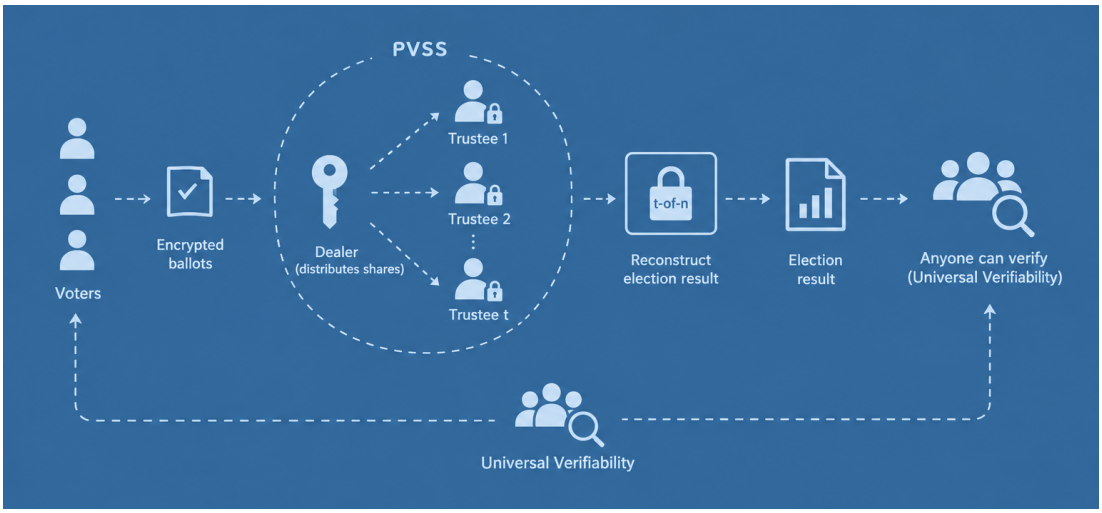
On Universally Verifiable E-Voting Based on PVSS



Universally Verifiable E-Voting. Electronic voting protocols aim to provide secure and privacy-preserving elections while allowing the correctness of the election result to be verified. An important property is *universal verifiability*, which enables any external observer, rather than only voters or election authorities, to verify that all valid ballots were correctly processed and that the announced result follows from the published election transcript. Publicly Verifiable Secret Sharing (PVSS) provides a natural tool for constructing universally verifiable e-voting protocols [Sch99]. PVSS allows a dealer to distribute encrypted shares of a secret among a set of trustees while enabling anyone to verify that the shares form a valid threshold sharing. In a PVSS-based e-voting protocol, votes or election-related secret values can be distributed among several trustees and reconstructed only when a sufficiently large qualified set cooperates. The public verifiability of the sharing and reconstruction procedures can then contribute directly to the universal verifiability of the election. Recent work has proposed more efficient universally verifiable e-voting protocols based on PVSS [BKNR25]. Nevertheless, the performance of these protocols remains strongly influenced by the communication and computational costs of the underlying PVSS scheme, particularly when many votes or election instances must be processed.

Goal. The goal of this thesis is to investigate the use of state-of-the-art batched and packed PVSS schemes [ABNPS26] to improve the efficiency of universally verifiable e-voting. The student will first study existing PVSS-based e-voting protocols and relevant batched and packed PVSS constructions. Based on this study, the student will design more efficient e-voting protocols and analyze their security and performance. At least one of the proposed constructions will be implemented and experimentally compared with existing state-of-the-art protocols.

Practicalities

Promotor:	Bart Preneel		
Daily supervisors:	Karim Baghery	karim.baghery@kuleuven.be	office B01.26
	Shahla Atapoor	shahla.atapoor@kuleuven.be	office B01.25
	Hossein Moghaddas	hossein.moghaddas@kuleuven.be	office B01.26
Nature of the work:	30% literature, 40% theoretical work, 30% software		
Number of students:	1		

 © 2026–2027 COSIC