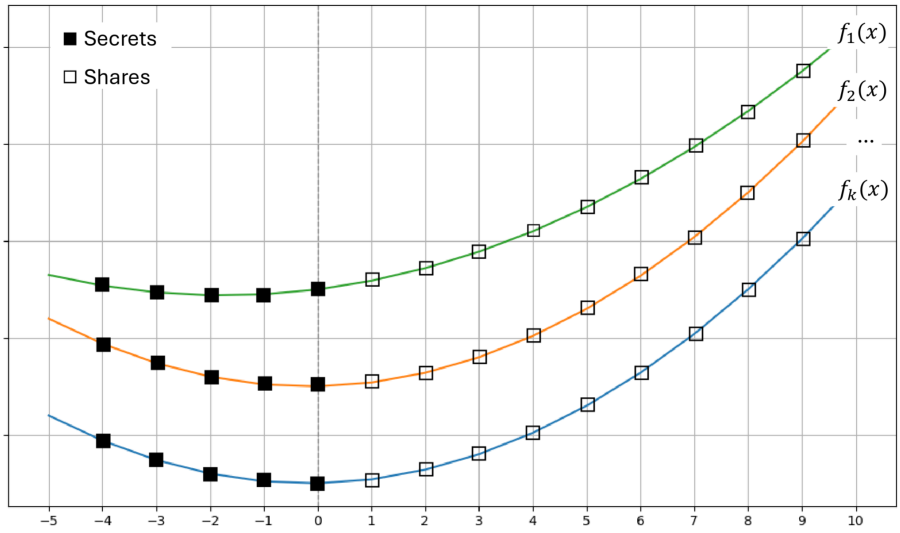
Packed Secret Sharing from Monotone Span Programs



The concept of secret sharing is one with many application across cryptography, not in the least enabling secure and private computation between multiple parties. The basic idea is that a value can be split into multiple pieces, such that individual pieces do not reveal any information, but when enough of them come together (not necessarily all pieces), it becomes possible to reconstruct the original value.

The best known example is *Shamir's Secret Sharing Scheme* [Sha79, link]. This is an example of a *threshold linear secret sharing scheme*, i.e. a secret sharing scheme in which linear operations on the underlying value can be computed over the shares and where the value can be reconstructed as soon as the number of available shares crosses a threshold t. All linear secret sharing schemes can further be cast into the framework of *Monotone Span Programs* [KW93, link], introducing support for more general *access structures* beyond the threshold structure. This is often useful for real-world requirements on who should be able to reconstruct a secret.

On top of Shamir's scheme, a *packed* version of secret sharing has been proposed [FY92, link] and used in several practical applications such as Secure Multiparty Computation [GPS22, link] and Verifiable Secret Sharing [ABN$^+$25, link]. However, it comes at a cost of reducing the threshold for privacy, while not changing the threshold for reconstruction.

The goal of this thesis is to work towards a clean and generalized framework for packed secret sharing, starting from a viewpoint of monotone span programs. In such a framework, it would then be possible to recast the existing constructions of packed secret sharing, without losing security or functionality.

Practicalities

Promotor:	Bart Preneel		
Daily supervisor:	Barry Van Leeuwen	barry.vanleeuwen@kuleuven.be	office B01.19
	Robin Jadoul	robin.jadoul@esat.kuleuven.be	
Nature of the work:	40% literature, 60% theoretical work		
Number of students:	1		
Requirements:	Algebra Linear algebra		

[ABN+25] Shahla Atapoor, Karim Baghery, Georgio Nicolas, Robi Pedersen, and Jannik Spiessens. Batched and packed (publicly) verifiable secret sharing: A unified framework and applications. Cryptology ePrint Archive, Paper 2025/2018, 2025.

[FY92] Matthew Franklin and Moti Yung. Communication complexity of secure computation (extended abstract). In *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing*, STOC '92, page 699–710, New York, NY, USA, 1992. Association for Computing Machinery.

[GPS22] Vipul Goyal, Antigoni Polychroniadou, and Yifan Song. Sharing transformation and dishonest majority mpc with packed secret sharing. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*, pages 3–32, Cham, 2022. Springer Nature Switzerland.

[KW93] Mauricio Karchmer and Avi Wigderson. On span programs. In *[1993] Proceedings of the Eigth Annual Structure in Complexity Theory Conference*, pages 102–111. IEEE, 1993.

[Sha79] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, November 1979.