Quantum SMPC: Rich in theory, limited in practice

A systematic review of quantum secure multi-party computation

Author: Nicoleta Dobrică[1]
n.dobrica@student.tudelft.nl
Supervisor: Dr. Roland Kromes[1]
Responsible Professor: Dr. Zeki Erkin[1]
[1]TU Delft, Faculty of EEMCS

1. Background

- **Secure Multi-Party Computation (SMPC)** is a cryptographic technique which allows two or more parties to jointly compute a function based on their private inputs [1] (Fig. 1).

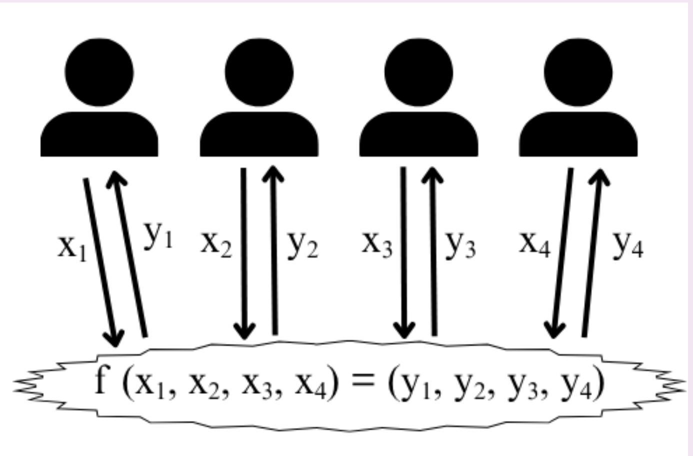

Figure 1: Representation of SMPC

- **Quantum SMPC (QSMPC)** has evolved from early quantum secret sharing [2] into a wide field of protocols that enable secure multi-party collaboration using quantum techniques.
- **The motivation** for designing QSMPC is to achieve security against quantum adversaries and to leverage quantum physics for privacy guarantees beyond computational assumptions.
- **Our contribution** is to provide an analysis of current QSMPC protocols, examining necessary quantum resources, privacy guarantees and feasibility. No other study has done such a systematic review.

2. Research Question

RQ: How has SMPC been adapted to quantum computing?

- RQ1: What QSMPC protocols are proposed?
- RQ2: What are the quantum resource requirements for these protocols?
- RQ3: How do these protocols ensure privacy?
- RQ4: Which of the proposed schemes are feasible on current technology and what are the main implementation obstacles?

3. Methodology

- PRISMA [3] methodology (Fig. 2).
- Included papers have to be published between 2020-2025 and contain technical descriptions or implementation details. Papers have to be written in English.
- We excluded papers that discuss only post-quantum or quantum-safe SMPC or quantum primitives that are not applied to actual QSMPC protocols.
- 37 papers were included in the final version of the survey.

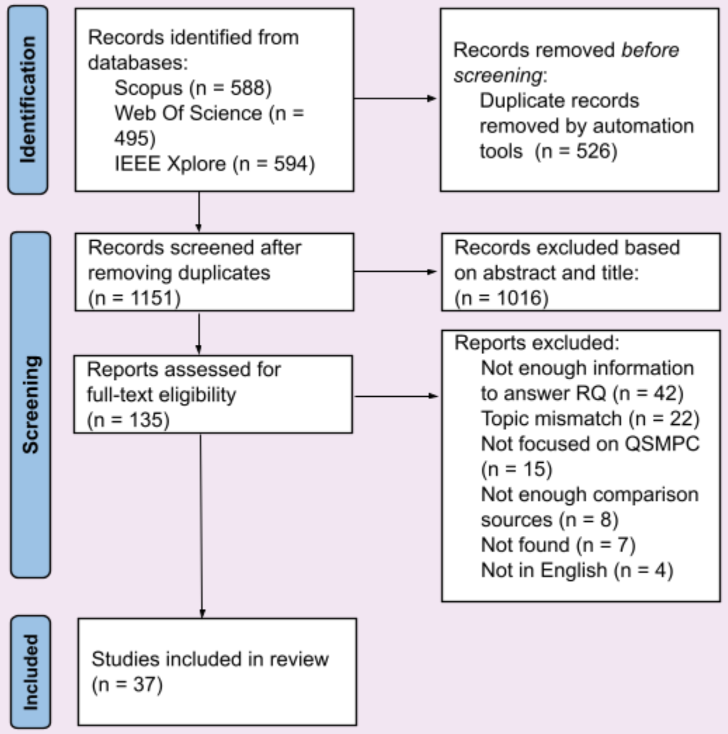

Figure 2: PRISMA flowchart diagram

4. Analysis of QSMPC protocols

RQ1: Overview of QSMPC protocols

- Wide range of functionalities identified (Fig. 3).
- Most numerous: **Summation** and **Comparison**.

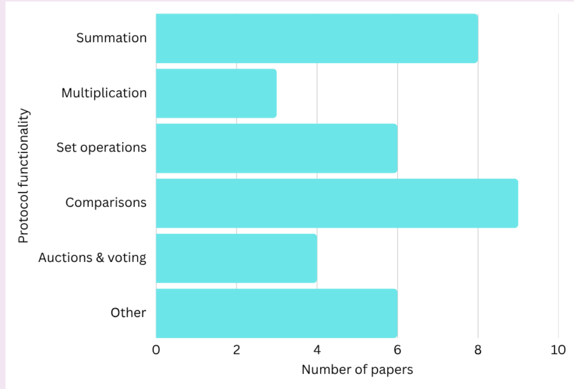

Figure 3: Included papers grouped by protocol functionality

RQ2: Quantum resource requirements

- Frequently used: **Entangled states**, **QFT**, **QKD**, **single photon states** (Fig. 4)
- Resource choice impacts feasibility.

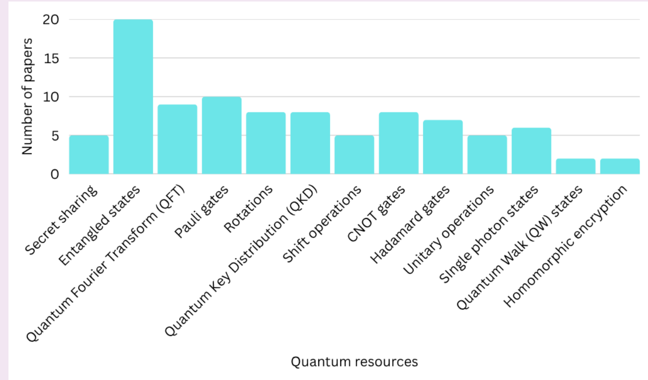

Figure 4: Identified quantum resources

RQ3: How privacy is ensured

- 25 out of 37 papers rely on **semi-honest third parties** that do not collude with other parties.
- **Decoy particles** are most commonly used.

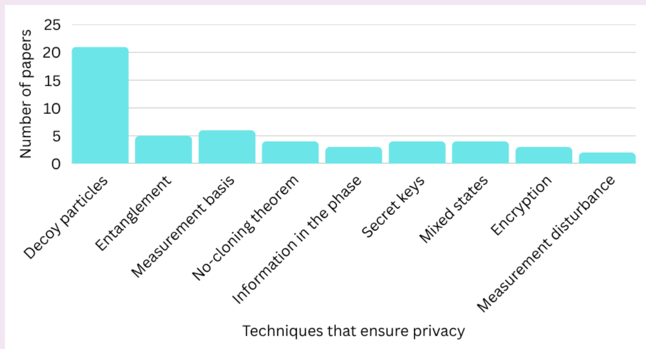

Figure 5: Techniques used for ensuring privacy

RQ4: Feasibility analysis

- Only 18 out of 37 papers discuss feasibility.
- Simulations in IBM Qiskit are conducted on a small scale, without accounting for noise.
- The QFT cannot be currently implemented.

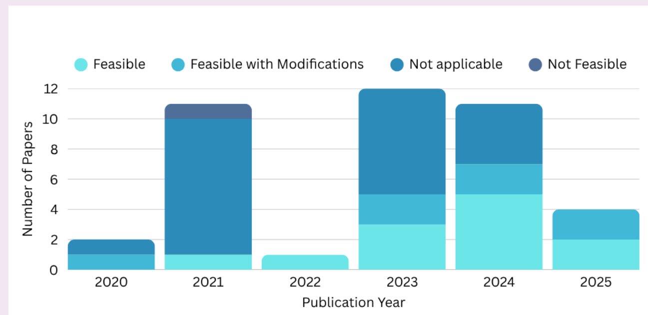

Figure 6: Feasibility of protocols over the years

5. Discussion and Conclusion

- QSMPC is applied to multiple privacy-dependent domains.
- Privacy guarantees are generally rooted in quantum properties and honesty assumptions.
- Simulations of protocols require scale reductions and algorithmic simplifications.
- **Limitation**: Not all SMPC protocols could be included in the search query.
- **Limitation**: The lack of data on feasibility and precise quantum resources has to be accounted for.
- Due to missing necessary hardware, there is a noticeable feasibility gap.
- **Future Work**: Research in protocols that account for quantum noise or do not require semi-honest third parties and analysis and comparison of qubit efficiency.

References

[1] Y. Lindell. "Secure multiparty computation". In: *Communications of the ACM* 64.1 (2021), pp. 86–96.

[2] R. Cleve, D. Gottesman, and H.-K. Lo. "How to share a quantum secret". In: *Physical review letters* 83.3 (1999), p. 648.

[3] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, et al. "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews". In: *British Medical Journal* 372.71 (2021).