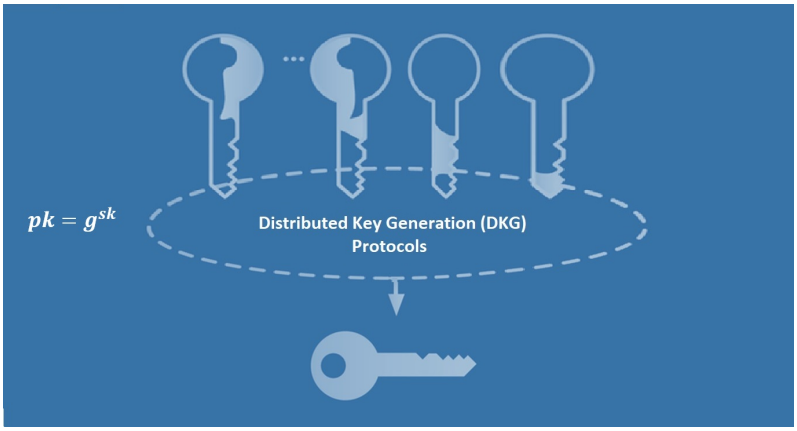
Batched Distributed Key Generation for Discrete Logarithm



Distributed Key Generation (DKG) Protocols. In the landscape of threshold cryptography, a Distributed Key Generation (DKG) protocol holds a critical role. A DKG protocol allows a set of parties to sample a pair of public and secret keys in a fully distributed manner. Upon the completion of the protocol, all parties obtain the public key, while each party receives a share of the secret key. A *robust* DKG protocol goes a step further by guaranteeing the successful generation of the key pair, even in the face of malicious parties attempting to disrupt the process. In the Discrete Logarithm (DL) setting, Pedersen's robust DKG protocol, as introduced by Pedersen in [Ped91], stands as one of the most widely recognized constructions, extensively used in various threshold protocols. In a study by Gennaro, Jarecki, Krawczyk, and Rabin in [GJKR07], authors presented a variation of Pedersen's DKG protocol that ensures the uniformly random distribution of generated keys. In Pedersen's DKG protocol [Ped91], the computational cost for each participating party is dominated by $O(nt)$ exponentiations, where n denotes the number of parties and $t \approx n/2$ is the threshold parameter. Recently, Baghery and Moghaddas [BM26] revisited fully secure DKG protocols in the DL setting and proposed more efficient constructions. Their protocols reduce the number of exponentiations required per party to $O(n)$.

Goal. The goal of this thesis is to extend the recently proposed efficient DKG protocols of Baghery and Moghaddas [BM26] to the *batched setting*. Specifically, the thesis will design batched variants that allow the generation of k independent public/secret key pairs within a single protocol execution, reducing the amortized computational and communication costs compared to running the protocol k times independently. The thesis will also include an implementation of (at least one of) the proposed protocols and an experimental evaluation comparing the performance of the batched and non-batched versions. Finally, potential applications and possible improvements of the proposed constructions will be explored.

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:	20% literature, 40% theoretical work, 40% software		
Number of students:	1		

 © 2026 – 2027 COSIC