

System and method for generating a symmetric cryptographic key and random numbers

About the solution

The invention concerns a system and method for generating a symmetric cryptographic key and random numbers designed to secure communication in public infrastructure.

The solution is based on device-independent cryptography and optimized entangled states, enabling certified randomness generation and quantum-resistant symmetric keys.

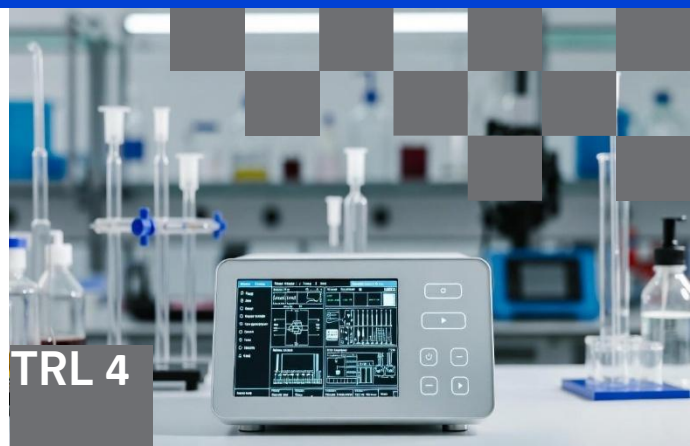
The system increases the operational range of secure key distribution while reducing hardware requirements for end users, maintaining high security even with low detection efficiency.

AIP protection

The invention is protected by the Polish Patent Office under the following number:
Pat.246884

Technology readiness level

TRL 4 – Technology validated in laboratory conditions.



Authors

University of Gdańsk
Prof. Marcin Pawłowski

Quantum Cybersecurity Group
Limited Liability Company
PhD Anubhav Chaturvedi
PhD Giuseppe Viola

Applications

- Secure communication in public infrastructure,
- Telecommunication systems requiring quantum-resistant security,
- Generation of certified keys and random numbers.

Possible cooperation

- Technology licensing and implementation in public institutions,
- Collaboration on integration with existing security systems,
- Joint development and optimization research.