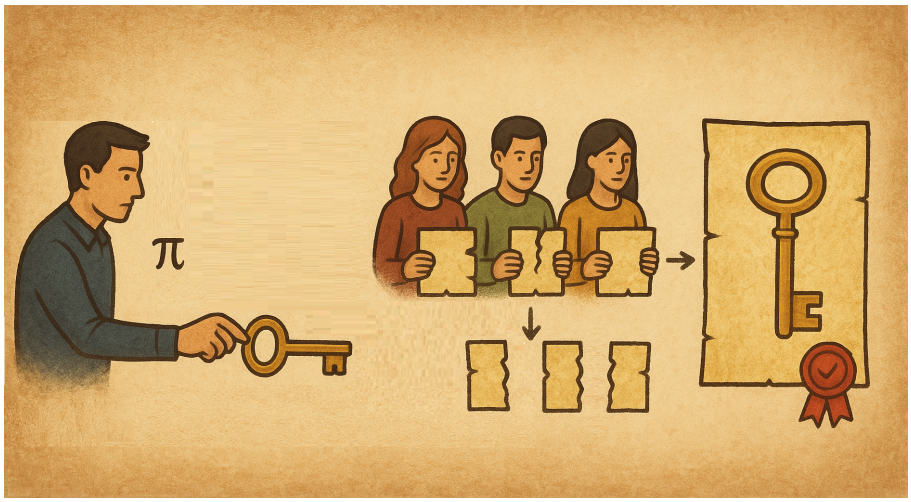
On Pre-Constructed PVSS Over Class Groups and Applications



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 [CD24], Cascudo and David proposed a PVSS scheme over class groups that achieves similar efficiency to state-of-the art schemes that only allow for reconstructing a *function* of the secret, e.g., [Sch99, CD17, Bag25], while their scheme allows the reconstruction of the original secret. More recently, Baghery, Knapen, Nicolas, Rahimi [BKNR25] introduced the notion of Pre-constructed PVSS (PPVSS), which extends standard PVSS schemes with additional features and has been shown to be more practical and versatile.

Goal. The primary objective of this thesis is to design a Pre-constructed PVSS (PPVSS) variant of Cascudo and David's PVSS scheme over class groups, with the aim of investigating how pre-constructability can improve both efficiency and usability. In the second phase, the developed PPVSS construction might be applied to revisit existing cryptographic protocols, like distributed key generation with the goal of enhancing their efficiency or even proposing new protocol designs.

Practicalities

Promotor:	Bart Preneel		
Daily supervisor:	Karim Baghery	karim.baghery@kuleuven.be	office B01.26
	Mahdi Rahimi	mahdi.rahimi@kuleuven.be	office B01.27
	Shahla Atapoor	shahla.atapoor@kuleuven.be	office B01.25
Nature of the work:	30% literature, 40% theoretical work, 30% software		
Number of students:	1		

 © 2026 – 2027 COSIC