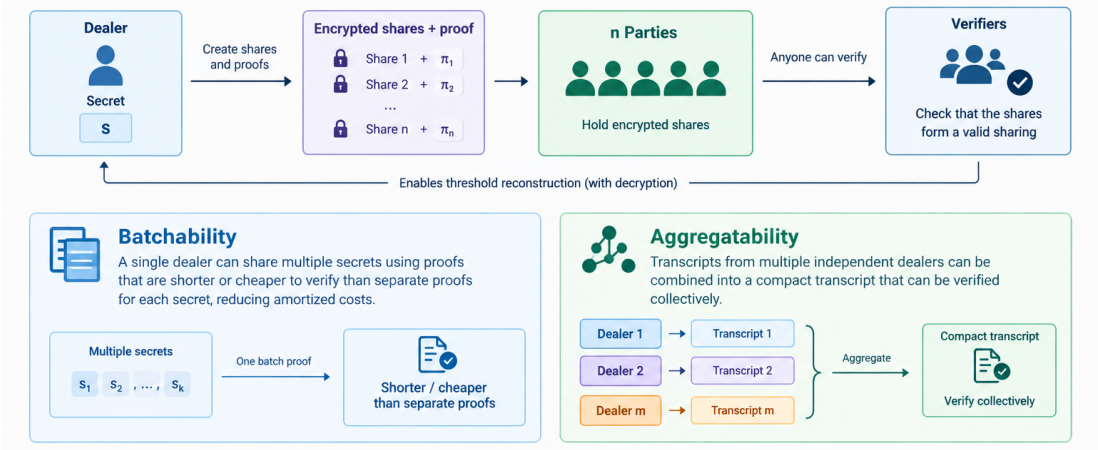
On Aggregatable and Batchable PVSS and Applications



Publicly Verifiable Secret Sharing. Publicly Verifiable Secret Sharing (PVSS) allows a dealer to distribute encrypted shares of a secret among n parties while enabling anyone to verify that they form a valid threshold sharing. PVSS is a fundamental building block for distributed randomness beacons, distributed key generation, threshold cryptography, and secure multiparty computation. Two important efficiency properties of PVSS protocols are *batchability* and *aggregatability*. Batchability allows a single dealer to share multiple secrets using proofs that are shorter or cheaper to verify than separate proofs for each secret, thereby reducing amortized costs. In contrast, aggregatability allows transcripts generated by multiple independent dealers to be combined into a compact transcript that can be verified collectively. These properties are particularly useful in distributed randomness generation: ALBATROSS+ [ABNPS26] exploits batched or packed PVSS, whereas OptRand [BSKN22] uses aggregatable PVSS to combine independent contributions. Existing schemes typically achieve one of these properties, but not both simultaneously. Combining them requires proving the correctness of each dealer's batched sharing while preserving efficient aggregation, verification, decryption, and reconstruction.

Goal. The goal of this thesis is to investigate the construction of PVSS schemes that are simultaneously *batchable* and *aggregatable*. The student will first study existing PVSS constructions and formalize the two properties in a common framework. The thesis will then explore whether existing batchable or aggregatable PVSS schemes can be extended to achieve both properties, and analyze the resulting security, communication complexity, and computational costs. Finally, the thesis will study applications of the resulting techniques. Ideally, at least one promising construction or application will be implemented and experimentally compared with current protocols.

Practicalities

Promotor:	Bart Preneel		
Daily supervisor:	Karim Baghery	karim.baghery@kuleuven.be	office B01.26
	Hossein Moghaddas	hossein.moghaddas@kuleuven.be	office B01.26
Nature of the work:	25% literature, 45% theoretical work, 30% software		
Number of students:	1		