

ITU KALEIDOSCOPE

ONLINE 2021

6-10 December 2021

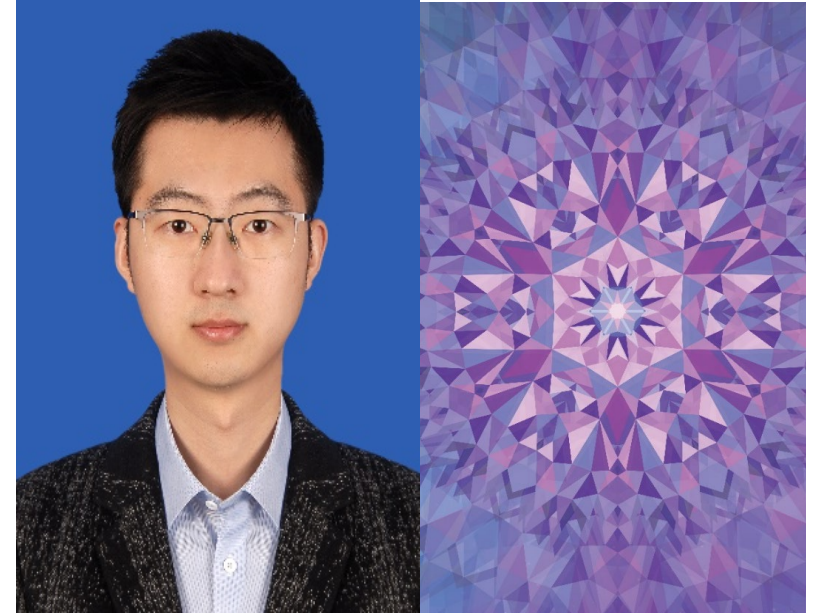
**Strengthen the security of
cyberspace with device-
independent quantum
randomness**

Dr. Ming-Han Li

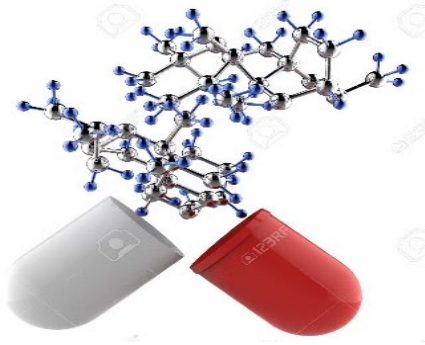
CAS Quantum Network Co., Ltd. China

Session 2: Contributions to security

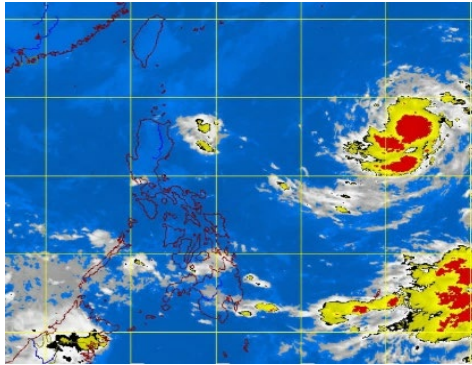
Paper S3.1: Strengthen the security of cyberspace with device-independent quantum randomness



Randomness have a wide range of applications



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



Lottery



Cyberspace security



Uniformity



Unpredictability

randomness

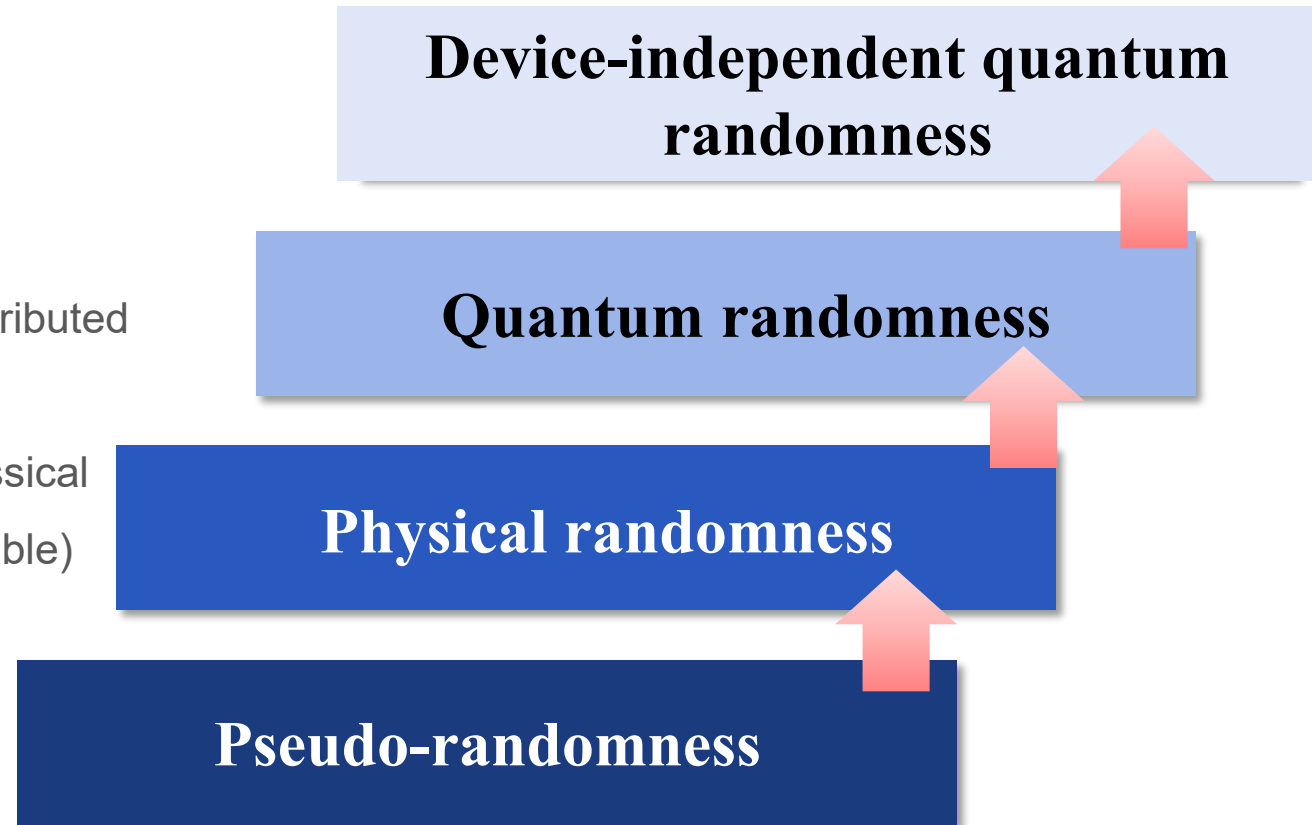
Different kinds of randomness

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)

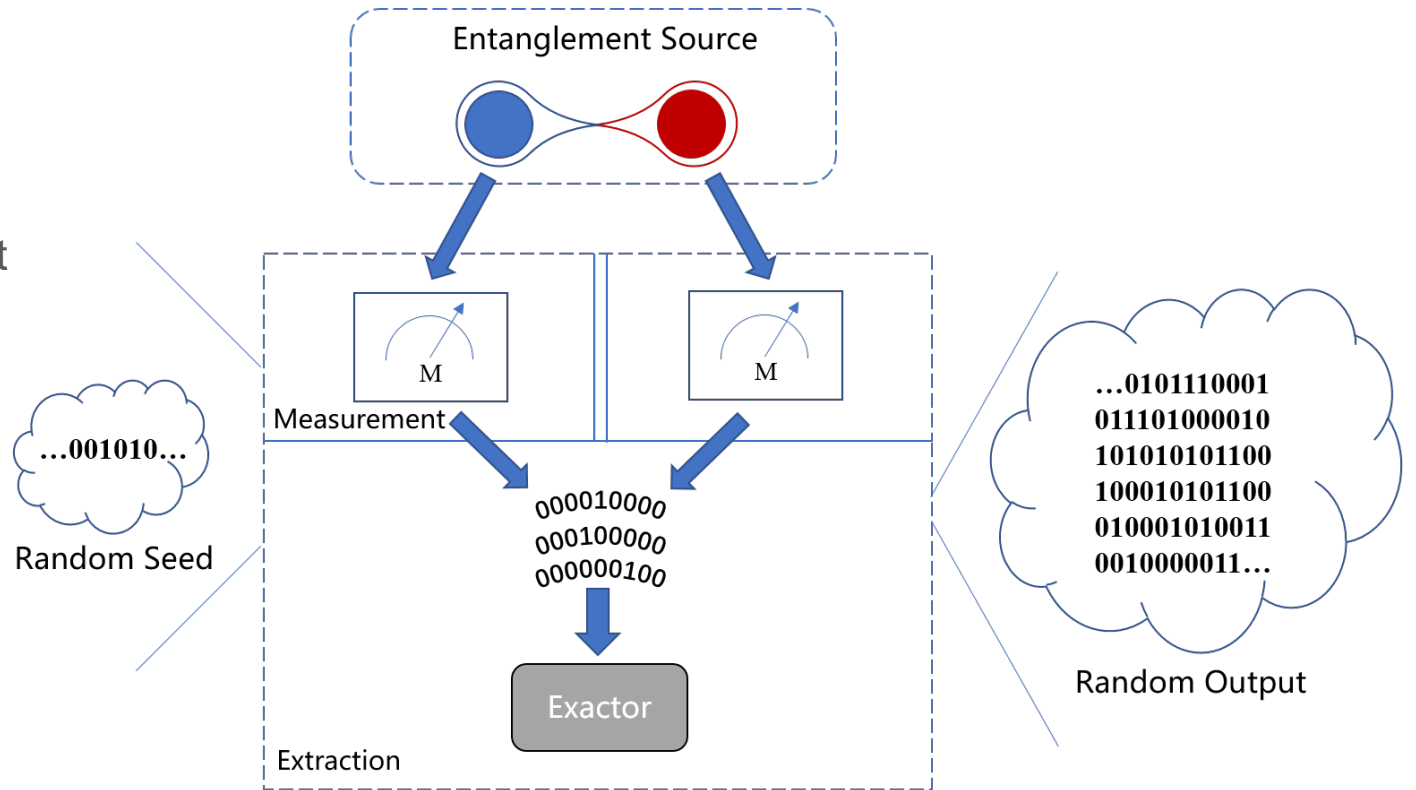


There is a trade-off between security and performance

Principle of Device-independent quantum randomness

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

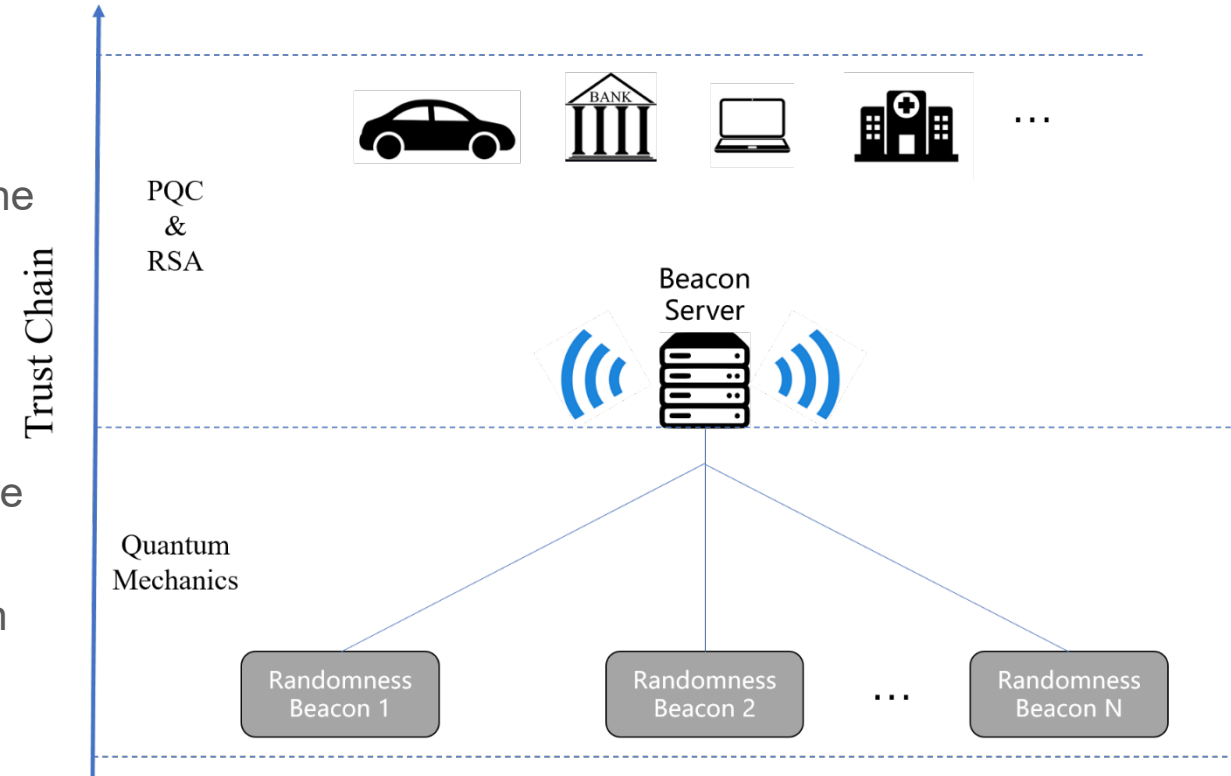
- Close detection loophole
- Prohibit communications between the measurements
- Measurement settings independent of entanglement creation



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

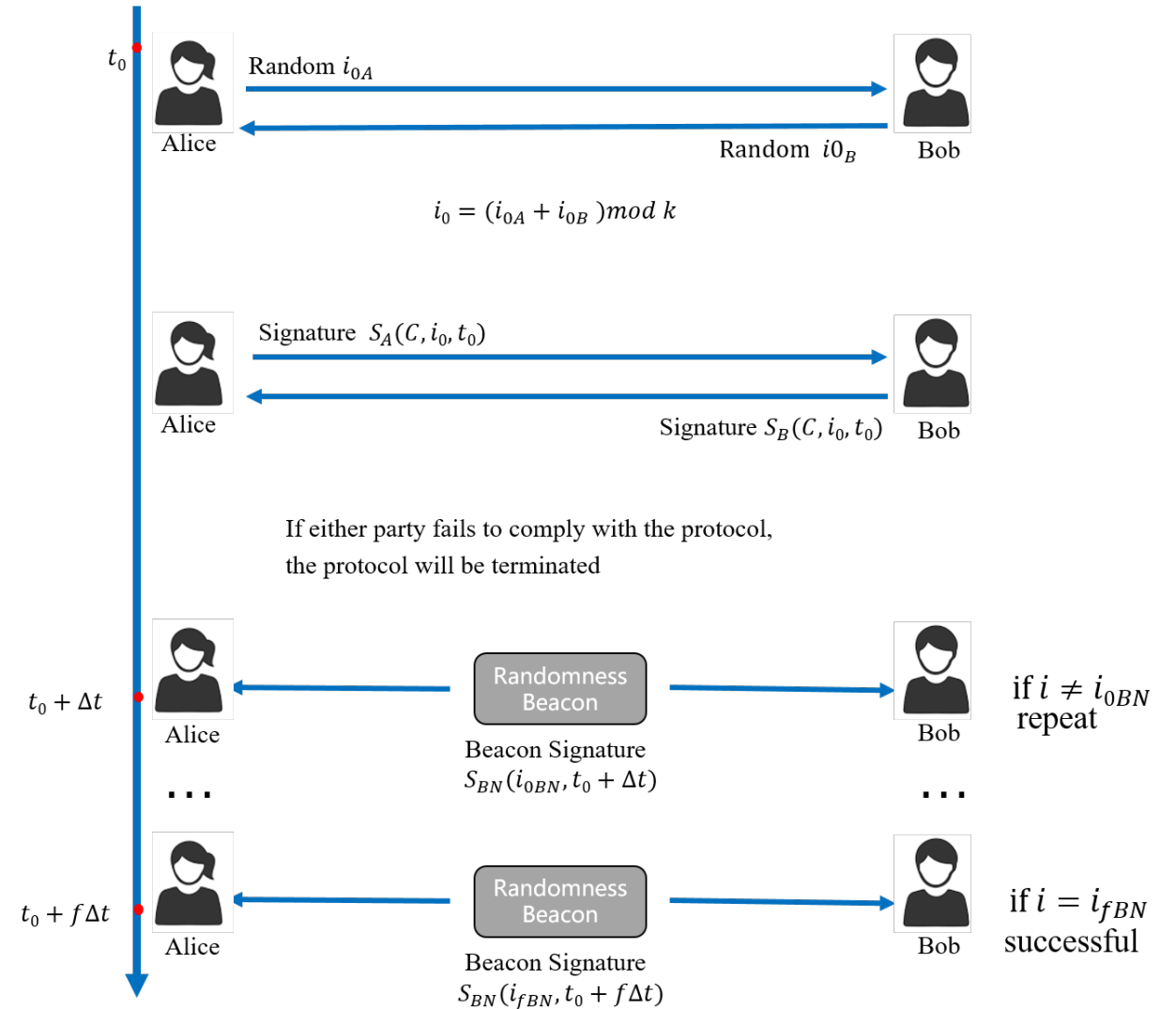


Use case of randomness beacon: Contract signing

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
- ...

BEACON | [Homepage](#) | [Overview](#) | [Download](#) | [Security](#) | [About](#) | [News](#) | [Login](#) | [Register](#) | [English](#) ▾

Device independent quantum random number beacon service (trial run)

Disclaimer: the beacon random numbers are provided based on the nonlocality principle of quantum mechanics, which have the best inherent randomness. However, due to the broadcast commonality of beacon random numbers, they cannot be directly used in cryptography. If beacon random numbers are used for business or other activities, we will not be responsible for all consequences.

This website provides [device independent quantum random numbers for users](#).

For the physical properties of quantum entanglement and the bell test without loopholes, the random numbers based on the intrinsic randomness of quantum mechanics can be generated, that is, the device-independent quantum random numbers. The security of the random numbers will not depend on the device used. This kind of random number generation device is considered to be the most secure random number generation device. The device-independent quantum random numbers provided in this website all pass the NIST randomness tests and can be traced back to the generation time, which is proven to be unpredictable before generation.

Random number information in the latest beacon pulse

SIGNATURE_RSA:	8D35843DCBC3A158F6DCB5D0247B8D6715CDDFFCFBFA940F43EFF5A8EB45EE4CFF09DC97E403C7935D92BF1EC7C9DCD5773780C44BC34B4161D9C50A89F607
SIGNATURE_PQC:	02C2CC1B91811AA78E2BF2403F381737E2EDDF9482638F08149BFF6B516E501B26D419ACA19E036ECD8CA06F2C5714FF659D49E61476853ED4BE32C718844072

[Overview](#) | [Download](#) | [Security](#) | [About](#)

[More >](#) | [More >](#) | [More >](#) | [More >](#)

ITU KALEIDOSCOPE

ONLINE 2021

Thank you!

