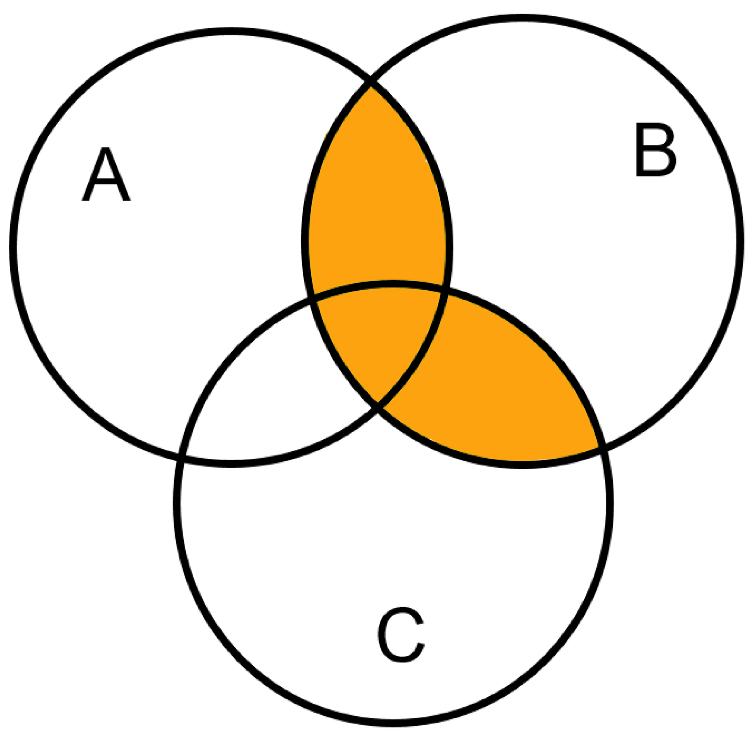
UNIVERSITY OF HELSINKI
FACULTY OF SCIENCE
DEPARTMENT OF COMPUTER SCIENCE

# Multi-party Private Set Operations with an External Decider

Sara Ramezanian, Tommi Meskanen and Valtteri Niemi
{sara.ramezanian, tommi.meskanen, valtteri.niemi@helsinki.fi}

- **Private Set Operation (PSO)**
  - ✓ A cryptographic protocol for two or more parties.
  - ✓ All / some of the parties have an input set of private elements.
  - ✓ All / some of the parties want to compute the output of one or more set operations of the input sets.
- **Goal** is to compute the output without revealing anything about the elements that are not in the output.




$$(A \cap B \cap \bar{C}) \cup (B \cap C)$$

**External Decider (D)** is a special party that does not have an input set, and is the only party who learns the output of the protocol [1].

**Examples:**

- Secure electronic voting.
- Privacy-preserving parental control [2].
- Decentralized social networking platform such as HELIOS [3], to obtain common interests between different groups of friends.

**Our Contribution:**

- A general solution to any PSO problem with D and with limited universe (PSO-Lim) by using a non-deterministic additively homomorphic cryptosystem.
- A general solution to find cardinality and emptiness of the output to any PSO problem with D and with unlimited universe (PSO-Unlim) by using keyed hash function.

**PSO-Lim Protocol for parties $P_1, \dots, P_n$ and a decider D:** Private sets $S_1, \dots, S_n$ are subsets of $U = \{a_1, \dots, a_u\}$. The decider wants to learn $S_T = (A_{1,1} \cup \dots \cup A_{1,\alpha_1}) \cap \dots \cap (A_{\beta,1} \cup \dots \cup A_{\beta,\alpha_\beta})$ where $1 \le \alpha_i \le n$, $\beta \in \mathbb{N}$, and each $A_{i,j} \in \{S_1, \dots, S_n, \bar{S}_1, \dots, \bar{S}_n\}$.

**Set-up phase**

1. D creates public and private keys for Paillier cryptosystem, and sends public keys and $U$ to parties. Parties create a shared repository.
2. Each $P_i$ creates a set containing many instances of $enc(0)$, and another set containing many instances of $enc(r)$, where $r$ is a random number chosen for that instance.
3. Parties create $\beta$ vectors $W^k$ of length $u$, where $W^k = (enc(r_{1,k}), \dots, enc(r_{u,k}))$, when $1 \le k \le \beta$.

**On-line phase**

1. For every vector $W^k$ each $P_i$ modifies the vector as follows. If $u_j \in S_i$ then $P_i$ replaces $W_j^k$ with $enc(0)$. Otherwise, $P_i$ multiplies $W_j^k$ with $enc(0)$.
2. After all the vectors $W^k$ have been computed, one of the parties (e.g., $P_n$) creates a vector $Z$ where $Z_j = \prod_{k=1}^{\beta} W_j^k$. Party $P_n$ sends vector $Z$ to D.
3. D decrypts $Z$. If $dec(Z_j) = 0$, then $a_j \in S_T$. Otherwise, $a_j$ is not in $S_T$.

**Performance:** If public key in Paillier is of length 4096 bits and we assume that $\alpha = \beta = n$, the numbers in the table show the required time for each party to modify $Z$ with a single thread. When $u = 2^2, 2^5, 2^7, 2^{10}$ the decider needs 0.02, 0.17, 0.68, 5.51 seconds respectively, to decrypt this vector with 32 threads.

| | $n=3$ | $n=5$ | $n=10$ | $n=15$ | $n=20$ |
|---|---|---|---|---|---|
| $u=2^2$ | 0.001 | 0.002 | 0.003 | 0.005 | 0.007 |
| $u=2^5$ | 0.008 | 0.013 | 0.025 | 0.039 | 0.05 |
| $u=2^7$ | 0.031 | 0.05 | 0.1 | 0.15 | 0.2 |
| $u=2^{10}$ | 0.237 | 0.391 | 0.786 | 1.178 | 1.56 |

**[1]:** Ramezanian, S., Meskanen, T., & Niemi, V. Multi-party Private Set Operations with an External Decider. In 35th *DBSEC* (pp. 117-135). Springer, Cham. 2021.
**[2]:** Ramezanian, S., Meskanen, T., & Niemi, V. Parental Control with Edge Computing and 5G Networks. In 29th FRUCT Conference (pp. 290-300). IEEE. 2021.
**[3]:** HELIOS project homepage (2022). Retrieved from https://helios-h2020.eu/

HELIOS
European Commission
5G FORCE
BUSINESS FINLAND