

PROJECT / Quantum Security

QSec

Main Objective:

The main goal of the project is to address and tackle some of the most challenging open problems in the area of quantum security. Significant original results are expected in several fronts, such as: design and analysis of quantum protocols, model checking of quantum systems, quantum cryptanalysis of classical protocols, quantum solutions to classical impossibilities. Several applications will be investigated with the purpose of understating how they can be speed up using quantum information. The focus will be on cryptographic tasks, such as zero knowledge proof systems, e-voting, authentication and contract signing. A model-checking tool for quantum systems will be produced within the project, as well as a simulator for testing quantum attacks on symmetric cryptosystems.

Reference: PTDC/EIA/67661/2006 , Funding: FCT/PTDC, Start Date: 01-11-2007

Team: [Paulo Alexandre Carreira Mateus](#), João Filipe Quintas dos Santos Rasga, Amílcar dos Santos Costa Sernadas, [Filipe Alexandre Pedra Aguiar de Moura](#), [Nikola Paunkovic](#), [Pedro Miguel dos Santos Alves Madeira Adão](#), Pedro Alexandre Cardoso Baltazar

Local Coordinator: [Paulo Alexandre Carreira Mateus](#)
