathrm{GBF}^i = M^i \bigoplus_{l \in [t] \setminus \{i\}} \left[S^{li} \oplus S^{il} \right].$$
For each item x in P_i's input set, it computes a summary value $K^i_x = \bigoplus_{r \in h_*(x)} GBF^i[r]$, where $h_*(x) = \{h_i(x) | i \in [k]\}$. P_i sends a random permutation of $K^i = \left\{ K^i_x | x \in X_i \right\}$ to P_0. If $|X_i| < n$, then P_i completes K^i up to size n by uniformly random σ-bit values before the permutation.
7. **[output]** For each $x_{0j} \in X_0$, P_0 outputs x_{0j} as a member of the intersection, if there exist $K^1[j_1]$, $K^2[j_2]$, ..., $K^t[j_t]$ such that
$$\bigoplus_{r \in h_*(x_{0j})} \mathrm{GBF}^0[r] = K^1[j_1] \oplus K^2[j_2] \oplus ... \oplus K^t[j_t].$$

Figure 1: Direct multiparty extension of the PSI protocol of RR17b