Call 2019

eDict

Experimentally-oriented Device Independent CrypTography

Marcin Pawłowski

PROJECT PROGRESS (highlights)

- **CHALLENGE** – quantum cryptography **in principle** offers security much higher than its classical counterpart but **in practice** problems with implementation make it much less
- **SOLUTION** – use Device Independent Cryptography (DIC) that is immune to implementation level atatcks and problems
- **IMPLEMENTATION** – we developed new tests of nonclassicality which form the basis of DIC, that make it more feasible and novel methods fro security analysis
- **HURDLES –** we did it all in Covid times

IMPACT (RRI aspects)

PUBLIC ENGAGEMENT: we helped to create Quantum Cybersecurity Hub Europe a foundation which propotes awarness of threats and solutions to security stemming from quantum technologies

ETHICS: the whole eDict project is about creating socjety in which every citizen will be able to communicate with their peers without a possibility of any government or company eavesdropping on their exchange

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731473.