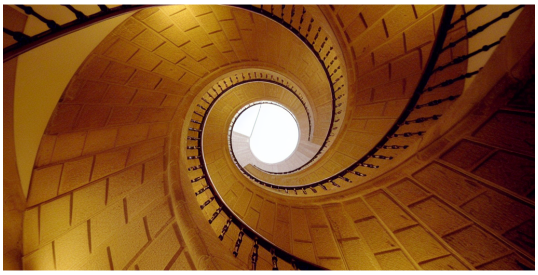
Quantum Information in Spain ICE-8



Contribution ID: **96** Type: **Poster**

A zk-SNARK Scheme for Quantum Computers

The cryptographic primitive zk-SNARK allows users to prove knowledge of something without revealing its exact value. Using a secret value W (”witness”) and a public value X, a zk-SNARK π can be generated such that anyone who only knows π and X can be sure that the prover must know W. As zero-knowledge proofs, zk-SNARKs meet the requirements of Completeness, Soundness and Zero Knowledge. Zk-SNARKs are particularly useful in decentralized environments where privacy is essential, such as verifiable voting systems, multipart computation or anonymous authentication.

The creation of a zk-SNARK scheme involves performing transformations to an algorithm with the objective of being able to prove that it has been successfully computed. However, generation of zk-SNARKs is a notoriously inefficient task. Proof generation time scales poorly with the complexity of the algorithm, and while keeping proof size and validation time small is considered a priority, not all zk-SNARK schemes are able to accomplish that requirement.

Quantum computers are currently becoming a reality, and their unprecedented processing power could solve the inefficiency problem presented by the current state of zk-SNARK schemes. This work aims to study the possibility of creating a zk-SNARK scheme using quantum circuits, such that zk-SNARKs can be generated and validated by quantum computers.

A zk-SNARK scheme for quantum computers could substantially increase the efficiency of the proof generation and validation operations, enhancing the security of classical communications. Furthermore, since quantum channels and QKD are creating a new generation of networks and security protocols, zk-SNARKs could become an useful tool for developing more secure systems.

Though zk-SNARKs are not always post-quantum secure, schemes that circumvent this issue (by using lattice-based cryptography or removing the trusted-setup phase) have been proposed. Nevertheless, there are no studies on using quantum technology in favour of zk-SNARKs to the best of the authors’ knowledge.

Author: SOLER GARCIA, David

Co-authors: Mrs FERNÁNDEZ VILAS, Ana (AtlanTTic); Mr DAFONTE VÁZQUEZ, Carlos (Universidade da Coruña); Mr NÓVOA DE MANUEL, Francisco (Universidade da Coruña); Mr FERNÁNDEZ VEIGA, Manuel (AtlanTTic)

Presenter: SOLER GARCIA, David