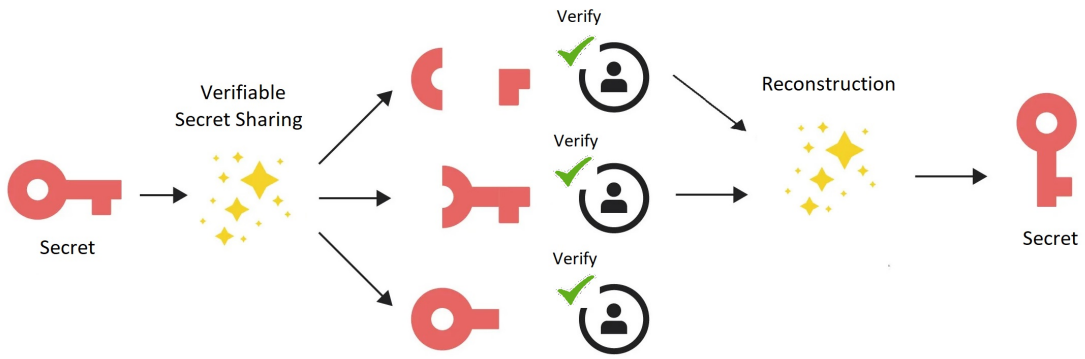
Over Publiek Verifieerbare Geheime Deling op Basis van Roosters



Publiek verifieerbare geheime deling. Geheime deling is een fundamentele cryptografische techniek waarbij een geheim wordt verdeeld onder meerdere deelnemers, zodanig dat enkel een drempelsubset het gezamenlijk kan reconstrueren. Verifieerbare geheime deling (Verifiable Secret Sharing, VSS) versterkt dit model door deelnemers in staat te stellen de correctheid van hun aandelen te verifiëren, waardoor wordt gegarandeerd dat de dealer deze eerlijk heeft verdeeld. Publiek verifieerbare geheime deling (Publicly Verifiable Secret Sharing, PVSS) breidt dit verder uit door iedereen — niet enkel de deelnemers — toe te laten de correctheid van de verdeling te controleren, wat het tot een belangrijke bouwsteen maakt in gedecentraliseerde systemen zoals drempelhandtekeningen, gedistribueerde sleutelgeneratie en consensusmechanismen gebaseerd op commissies [Sch99, CD17, BKNR25].

In [GHL22] stelden Gentry, Halevi en Lyubashevsky een PVSS-schema voor dat grootschalige protocollen ondersteunt. Recente resultaten van Baghery, Knapen, Nicolas en Rahimi [BKNR25] introduceerden het concept van Pre-constructed PVSS (PPVSS), dat standaard PVSS verrijkt met bijkomende eigenschappen en waarvan is aangetoond dat het praktischer en veelzijdiger is.

Doel. Het hoofddoel van deze stage is het ontwerpen van een roostergebaseerd Pre-constructed Publiek Verifieerbaar Geheime-Deling-schema (PPVSS), met als doel te onderzoeken hoe pre-constructie zowel de efficiëntie als de bruikbaarheid kan verbeteren. In een tweede fase kan de ontwikkelde PPVSS-constructie worden gebruikt om bestaande cryptografische protocollen opnieuw te bestuderen, met als doel hun efficiëntie te verhogen en mogelijk nieuwe protocolontwerpen mogelijk te maken.

Practische informatie

Begeleiding:	Karim Baghery	karim.baghery@kuleuven.be	kantoor B01.26
	Hossein Moghaddas	hossein.moghaddas@kuleuven.be	kantoor B01.26
Aard van het werk:	30% literatuur, 40% theoretisch werk, 30% software		
Aantal studenten:	1		

 © 2025-2026 COSIC