

Application and Use case of Device-independent quantum random number

Ming-Han Li
May 27, 2021





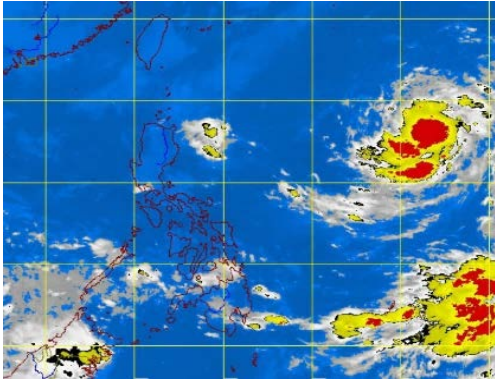
The nature of random numbers

Random number: a number generated in a random process

- Uniformity
- Unpredictable



RNG is widely used



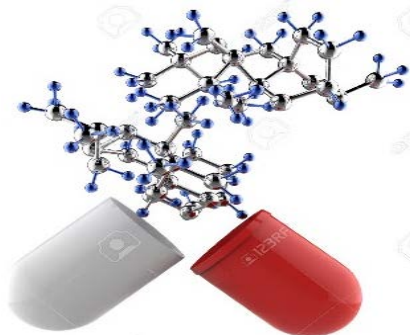
**Numerical
weather forecasting**



Lottery



AI



Drug development



Information security

The principle of classical random number generation

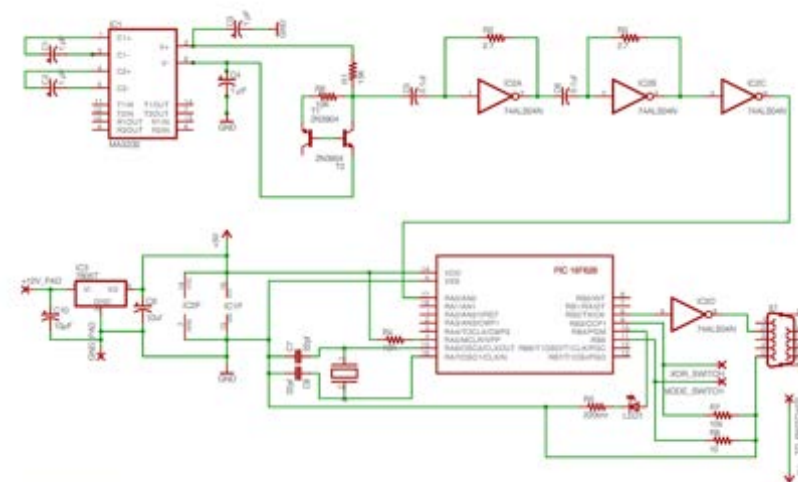
Algorithm-based

```
FUNCTION Uniform : REAL;  
  VAR  
    Z, k : INTEGER;  
  BEGIN  
    k := s1 DIV 53668;  
    s1 := 40014 * (s1 - k * 53668) - k * 12211;  
    IF s1 < 0 THEN s1 := s1 + 2147483563;  
  
    k := s2 DIV 52774;  
    s2 := 40692 * (s2 - k * 52774) - k * 3791;  
    IF s2 < 0 THEN s2 := s2 + 2147483399;  
  
    Z := s1 - s2;  
    IF Z < 1 THEN Z := Z + 2147483562;  
  
    Uniform := Z * 4.656613E-10  
  END
```

FIGURE 3. A Portable Generator for 32-bit Computers

- ✓ Uniform distribution
- ✗ Predictable

Based on classical thermal noise



(c) Rick Seaward 2005

- ✓ Uniform distribution
- ✗ Predictable in principle



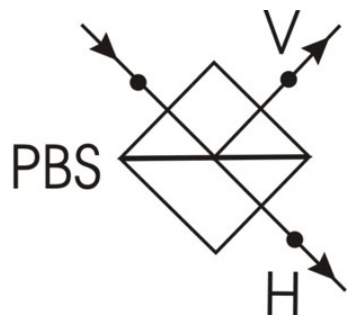
The principle of quantum random number generation

- ✓ Quantum state obeys superposition rule
- ✓ Measurement may induce random state collapse

Photon Polarization

$$\begin{array}{cc} \longleftrightarrow & \updownarrow \\ |H\rangle = |0\rangle & |V\rangle = |1\rangle \end{array}$$

$$|\nearrow\rangle = |\rightarrow\rangle + |\updownarrow\rangle$$



50% probability to get the result "1"

Intrinsic randomness!

50% probability to get the result "0"



- ✓ Uniform distribution
- ✓ Unpredictable in principle

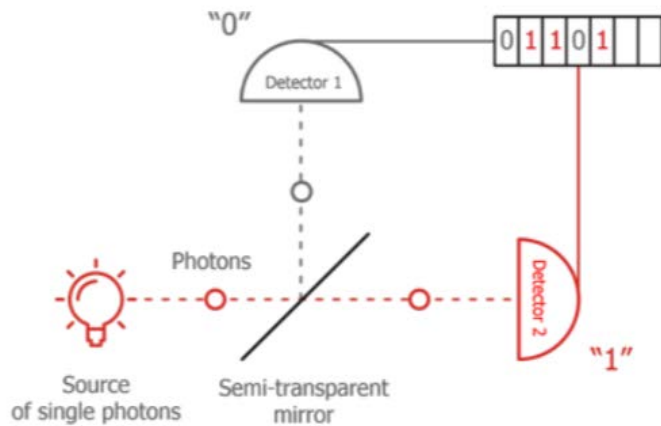


God does not play dice...

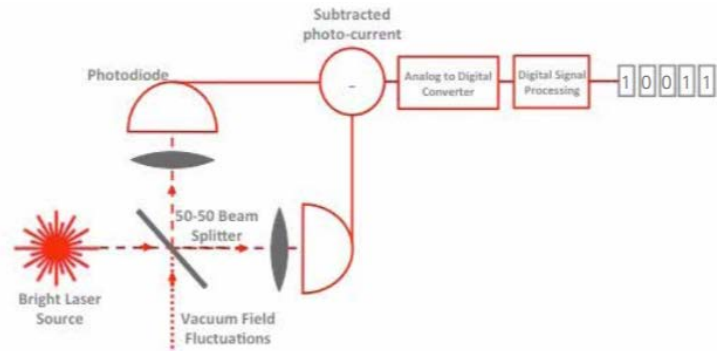


QRNG technology path

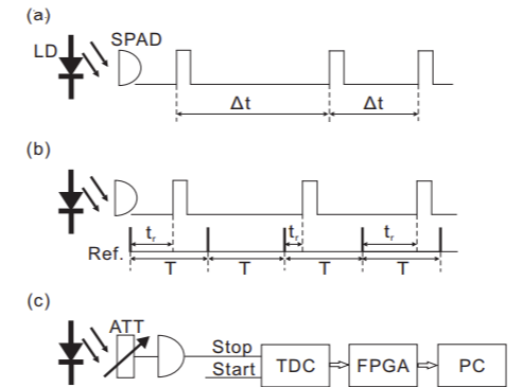
The basic principles of quantum mechanics have inherent randomness that is not found in classical physics. Therefore, a real random number generator, that is, a quantum random number generator, can be designed based on quantum mechanics



single photon beam splitting



vacuum fluctuation noise



Photon arrival time

QRNG products are mature



IDQ



QuantumCTek



Quintessence Lab



PICO Quant



Realistic security

In theory, randomness is based on the principles of quantum physics, and no one (including eavesdroppers) can predict

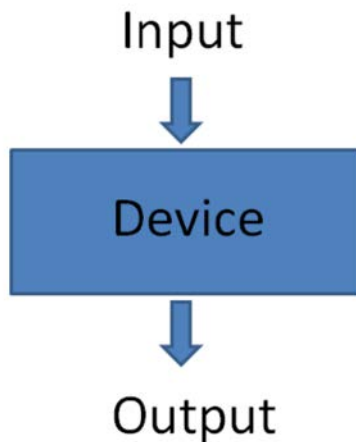
In reality, there are problems with quantum random numbers :

Device defect, component deviation, classical noise, side channel, adversary.
Therefore, users need to trust the device manufacturer.

- ⊗ Attackers may use device vulnerabilities to obtain random numbers
- ⊗ Need to test the implementation process

Device independent

The original device-independent idea was proposed in 1998 by Mayers and Yao¹ in the study of quantum serial distribution.



Highest security level! even if:

- The devices are untrusted
- The eavesdropper has the most computationally capable quantum computer

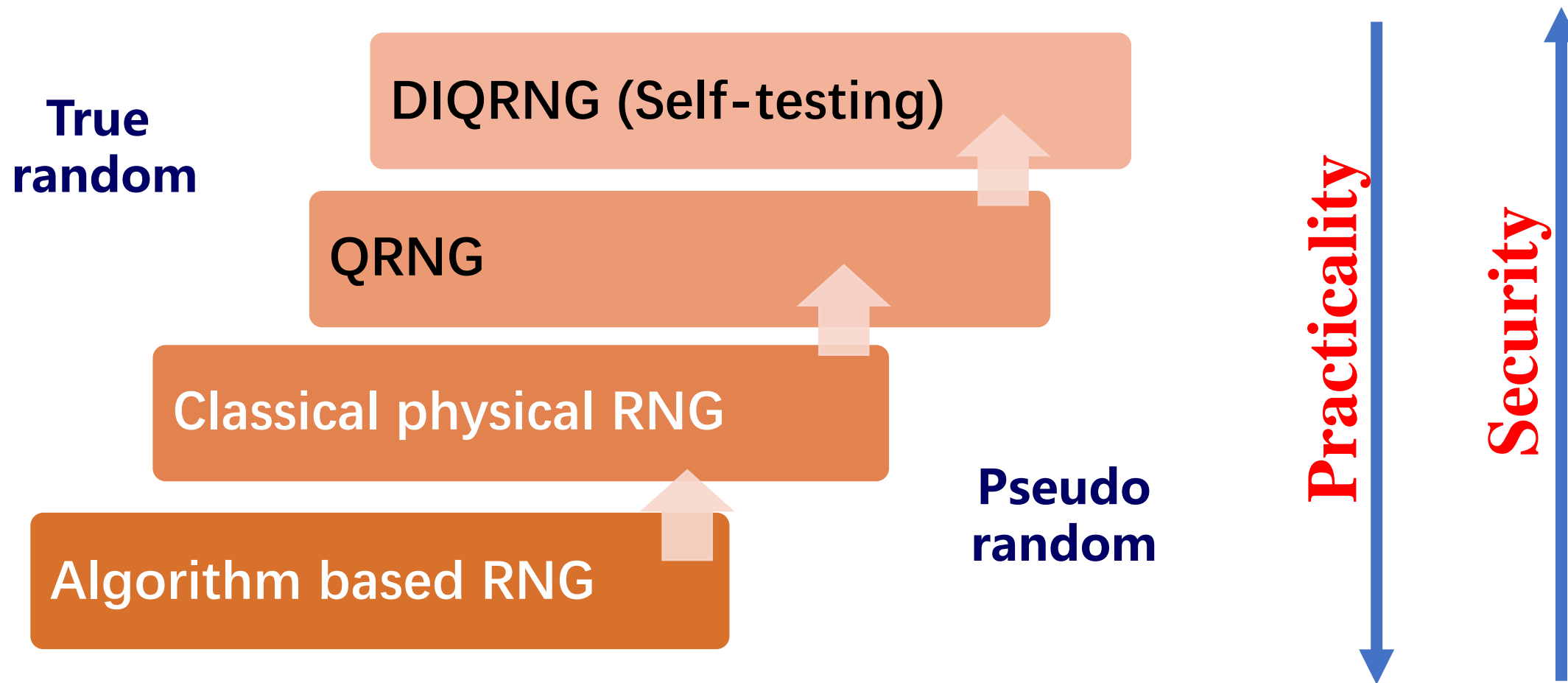
Can also generate unpredictable random numbers

The loophole free Bell test can realize device-independent quantum random numbers

[1] Mayers D, Yao A. Quantum Cryptography with Imperfect Apparatus. Annual Symposium on Foundations of Computer Science - Proceedings, 1998.



QRNG security classification



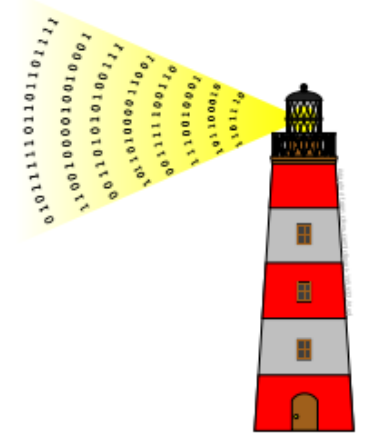


Randomness Beacon

Randomness Beacon Periodically broadcast random numbers to other locations in the system. As a public service, it is an important social resource in many application scenarios.

Random number beacon description:

- 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



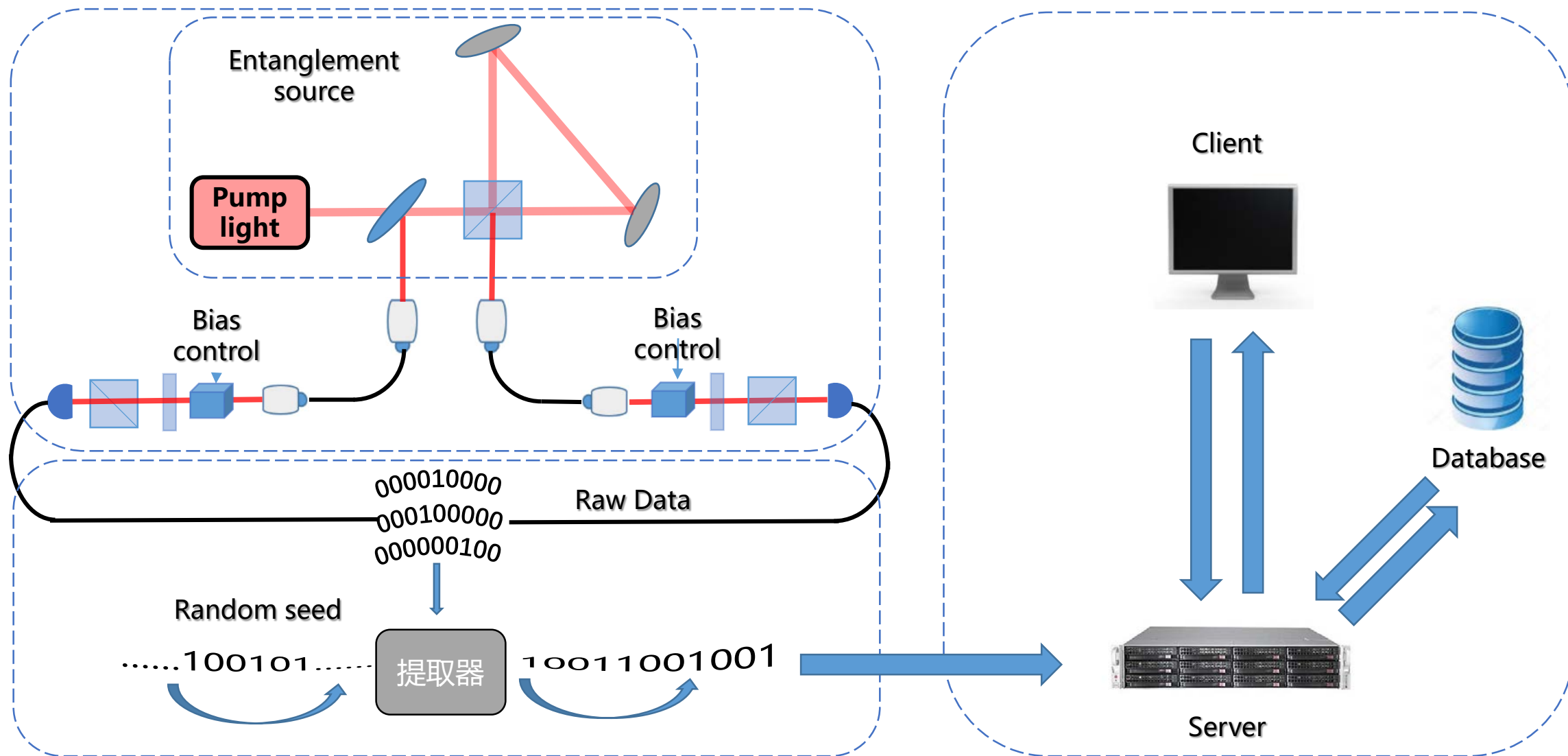


Randomness beacon

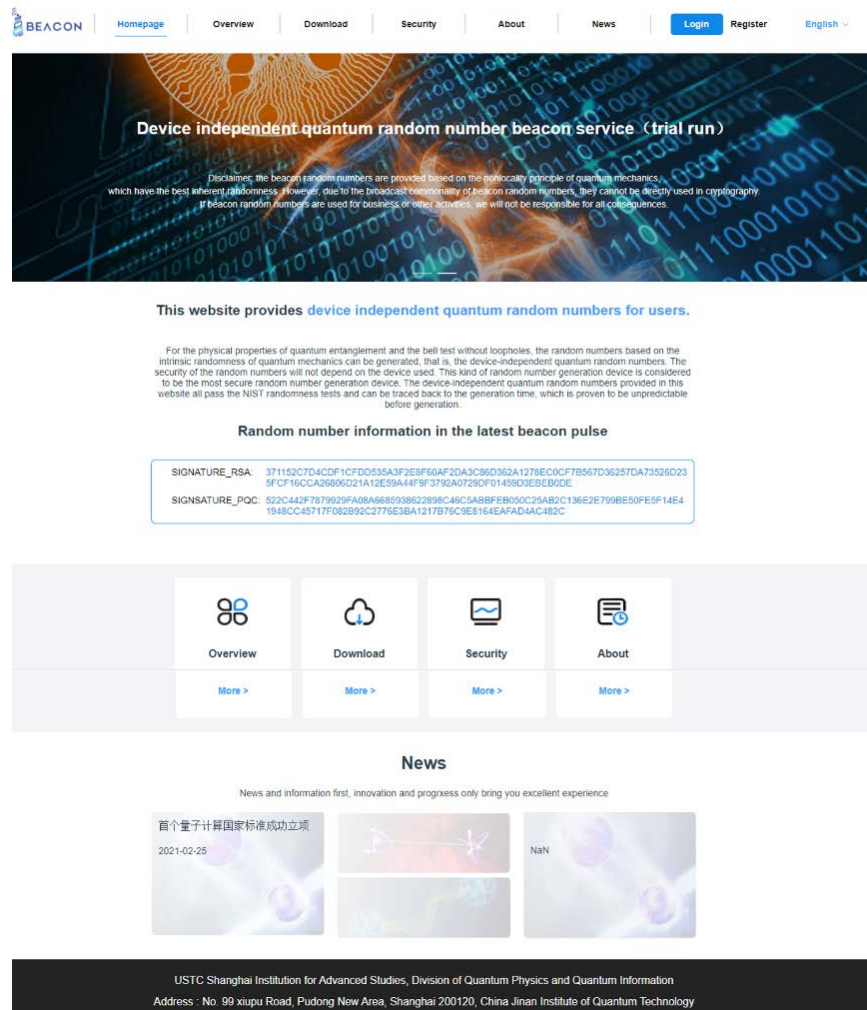
The random number beacon shall meet:

- Availability
- Unpredictability
- Authority
- Consistency
- Verifiability
- High efficiency

Use Case 1: Beacon Service for public entropy source



Use Case 1: Beacon Service for public entropy source



The screenshot shows the BEACON website homepage. The header includes the BEACON logo and navigation links: Homepage, Overview, Download, Security, About, News, Login, Register, and English. The main banner features the text "Device independent quantum random number beacon service (trial run)" and a disclaimer. Below the banner, a section titled "This website provides device independent quantum random numbers for users." explains the service. A "Random number information in the latest beacon pulse" section displays two signatures: SIGNATURE_RSA and SIGNATURE_PQC. The footer includes a navigation bar with icons for Overview, Download, Security, and About, a "News" section with a date "2021-02-25", and contact information for the USTC Shanghai Institute for Advanced Studies.

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 beacon's transparency 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: 371152C7D4CDF1CFDD535A3F2E8F60AF2DA3C86D362A1278E0CF7B567D3625DA73526D23
8FCF16CCA26806D21A12E59A44F9F379A07290F0145803EBE00DE

SIGNATURE_PQC: 522C442F787929FA08A6885938622898C46C5A8BFEB050C25AB0C136E2E7998E50FE5F14E4
1948CC45717F082B92C2776E3BA1217B76C9E8164EAFAD4AC482C

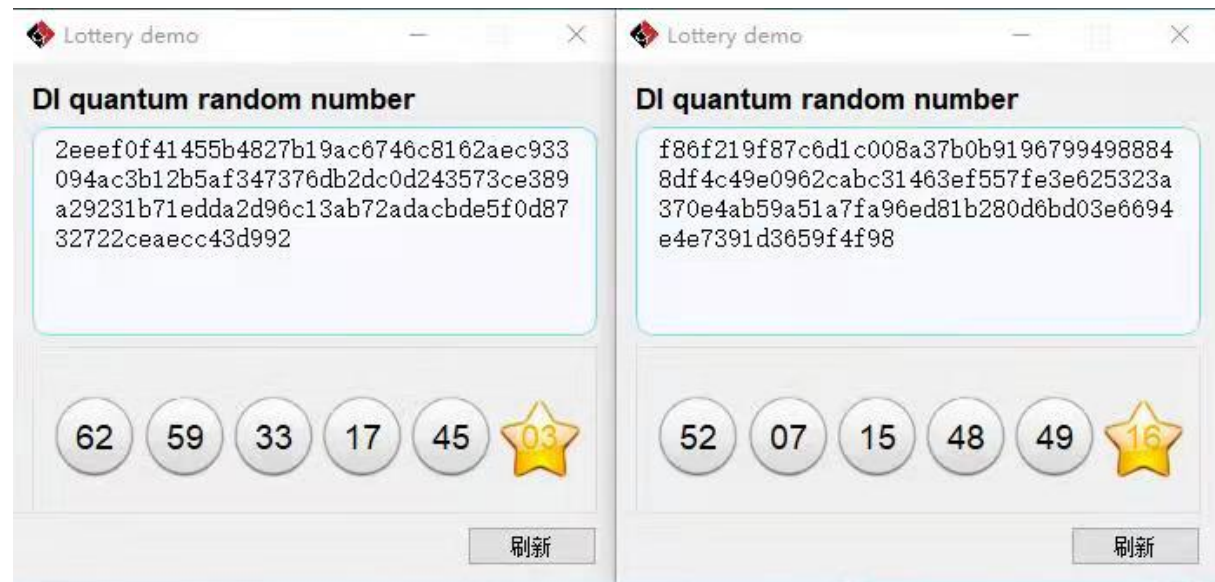
Overview | Download | Security | About

News

News and information first, innovation and progress only bring you excellent experience

首个量子计算国家标准成功立项
2021-02-25

USTC Shanghai Institute for Advanced Studies, Division of Quantum Physics and Quantum Information
Address : No. 99 xiupu Road, Pudong New Area, Shanghai 200120, China Jinan Institute of Quantum Technology



The screenshot shows a "Lottery demo" application window. It displays two "DI quantum random number" results. The left result is a long hexadecimal string: 2eeef0f41455b4827b19ac6746c8162aec933094ac3b12b5af347376db2dc0d243573ce389a29231b71edda2d96c13ab72adacbbe5f0d8732722ceaecc43d992. The right result is another long hexadecimal string: f86f219f87c6d1c008a37b0b91967994988848df4c49e0962cab31463ef557fe3e625323a370e4ab59a51a7fa96ed81b280d6bd03e6694e4e7391d3659f4f98. Below the numbers, there are five circular buttons with the numbers 62, 59, 33, 17, and 45, followed by a yellow star button with the number 08. A "刷新" (Refresh) button is at the bottom right.

Lottery demo

DI quantum random number

2eeef0f41455b4827b19ac6746c8162aec933094ac3b12b5af347376db2dc0d243573ce389a29231b71edda2d96c13ab72adacbbe5f0d8732722ceaecc43d992

62 59 33 17 45 08

刷新

Lottery demo

DI quantum random number

f86f219f87c6d1c008a37b0b91967994988848df4c49e0962cab31463ef557fe3e625323a370e4ab59a51a7fa96ed81b280d6bd03e6694e4e7391d3659f4f98

52 07 15 48 49 16

刷新

<http://sjs.qilushop.cn/web/#/>

A demo to use DIQRNG for lottery

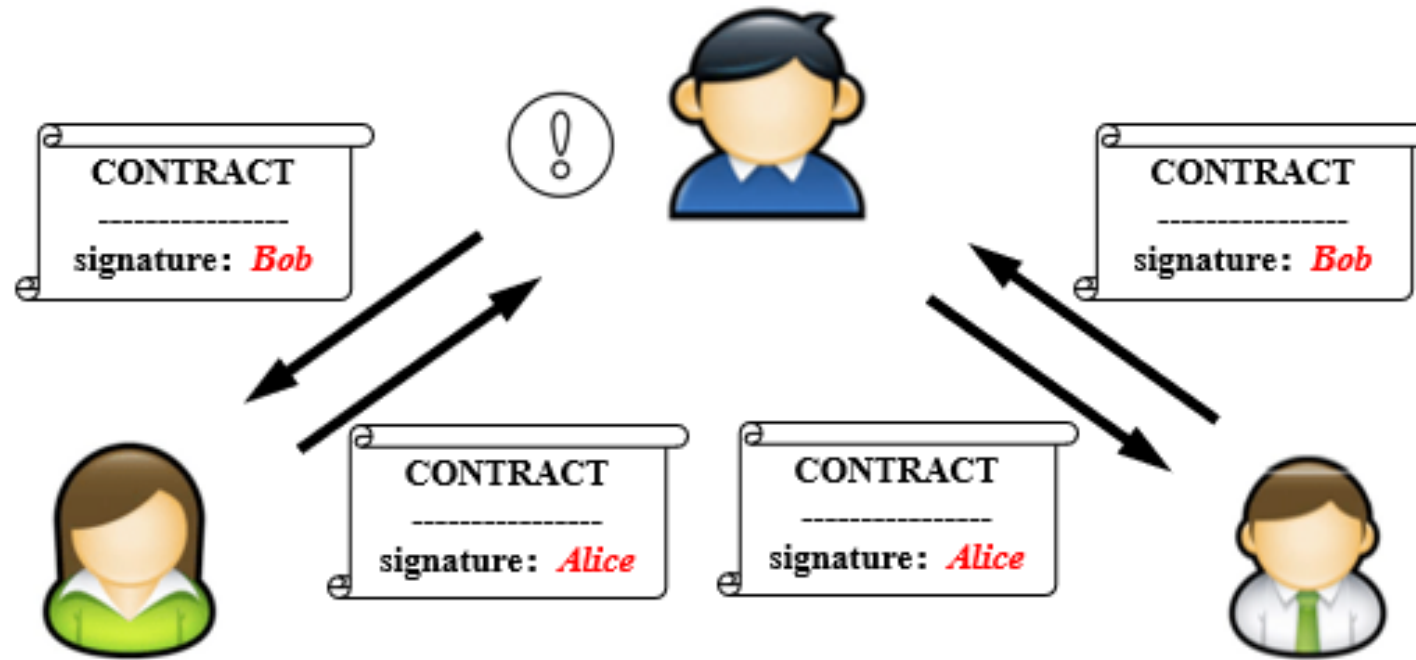
Use Case 2: Beacon Service for Smart Contract

How to ensure simultaneous signing?



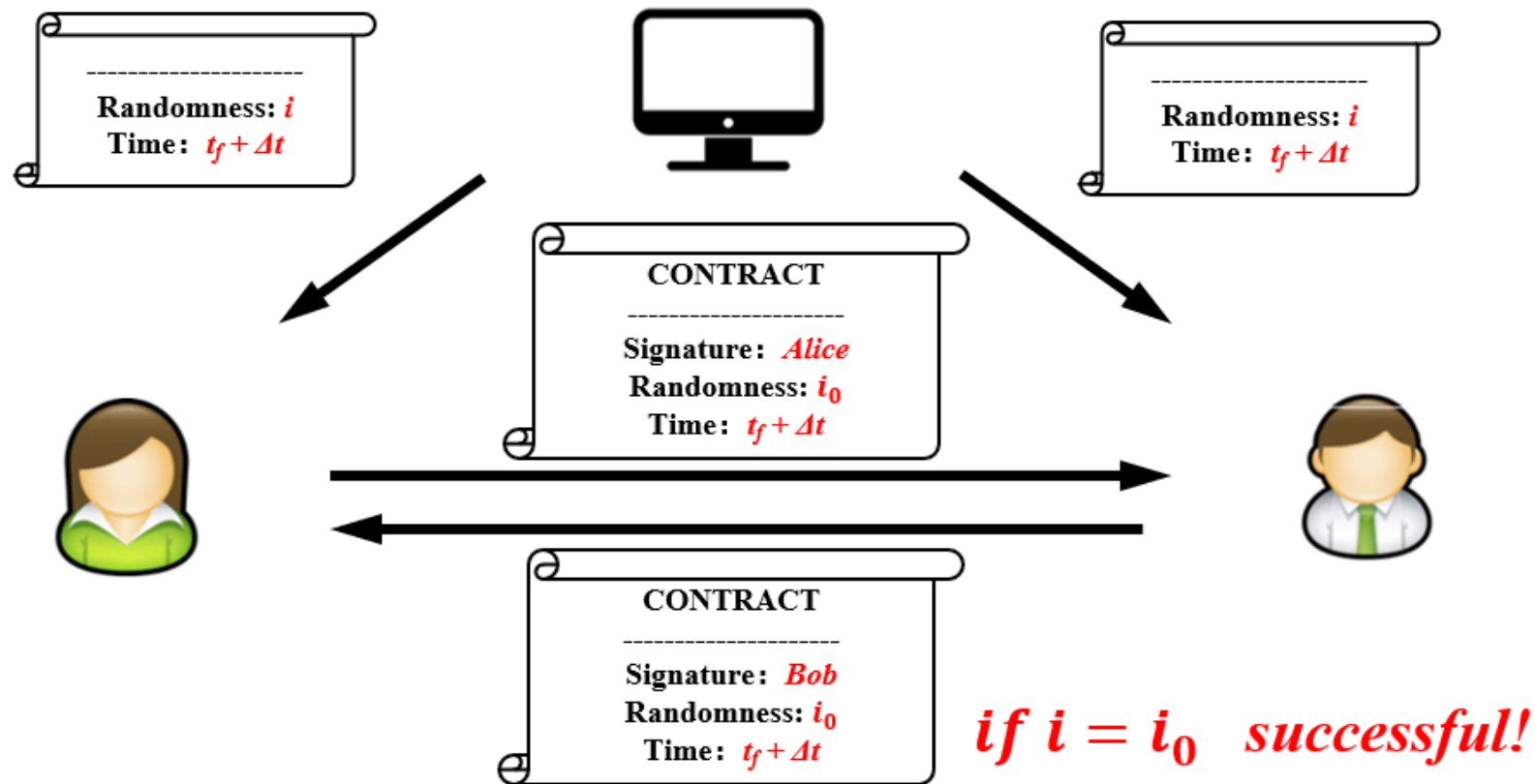
Alice committed to Bob without Bob' s corresponding commitment

Use Case 2: Beacon Service for Smart Contract



A centralised solution for contract signing, while the third party may have the information of the contract which should be secret

Use Case 2: Beacon Service for Smart Contract



Randomness beacon utilized for smart contract

Thanks