Privacy Preserving, Structure-Aware, Multi-party Protocols

Jean-Guillaume Dumas and Aude Maignan

October 8, 2026

Consider a situation where it is desirable to protect the privacy of whistle-blowers. There, it would be interesting to be able to determine if an alert has already been raised but not who has already done so. Similarly, in order to minimize vulnerabilities in their infrastructure, several organizations want to optimize their security updates but are reluctant to reveal details pertaining to their current or past attacks or sensitive network data.

Secure multi-party computing (SMC) is a subfield of cryptography dedicated to the protection of the privacy of the participants. To solve the above type of issues, the idea is to create methods or protocols for parties to jointly compute a function over their inputs while keeping those inputs private [5, 3]. More precisely, a secure multi-party computation is an *interactive protocol* between several participants (players) ensuring some security properties such as privacy of parts of the involved data (potentially differential), but it can also be anonymity, a (potentially zero-knowledge) proof of knowledge, or a verifiable computation. The efficiency is measured both in terms of average communication/rounds and computations/storage, all depending on the attacker model (ranging from malicious insider, to random faults, or honest but curious observer).

In this setting, performing a private set union (PSU), for instance, allows one party, and only one, to learn the union of its set to that of another party, while keeping the intersection secret. Several methods for PSU were developed in recent years [5, 8, 14] using techniques such as Linear or Fully Homomorphic Encryption, Oblivious Transfer or Oblivious Key-Value Stores, etc. We want to investigate in this work the "fuzzy" or "structure-aware" case were one wants to decide whether an element is in a neighborhood of the elements of the other set. This is crucial to be able to handle for instance variants of alerts or vulnerabilities. Both the theoretical and practical aspects are important in order to design efficient solutions.

The Fuzzy Private Set Union (FPSU) problem [7, 13] is a recent research topic that builds upon the Fuzzy Private Set Intersection (FPSI) setting [10]. The first goal of this internship is to investigate how the approaches proposed in [7] can be efficiently implemented in practice. More specifically, these approaches combine several cryptographic building blocks, including Oblivious Key-Value Stores (OKVS) [11] and Private Information Retrieval (PIR) [2], together with linearly or fully homomorphic encryption schemes. A key challenge is to carefully design and tune the interaction between these building blocks in order to minimize the number of communication rounds, as well as the overall computational and communication costs.

Second, the idea will be to design new methods for the fuzzy case that could take advantage of different trade-offs and algebraic structures, in order to support static or iterative unions, and various security, privacy and attacker models (honest but curious, malicious, etc.).

This master project can lead to a PhD project on further secure multi-party computing protocols, for instance to compute the private set difference, private membership test, or more generally to be able to efficiently update existing private set settings [6, 1], as well as introducing proven verifiability of the protocols in the malicious setting [4, 9, 12].

References

[1] A. Agarwal, D. Cash, M. George, S. Kamara, T. Moataz, and J. Singh. Updatable Private Set Intersection from Structured Encryption. *IACR Communications in Cryptology*, 2(4):cc2–4–48, Jan. 2026.

URL: https://cic.iacr.org/p/2/4/25, doi:10.62056/av4fsgbmo.

[2] S. Angel, H. Chen, K. Laine, and S. Setty. Pir with compressed queries and amortized computation. In *IEEE Symposium on Security and Privacy, S &P (Oakland) 2018*, April 2018. URL: https://www.microsoft.com/en-us/research/publication/pir-compressed-queries-amortized-computation/.

[3] M. Bellare, R. Ranjan, D. Riepel, and A. Aldakheel. The concrete security of two-party computation: Simple definitions, and tight proofs for PSI and oprfs. In K. Chung and Y. Sasaki, editors, *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part VI*, volume 15489 of *Lecture Notes in Computer Science*, pages 328–362. Springer, 2024. doi:10.1007/978-981-96-0938-3_11.

[4] S. Bettaieb, L. Bidoux, O. Blazy, B. Cottier, and D. Pointcheval. Secure decision forest evaluation. In *ARES 2021: The 16th International Conference on Availability, Reliability and Security, all digital, August 17–20, 2021*. ACM, 2021. doi:10.1145/3465481.3465763.

[5] A. Davidson and C. Cid. An Efficient Toolkit for Computing Private Set Operations. In J. Pieprzyk and S. Suriadi, editors, *Information Security and Privacy - 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3-5, 2017, Proceedings, Part II*, volume 10343 of *Lecture Notes in Computer Science*, pages 261–278. Springer, 2017. doi:10.1007/978-3-319-59870-3_15.

[6] P. de Perthuis and D. Pointcheval. Two-client inner-product functional encryption with an application to money-laundering detection. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, (CCS'22), page 725–737, New York, NY, USA, 2022. Association for Computing Machinery. doi:10.1145/3548606.3559374.

[7] J. Dumas, A. Maignan, and L. Soezima. Fuzzy private set union via oblivious key homomorphic encryption retrieval. *CoRR*, abs/2601.20400, 2026. URL: https://doi.org/10.48550/arXiv.2601.20400, arXiv:2601.20400, doi:10.48550/ARXIV.2601.20400.

[8] J.-G. Dumas, A. Galan, B. Grenet, A. Maignan, and D. S. Roche. Communication optimal unbalanced private set union. In M. Fischlin and V. Moonsamy, editors, *23rd International Conference on Applied Cryptography and Network Security (ACNS'25)*, pages 107–135, Munich, Germany, July 2025. URL: https://hal.science/hal-04475604, doi:10.1007/978-3-031-95764-2_5.

[9] J.-G. Dumas, A. Maignan, C. Pernet, and D. S. Roche. VESPo: Verified evaluation of secret polynomials: with application to low-storage dynamic proofs of retrievability. In *23rd Privacy Enhancing Technologies Symposium (PETS'23)*, number 3, pages 354–374, Lausanne, Switzerland, Oct. 2023. URL: https://hal.science/hal-03365854, doi:10.56553/popets-2023-0085.

[10] G. Garimella, B. Goff, and P. Miao. Computation Efficient Structure-Aware PSI from Incremental Function Secret Sharing. In L. Reyzin and D. Stebila, editors, *Advances in Cryptology – CRYPTO 2024*, volume 14927, pages 309–345. Springer Nature Switzerland, Cham, 2024. Series Title: Lecture Notes in Computer Science. doi:10.1007/978-3-031-68397-8_10.

[11] G. Garimella, B. Pinkas, M. Rosulek, N. Trieu, and A. Yanai. Oblivious key-value stores and amplification for private set intersection. *IACR Cryptol. ePrint Arch.*, 2021:883, 2021. URL: https://api.semanticscholar.org/CorpusID:235691899.

[12] C. Knabenhans, A. Viand, A. Merino-Gallardo, and A. Hithnawi. vfhe: Verifiable fully homomorphic encryption. In *Proceedings of the 12th Workshop on Encrypted Computing & Applied Homomorphic Cryptography*, (WAHC'24), page 11–22, New York, NY, USA, 2024. Association for Computing Machinery. doi:10.1145/3689945.3694806.

[13] Q. Liu, J. Bae, H. T. Lee, and J.-W. Lee. Fuzzy enhanced private set union in hamming and minkowski spaces. Cryptology ePrint Archive, Paper 2026/166, 2026. URL: https://eprint.iacr.org/2026/166.

[14] S. Pu, J. Gao, and N. Trieu. Malicious Private Set Union with Two-Sided Output. In *EUROCRYPT 2026*, 2026. doi:10.1007/978-3-032-25317-0_14.