Physic - Engineering sciences - TICS / Electronics and safety - TICS - Financial business services

RELATIVISTIC QUANTUM CRYPTOGRAPHY

Spacetime-constrained oblivious transfer (SCOT) is a cryptographic task extending one-out-of-m oblivious transfer (OT) by guaranteeing security from quantum physics and relativistic signalling constraints.

PRESENTATION

SCOT is performed by two mistrustful parties, Alice and Bob. Alice inputs secret messages and Bob obtains a message of his choice in a first spacetime region, i.e. , at a particular location and at a particular time. The security conditions are : Alice must be oblivious to Bob's chosen message, and Bob must be oblivious to the other messages of Alice in spacetime regions that are spacelike separated from the first spacetime region. This technology provides methods and systems to implement unconditionally secure SCOT based on quantum physics and the principle of no-superluminal signalling of special relativity, evading Lo's no-go theorem for one-out-of-m OT.

Quantum cryptography - Relativistic quantum cryptography - Oblivious transfer

APPLICATIONS

- Security of high-speed transactions in financial markets
- Security of privacy-preserving location-based data access
- Secure multi-party computation with spacetime constraints

COMPETITIVE ADVANTAGES

- Unconditional security
- Security based on quantum physics and special relativity
- Evades Lo's no-go theorem for one-out-of-m oblivious transfer
- Practical with current technology

DEVELOPMENT PHASE

- ☑ Although no experimental demonstration of SCOT has been performed, the technology required to implement it is already available
- ☑ TRL 3 to 4

INTELLECTUAL PROPERTY

Two patent applications filed (US 2018/0287788 A1, EP3777008A1)

PUBLICATIONS

- D. Pitalúa-García, "Spacetime-constrained oblivious transfer", Physical Review A 93, 062346 (2016).
- D. Pitalúa-García and I. Kerenidis, "Practical and unconditionally secure spacetime-constrained oblivious transfer", Physical Review A 98, 032327 (2018).
- D.Pitalúa-García, "One-out-of-m spacetime constrained oblivious transfer" Phys. Rev. A 100, 012302 (2019).
- T. Lunghi et al., Experimental bit commitment based on quantum communication and special relativity, Physical Review Letters 111, 180504 (2013).

CONTACT

+33 (0)1 44 23 21 50

industriels@erganeo.com

Ref. project : 438