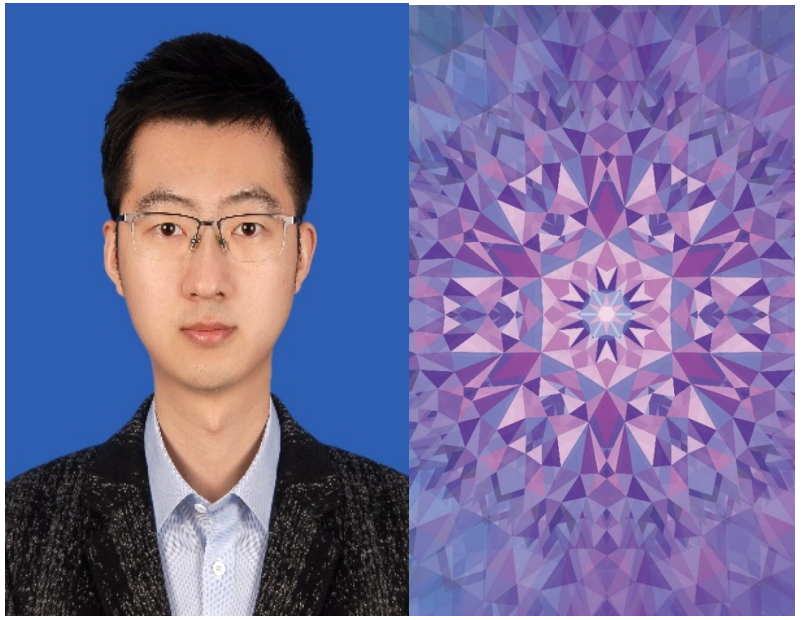
ITU KALEIDOSCOPE ONLINE 2021

6-10 December 2021

Strengthen the security of cyberspace with device-independent quantum randomness

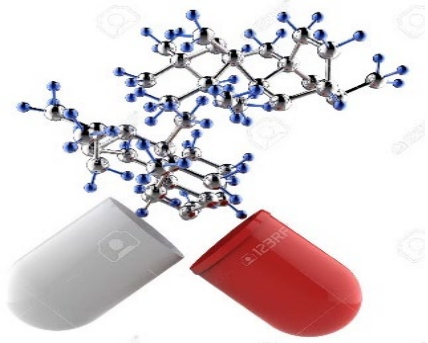
Dr. Ming-Han Li
CAS Quantum Network Co., Ltd. China

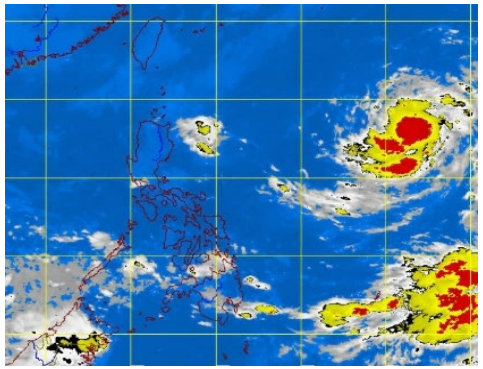


Session 2: Contributions to security

Paper S3.1: Strengthen the security of cyberspace with device-independent quantum randomness

Randomness have a wide range of applications





Numerical simulation required for weather forecasting, new drug development, etc.

Lottery

Cyberspace security

Uniformity **Unpredictability**

randomness

Different kinds of randomness

The principle of generating random numbers

- Classic Randomness

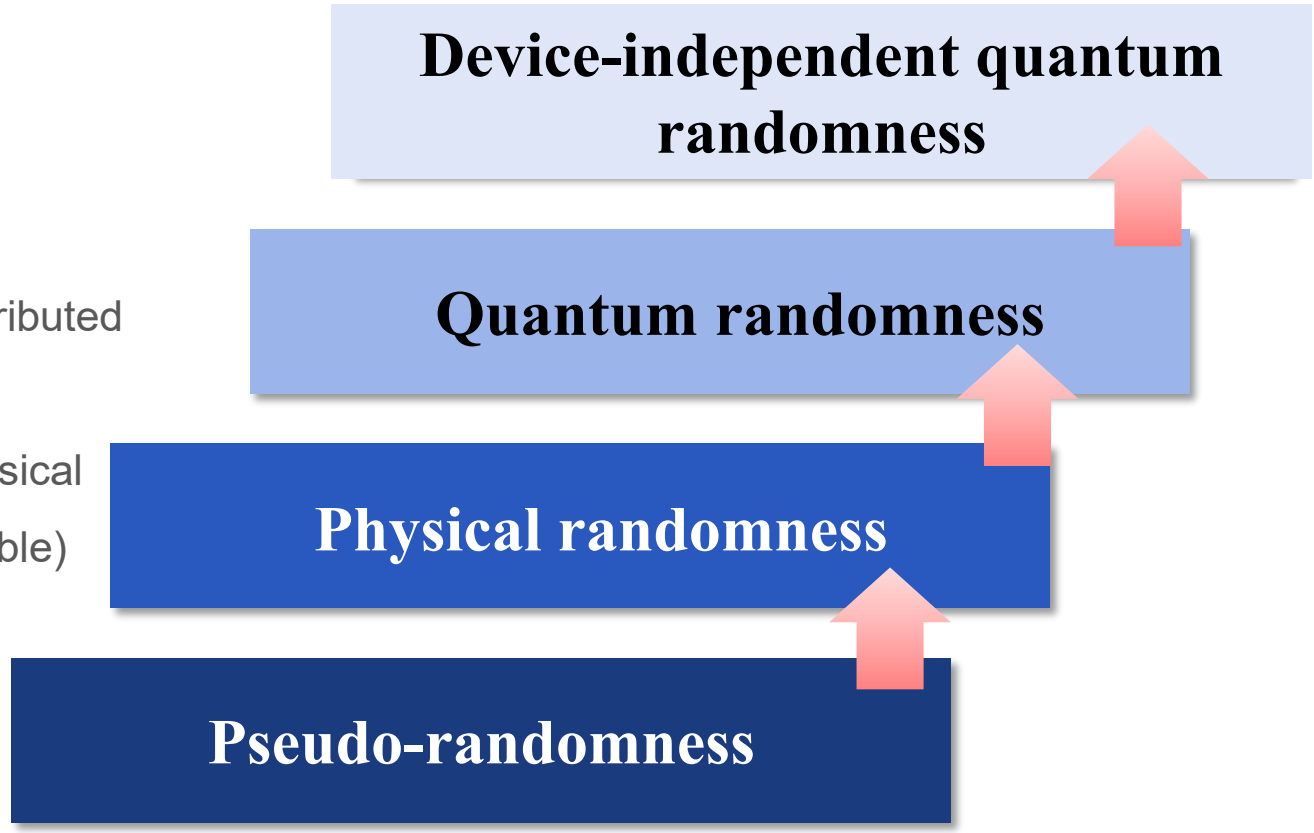
  Intrinsically predictable, uniformly distributed

- Quantum Randomness

  Inherent randomness (un-predicable), uniformly distributed

Practical issues in quantum randomness

- Device imperfections, components deviating, classical noises, side channels, adversary attacks (vulnerable)

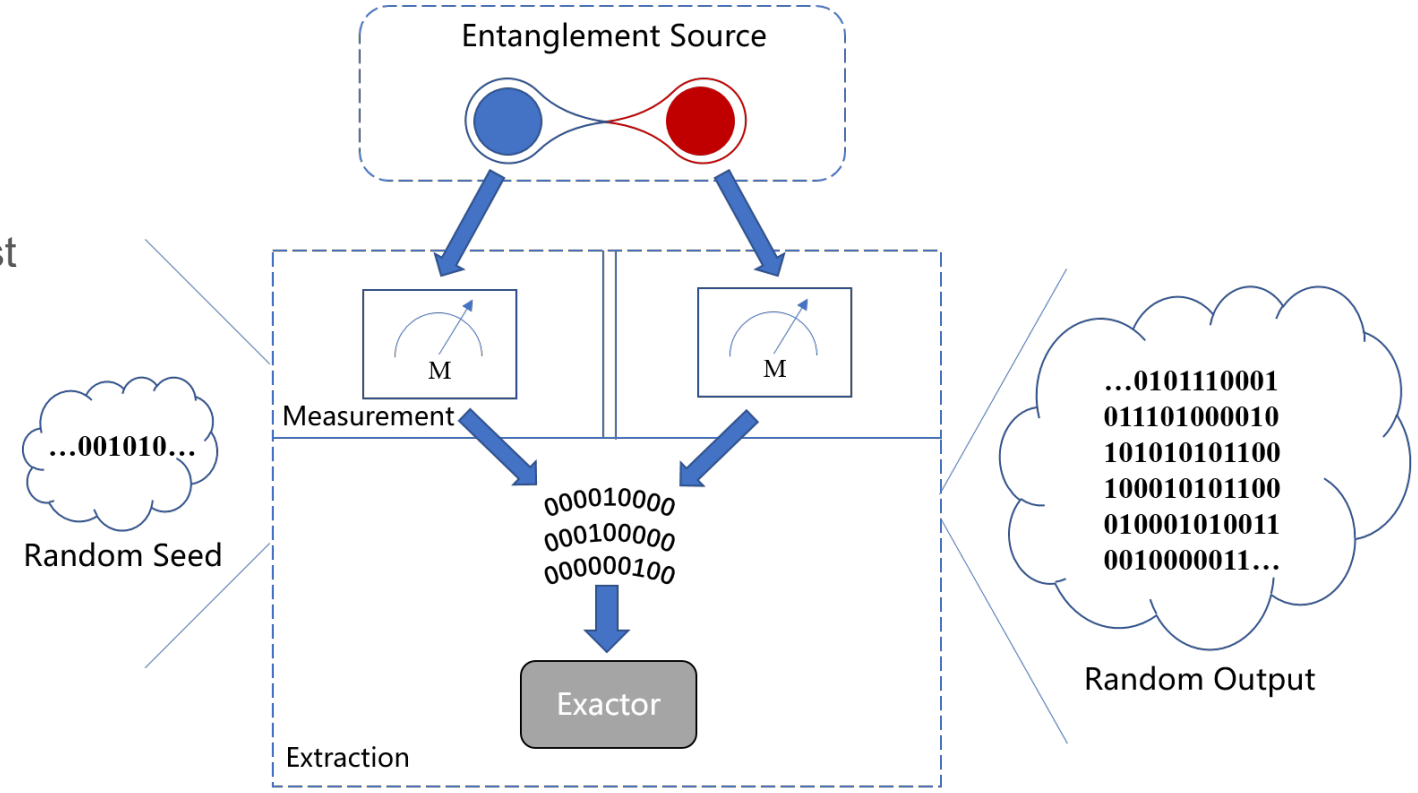


There is a trade-off between security and performance

Principle of Device-independent quantum randomness

Should based on (loophole-free) Bell's inequality test

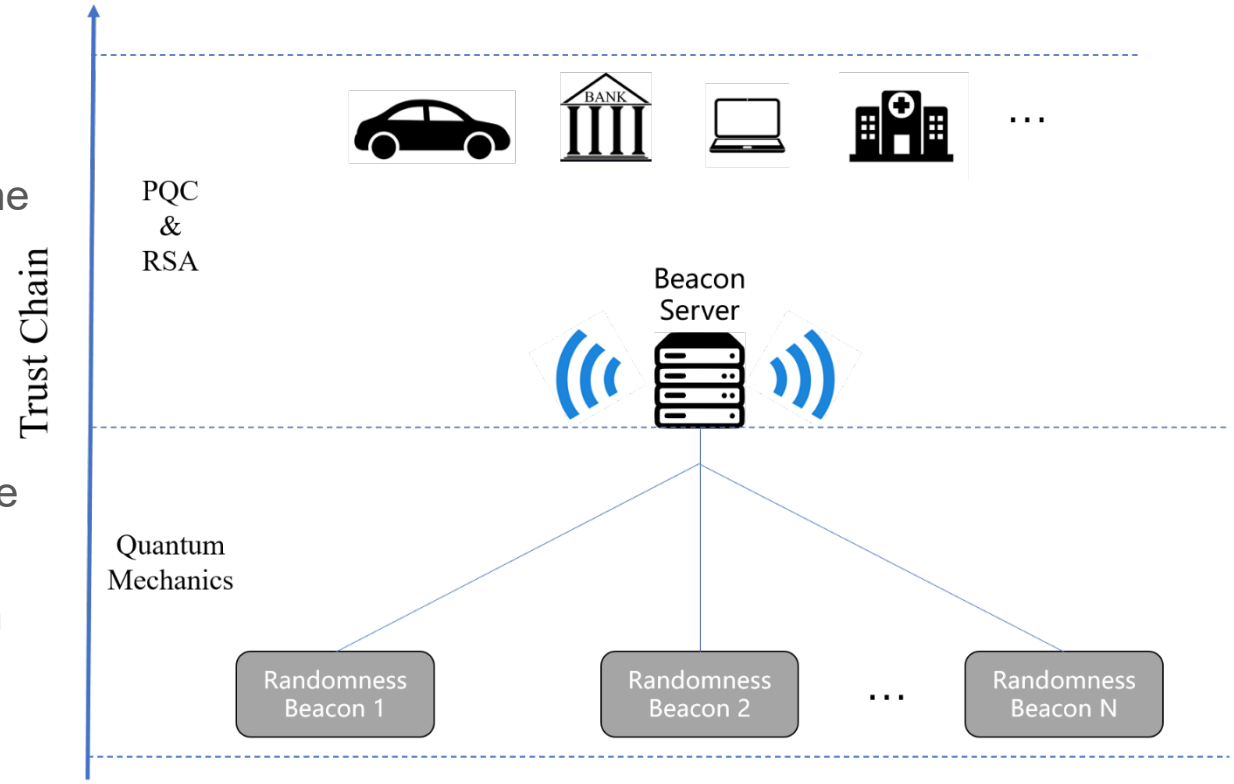
- Close detection loophole
- Prohibit communications between the measurements
- Measurement settings independent of entanglement creation



Randomness beacon

Periodically broadcast random numbers to other locations in the system. As a public service

- Send a random number periodically (1 per minute)
- Each pulse contains a 512-bit random number string
- Each pulse contains index, time stamp and digital signature
- Any past pulses are publicly available
- The pulse sequence before and after forming a hash chain



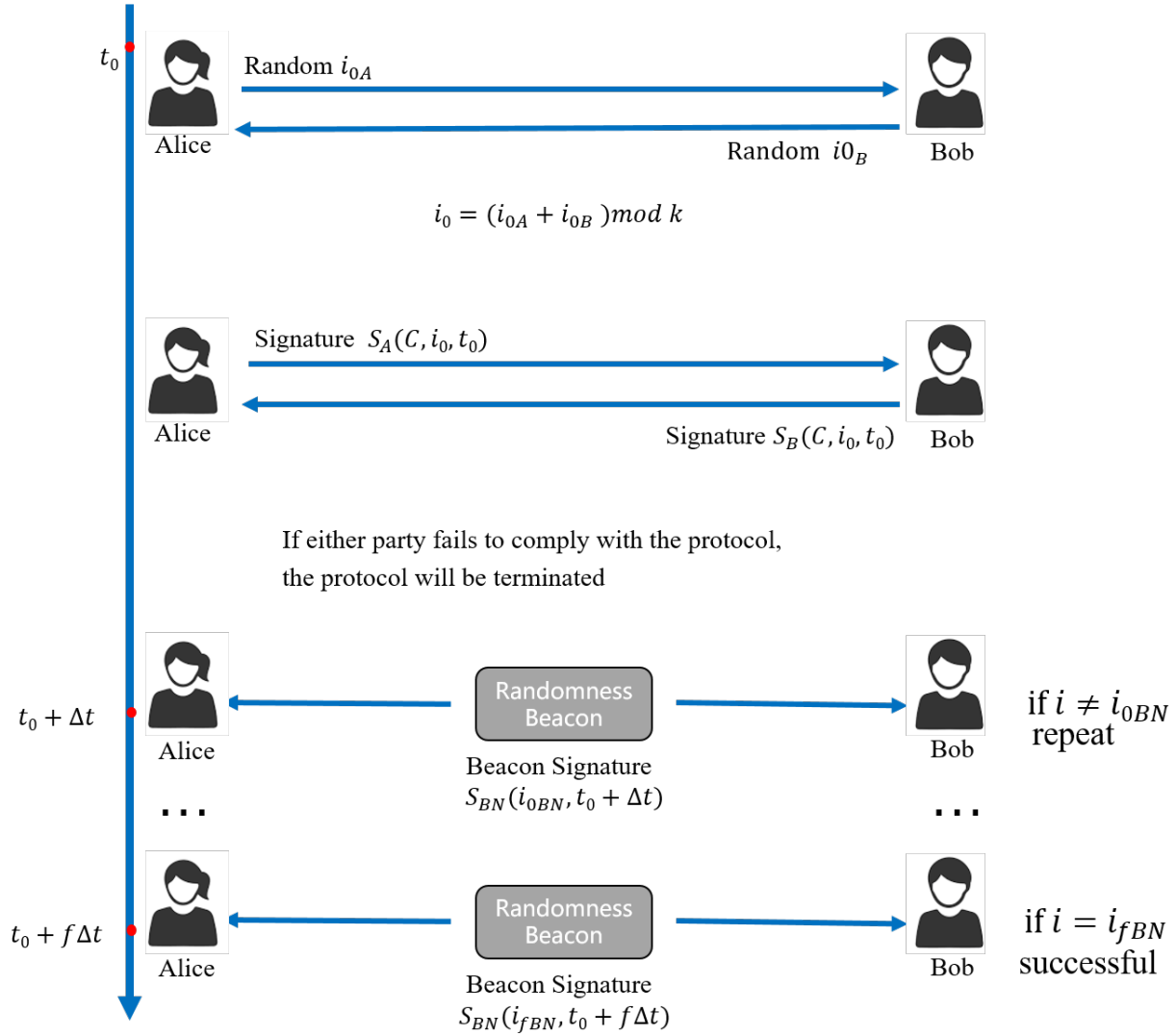
Use case of randomness beacon: Contract signing

Solve the problem of signing the contract by both parties who cannot meet

Ensure the fairness of both parties to the transaction

Contract information will not be disclosed to third parties

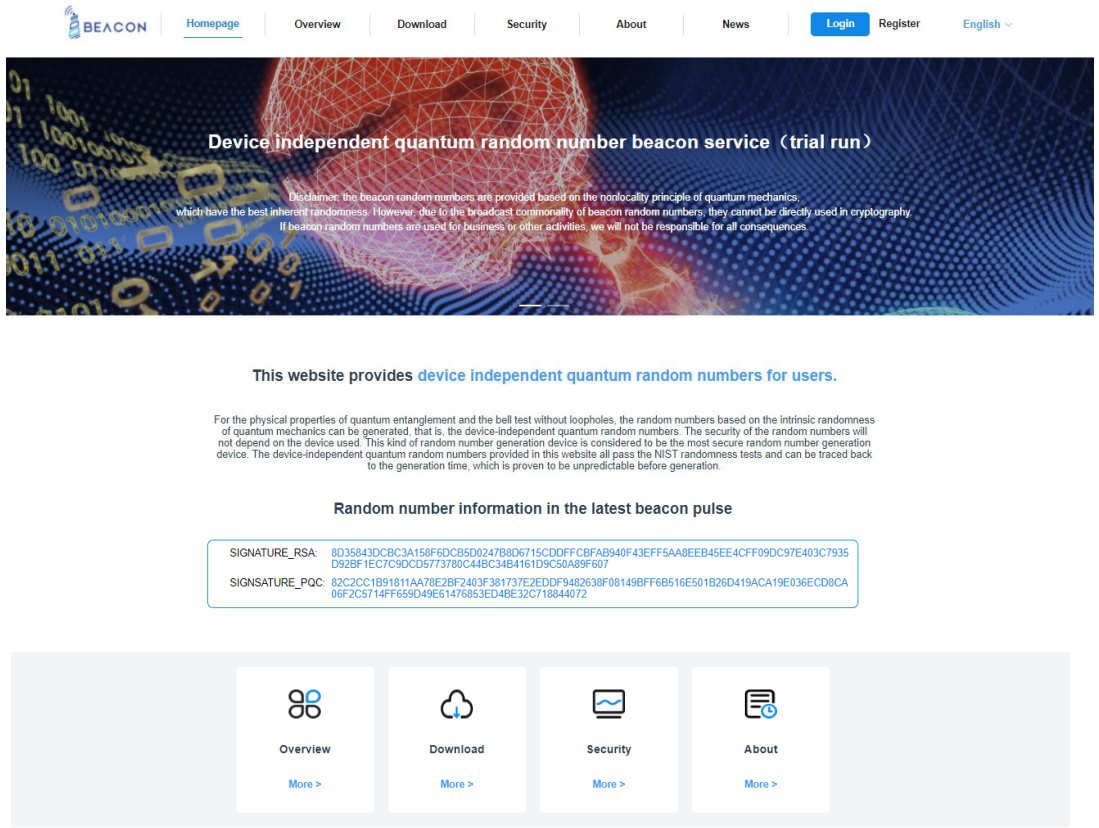
.



Outlook

As a source of quantum randomness, DIQRNG needs to overcome challenges

- How to miniaturize the complex systems
- How to distribute the device-independent randomness to users safely
- How to find more applications for randomness beacon
- …



ITU KALEIDOSCOPE
ONLINE 2021

Thank you!