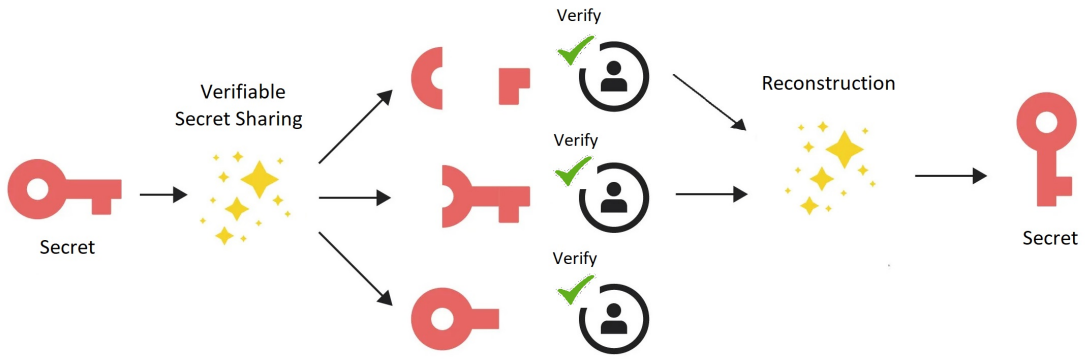
On Lattice-Based Publicly Verifiable Secret Sharing



Publicly Verifiable Secret Sharing. Secret sharing is a fundamental cryptographic technique that distributes a secret among multiple participants such that only a threshold subset can jointly reconstruct it. Verifiable Secret Sharing (VSS) strengthens this model by enabling participants to verify the correctness of their shares, ensuring the dealer distributed them honestly. Publicly Verifiable Secret Sharing (PVSS) extends this further by allowing anyone –not just the participants– to verify the correctness of the distribution, making it a key primitive in decentralized systems like threshold signatures, distributed key generation, and committee-based consensus [Sch99, CD17, BKNR25]. In [GHL22], Gentry, Halevi, and Lyubashevsky proposed a PVSS scheme that supports large-scale protocols. More recently, Baghery, Knapen, Nicolas, Rahimi [BKNR25] introduced the notion of Pre-constructed PVSS (PPVSS), which enriches standard PVSS with additional features and has been shown to be more practical and versatile.

Goal. The primary objective of this internship is to design a lattice-based Pre-constructed Publicly Verifiable Secret Sharing (PPVSS) scheme, with the aim of exploring how pre-constructability can enhance both efficiency and usability. In the second phase, the resulting PPVSS construction may be leveraged to revisit existing cryptographic protocols, with the goal of improving their efficiency and, potentially, enabling the design of new protocols.

Practicalities

Supervisors:	Karim Baghery	karim.baghery@kuleuven.be	office B01.26
	Hossein Moghaddas	hossein.moghaddas@kuleuven.be	office B01.26

Nature of the work: 30% literature, 40% theoretical work, 30% software
Number of students: 1

 © 2025-2026 COSIC