Security and Privacy of Dynamic Multi-party Computations

Jean-Guillaume Dumas and Aude Maignan

November 7, 2025

Secure multi-party computing (SMC) is a subfield of cryptography with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private.

For instance, consider two security agencies that wish to compare their lists of suspects without revealing their contents or an airline company that would like to check its list of passengers against the list of people that are not allowed to go abroad.

Another example is decentralized storage, emerging as an appealing alternative to commercial cloud storage. It consists of a peer-to-peer network that anyone can join to store and serve data for others. They rely on a general-purpose blockchain to serve as an unbiased public auditor. The challenge there is to combine trustless assumptions, privacy and heterogeneous ressources.

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 the attacker model (ranging from malicious insider, to random faults, or honest but curious observer).

The functionalities of interest thus include oblivious polynomial evaluation but also secure equality of strings, set membership, proof of data possession and more.

More precisely, in this internship we want to address *dynamicity* in the securisation of multi-party computations:

- How can the protocols efficiently take into account modifications when dynamic updates are possible, without requiring a full reset of the protocol? Protocols like secret polynomial evaluation and secret dot-products are the initial building blocks to target [7, 6, 2, 8, 5].
- How to adapt the protocols to peer-to-peer setting and players with different assumptions and rights [4, 3]?
- Overall, how to construct SMC protocols which take into account the static or dynamic cooperation graph (or social graph) between players while preventing security breaches, preserving privacy and adapting to multiple complexity measures [10]?

To address this research questions the proposed methodology is to first focus on algebraic problems involving polynomial arithmetic and linear algebra. The main tools are secret sharing techniques and homomorphic cryptography and verifiable fully homomorphic encryption [9] and those need to be adapted to efficiently take into account modifications of the assumptions during the protocols. Then the developed building blocks will be declined to give more efficient solutions for instance to dynamic proof of retreivability [6] systems for edge storage or decentralized storage networks, or also for private reputation systems or secure evaluation of decision forests [1].

References

[1] 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.

[2] A. Bois, I. Cascudo, D. Fiore, and D. Kim. Flexible and efficient verifiable computation on encrypted data. In J. A. Garay, editor, *24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13*, volume 12711 of *LNCS*, pages 528–558. Springer, 2021. doi:10.1007/978-3-030-75248-4_19.

[3] 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.

[4] H. Duan, Y. Du, L. Zheng, C. Wang, M. H. Au, and Q. Wang. Towards practical auditing of dynamic data in decentralized storage. *IEEE Transactions on Dependable and Secure Computing*, pages 1–1, 2022. doi:10.1109/TDSC.2022.3142611.

[5] 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 2025)*, pages 107–135, Munich, Germany, July 2025. URL: https://hal.science/hal-04475604, doi:10.1007/978-3-031-95764-2_5.

[6] 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 2023)*, number 3, pages 354–374, Lausanne, Switzerland, Oct. 2023. URL: https://hal.archives-ouvertes.fr/hal-03365854, doi:10.56553/popets-2023-0085.

[7] D. Fiore, A. Nitulescu, and D. Pointcheval. Boosting verifiable computation on encrypted data. In A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas, editors, *23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4-7*, volume 12111 of *LNCS*, pages 124–154. Springer, 2020. doi:10.1007/978-3-030-45388-6_5.

[8] M. Izabachène, A. Nitulescu, P. de Perthuis, and D. Pointcheval. Myope: Malicious security for oblivious polynomial evaluation. In *Security and Cryptography for Networks: 13th International Conference, SCN 2022, Amalfi (SA), Italy, September 12–14, 2022, Proceedings*, page 663–686, Berlin, Heidelberg, 2022. Springer-Verlag. doi:10.1007/978-3-031-14791-3_29.

[9] 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.

[10] E. V. Mangipudi, D. Lu, A. Psomas, and A. Kate. Collusion-deterrent threshold information escrow. In *2023 IEEE 36th Computer Security Foundations Symposium (CSF)*, pages 584–599, 2023. doi:10.1109/CSF57540.2023.00010.