Physics & Quantum Information

中国科学技术大学
University of Science and Technology of China

Device independent quantum random number generation

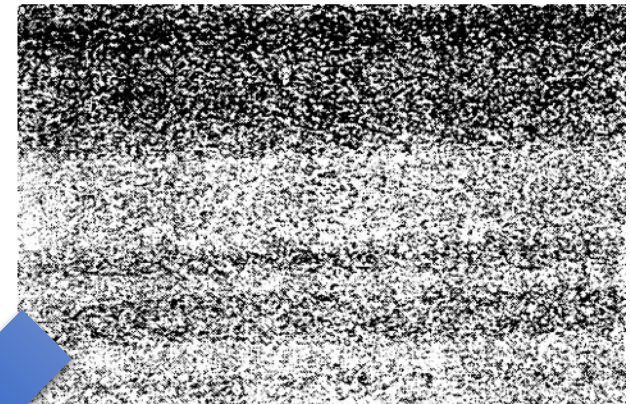
Yang Liu, Qi Zhao, Ming-Han Li, Jian-Yu Guan, Yanbao Zhang, Bing Bai, Weijun Zhang, Wen-Zhao Liu, Cheng Wu, Xiao Yuan, Hao Li, W. J. Munro, Zhen Wang, Lixing You, Jun Zhang, Xiongfeng Ma, Jingyun Fan, Qiang Zhang, Jian-Wei Pan

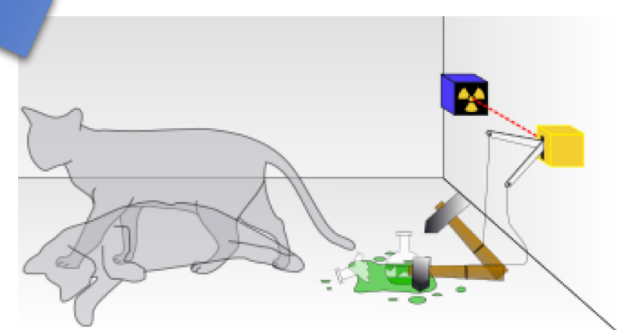
University of Science and Technology of China

27th Aug, QCrypt2018, Shanghai

I. Introduction

Randomness in Nature





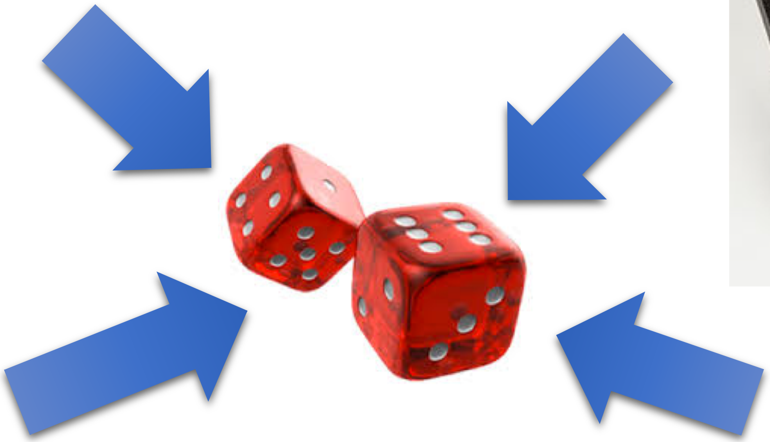
Random Number Generation

Algorithm Based

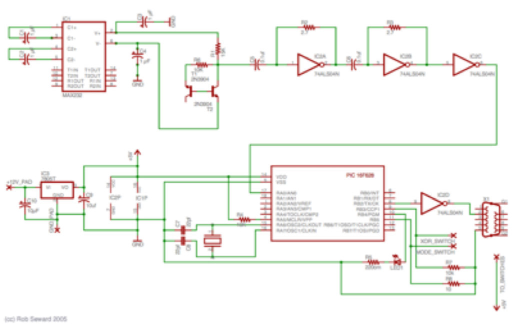
```
FUNCTION Uniform : REAL:
   VAR
      Z, k : INTEGER;
   BEGIN
   k   := s1 DIV 53668;
   s1  := 40014 * (s1 - k * 53668) - k * 12211;
   IF s1 < 0 THEN s1 := s1 + 2147483563;

   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

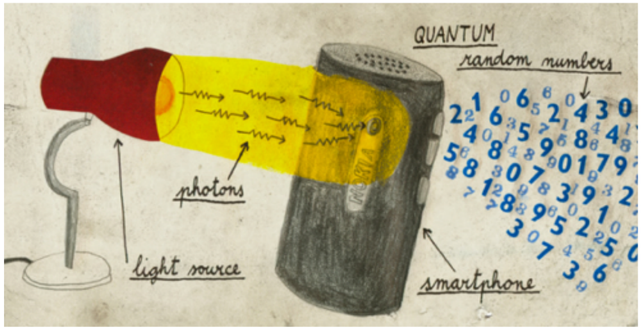
Classical



Thermal Noise Based



Quantum Random Number

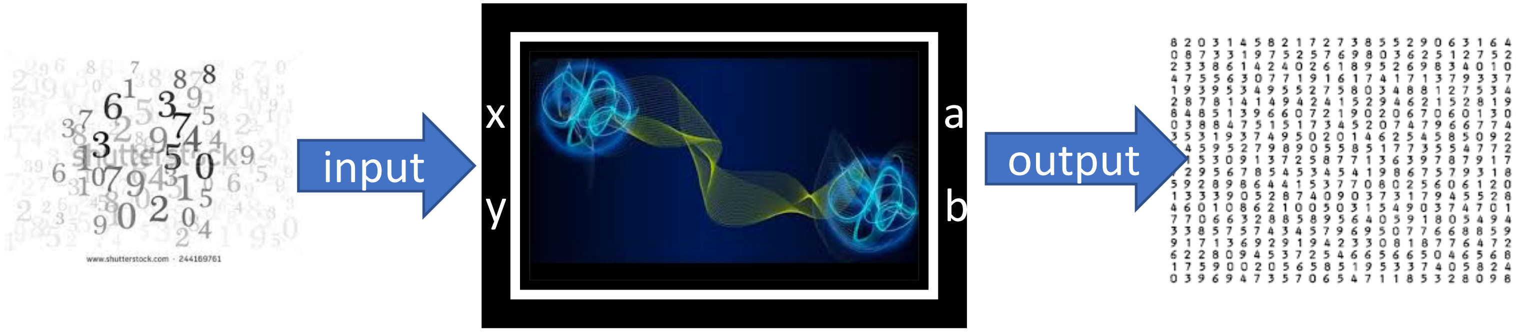


Random Number Generator (RNG)

- True Randomness: unpredictable to any adversary
- The principle of generating random numbers
  - Pseudo Random Number Generators (PRNG):
    - Intrinsically predictable, uniformly distributed
  - Quantum Random Number Generators (QRNG):
    - Inherent randomness (un-predicable), uniformly distributed
- Practical issues in QRNG
  - Device imperfections, components deviating, classical noises, side channels, adversary attacks (vulnerable)
  - Requires real-time monitoring and shielding (impractical)

Device Independent Quantum Random Number Generation (DIQRNG)

- QRNGs: Trusted device, Semi-DI, DIQRNG
  - Goal: Generate randomness without relying on physical implementations
- DIQRNG (Self-testing QRNG)
  - Output randomness is certified independent of device implementations



DIQRNG – Theory Requirement

- DIQRNG against quantum adversary
  - ➢ Do not assume independent and identical distribution
  - ➢ Consider classical and quantum side information
  - ➢ Produce random bits with non-vanishing rate
  - ➢ Should noise-tolerant, and efficient for finite-data size
- With entropy accumulation theorem
  - ✓ do not use the i.i.d. assumption
  - ✓ consider the quantum side information
  - ✓ produce randomness approaching i.i.d. rate

F. Dupuis, O. Fawzi, and R. Renner, **arXiv**:1607.01796 (2016).
R. Arnon-Friedman, R. Renner, and T. Vidick, **arXiv**:1607.01797 (2016)

DIQRNG – Experiments

- Based on (loophole-free) Bell's inequality test
  - Close detection loophole — High System Efficiency
  - Prohibit communications between the measurements
  - Measurement settings independent of entanglement creation — Space-like Separation — Proper Shielding

- Related DIQRNG experiments:
  - DIQRNG against classical adversary — P. Bierhorst, et.al., Nature **556**, 223 (2018).
  - DIQRNG closing detection loophole — Y. Liu, et.al., PRL **120**, 010503 (2018).
  - Randomness extraction with continuous down conversion source

    Lijiong Shen, et.al., ArXiv:1805.02828 (2018). Also in the next talk.

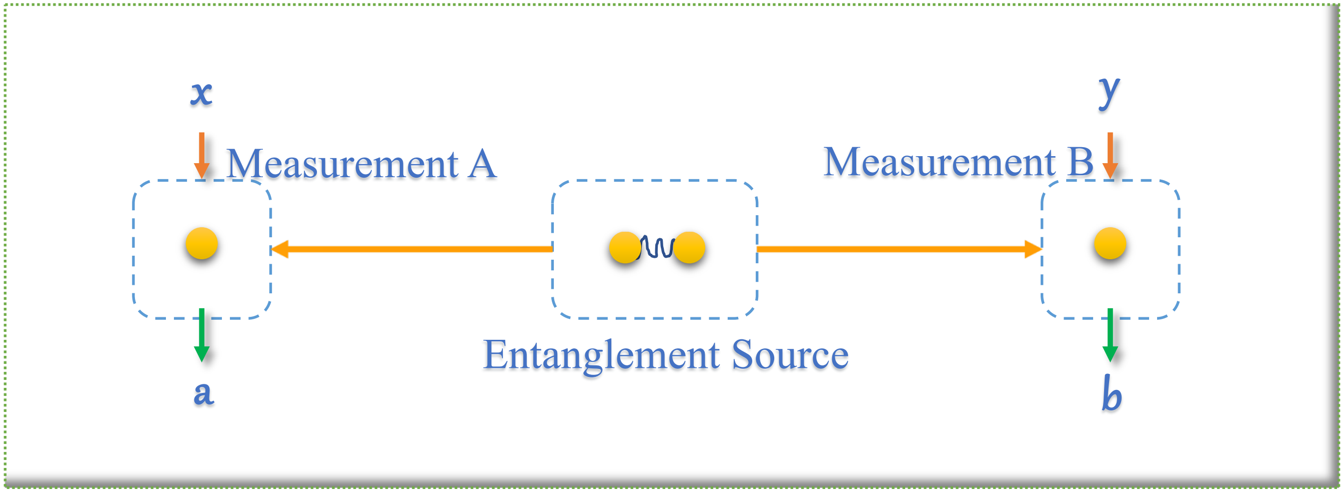
II. Theory

DIQRNG Theory (brief review)

- Entanglement pairs distribution and measurement

For each experimental trial i:

  - Generation trial: $x_i = 0$ and $y_i = 0$. with probability: 1-q
  - Test trial (Bell test): $x_i\ (y_i) \in \{0, 1\}$ with probability: q
  - CHSH game value: $J_i = 1$ if $a_i \oplus b_i = x_i \cdot y_i$ and 0, otherwise.



DIQRNG Theory (brief review)

- CHSH game value for n trials:

$$\bar{J} = \frac{1}{n}\sum_{i=1}^{n} J_i - 3/4.$$

$$\bar{J} = J_{A_1B_1} + J_{A_1B_2} + J_{A_2B_1} + J_{A_2B_2} - 3/4$$

With: $$\begin{cases} J_{A_1B_1} = (N_{ab=00|A_1B_1} + N_{ab=11|A_1B_1})/N, \\ J_{A_1B_2} = (N_{ab=00|A_1B_2} + N_{ab=11|A_1B_2})/N, \\ J_{A_2B_1} = (N_{ab=00|A_2B_1} + N_{ab=11|A_2B_1})/N, \\ J_{A_2B_2} = (N_{ab=01|A_2B_2} + N_{ab=10|A_2B_2})/N. \end{cases}$$

- Randomness Estimation

$$H_{\min}^{\varepsilon_s}(\mathbf{AB}|\mathbf{XY}E) \geq n \cdot R_{opt}(\varepsilon_s, \varepsilon_{\mathrm{EA}}, \omega_{\mathrm{exp}})$$

to extract $H_{\min}^{\varepsilon_s}(\mathbf{AB}|\mathbf{XY}E) - t_e$ random numbers

that is $\varepsilon_s + \varepsilon_{EA} + 2^{-t_e}$ close to uniform distribution

$$g(p) = \begin{cases} 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\frac{p}{q}(\frac{p}{q} - 1) + 3}\right) & \frac{p}{q} \in [0, \frac{2+\sqrt{2}}{4}] \\ 1 & \frac{p}{q} \in [\frac{2+\sqrt{2}}{4}, 1] \end{cases}$$

$$f_{\min}(p, p_t) = \begin{cases} g(p) & p \leq p_t \\ \frac{d}{dp}g(p)|_{p_t} \cdot p + (g(p_t) - \frac{d}{dp}g(p)|_{p_t} \cdot p_t) & p > p_t \end{cases}$$

$$R(p, p_t, \varepsilon_s, \varepsilon_e) = f_{\min}(p, p_t) - \frac{1}{\sqrt{n}} 2(\log 13 + \frac{d}{dp}g(p)|_{p_t})\sqrt{1 - 2\log(\varepsilon_s \cdot \varepsilon_e)}.$$

$$R_{opt}(\varepsilon_s, \varepsilon_e) = \max_{\frac{3}{4} < \frac{p_t}{q} < \frac{2+\sqrt{2}}{4}} R(\omega_{exp} \cdot q - \delta_{est}, p_t, \varepsilon_s, \varepsilon_e).$$

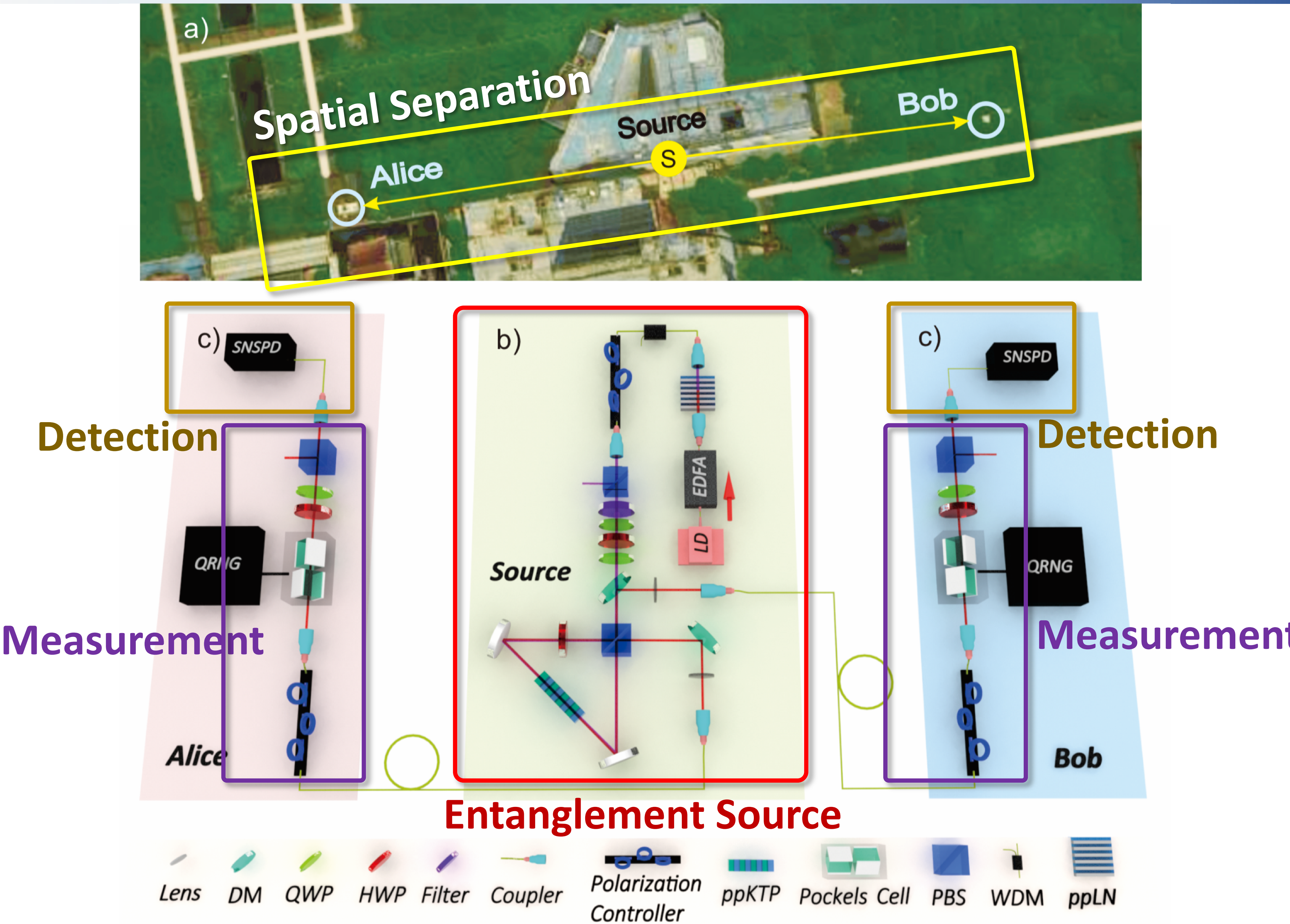
- Randomness Extraction

Based on entropy accumulation theorem (EAT)
R. Arnon-Friedman, R. Renner, and T. Vidick, arXiv:1607.01797 (2016), Nat Commun **9**, 459 (2018)

DIQRNG Theory (brief review)

- Do not assume the inner working of devices
- Assume the law of quantum mechanic is correct
- Assume A's/B's devices are in secure lab
  - Adversaries cannot access their measurement outcomes
- Assume the input random numbers are uniform & secure
- Assume classical post-processing is trusted

III. Experiment



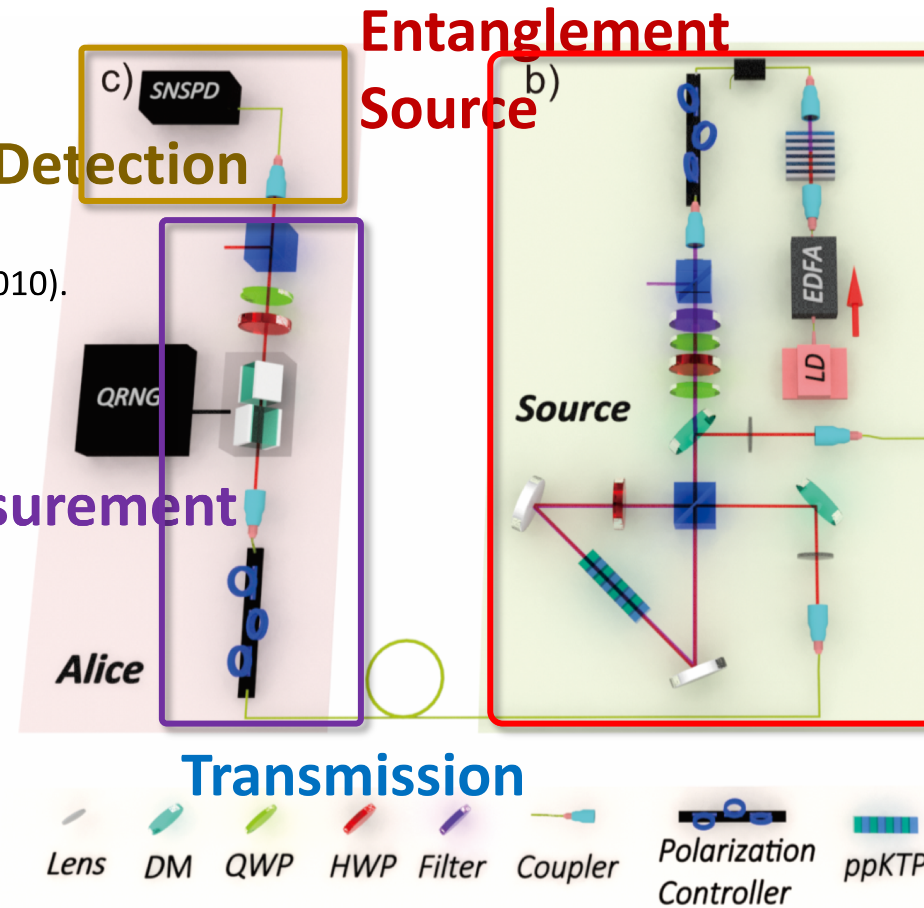
a)
Spatial Separation
Alice
Source
S
Bob
c)
SNSPD
b)
EDFA
LD
Source
QRNG
Alice
Bob
Detection
Measurement
Detection
Measurement
Entanglement Source
Lens
DM
QWP
HWP
Filter
Coupler
Polarization Controller
ppKTP
Pockels Cell
PBS
WDM
ppLN

DIQRNG Experiment
-- System Efficiency

- Entanglement Source
    - Optimize coupling efficiency

      P. Dixon, et. al., Phys Rev A **90**, (2014).
      R. Bennink, Physical Review A **81**, 053805 (2010).
    - Using high efficiency coating
- Transmission
- Measurement
    - Optimize coupling efficiency with classical reference
- Detection
    - Develop high efficiency SNSPD

  W. Zhang et. al., Science China, **60**, 120314 (2017).



DIQRNG Experiment
-- System Efficiency

- Experimental test of system efficiency

$$\eta = \eta^{sc} \times \eta^{so} \times \eta^{fiber} \times \eta^{m} \times \eta^{det}$$

Tab: System Efficiency		Alice	Bob
Source Collection (Coupling)	η^{sc}	93.9%	94.2%
Source Optics (Coating)	η^{so}	95.9%	
Fiber Transmittance	η^{fiber}	99.0%	
Measurement (Coupling & Coating)	η^{m}	94.8%	95.2%
Single Photon Detector	η^{det}	93.2%	92.2%
System Efficiency	η	**78.8%±1.9%**	**78.5%±1.5%**

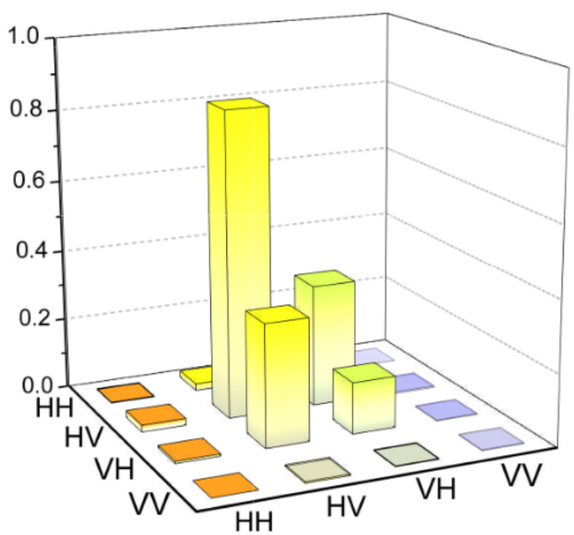
DIQRNG Experiment -- Quantum State

- Quantum State: $\cos(22.05°)\,|HV\rangle + \sin(22.05°)|VH\rangle$
- Measurement Bases: $a_0 = -83.5°, \mathrm{a}_1 = -119.4°$
  $\mathrm{b}_0 = 6.5°, \mathrm{b}_1 = -29.4°$

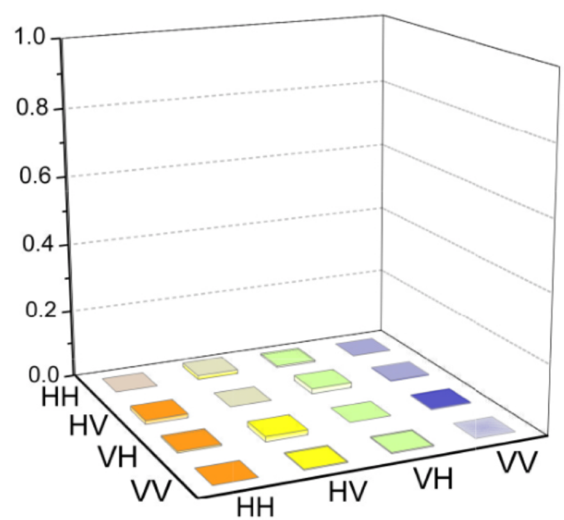
Optimized for the setup

- State Fidelity ~99.0%

State Tomography (Real)



State Tomography (Imaginary)



DIQRNG Experiment -- Spatial Separation

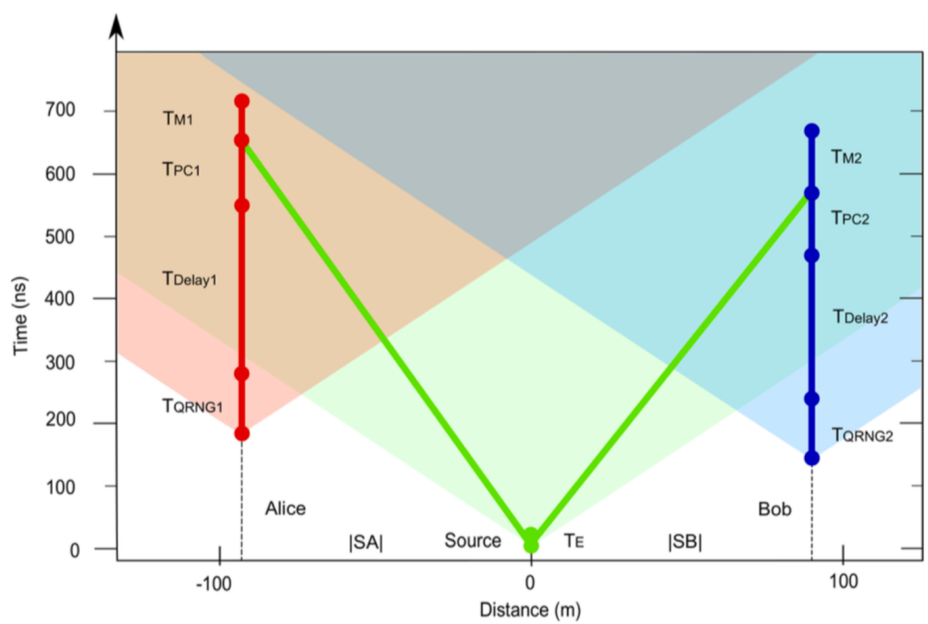
- Spatial separation between
  - Measurement at A(B) and setting choice/measurement outcome at B(A)

$$\begin{cases} (|SA|+|SB|)/c > T_E - (L_{SA}-L_{SB})/c + T_{QRNG1} + T_{Delay1} + T_{PC1} + T_{M2}, \\ (|SA|+|SB|)/c > T_E + (L_{SA}-L_{SB})/c + T_{QRNG2} + T_{Delay2} + T_{PC2} + T_{M1}, \end{cases}$$

  - Entanglement creation (S) and setting choice A/B

$$\begin{cases} |SA|/c > L_{SA}/c - T_{Delay1} - T_{PC1} \\ |SB|/c > L_{SB}/c - T_{Delay2} - T_{PC2} \end{cases}$$

- Characterize the delay
  - On site free-space measure
  - Optical reflection
  - Measure Cable length



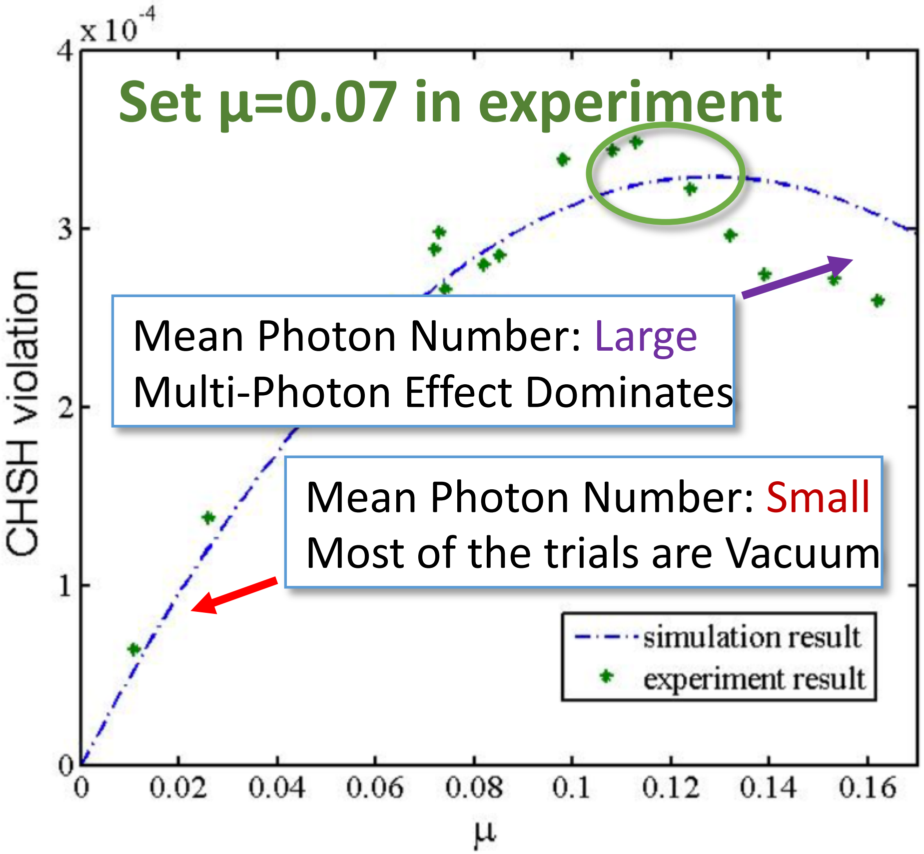
DIQRNG Experiment -- Optimized Intensity

- Theoretical Model: $J \approx J_B + P(1)J_{n=1} + P(2)J_{n=2} + P(3)J_{n=3}$
  - Vacuum: No contribution
  - 1-Photon: CHSH Violation
  - 2-Photon: No Violation

- Optimize CHSH with Intensity
  - Simulate Poisson Source with 0~3 pairs case
  - Consider all possible results

TABLE V. Possible events for single photon pair.

parties	1	2	3	4	5	6	7	8	9
Alice and Bob	0,0	0,1	0,u	1,0	1,1	1,u	u,u	u,u	u,u



DIQRNG Experiment -- Extraction

FFT Acceleration of Toeplitz Matrix Multiplication

$$R_m = \begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ \vdots \\ r_{m-1} \end{pmatrix} \qquad T_{m\times n} = \begin{pmatrix} a_0 & a_{-1} & \cdots & a_{-(n-2)} & a_{-(n-1)} \\ a_1 & a_0 & \ddots & & a_{-(n-1)+1} \\ a_2 & a_1 & \ddots & \ddots & \vdots \\ \vdots & \vdots & & \ddots & a_{-(n-1)+(m-2)} \\ a_{m-1} & a_{m-2} & \cdots & a_{-n+(m-1)} & a_{-(n-1)+(m-1)} \end{pmatrix} \qquad V_n = \begin{pmatrix} v_0 \\ v_1 \\ v_2 \\ \vdots \\ v_{n-1} \end{pmatrix}$$

$$\boxed{R_m = T_{m\times n} \times V_n = IFFT(FFT(T_{m+n-1}) \cdot FFT(V_m))}$$

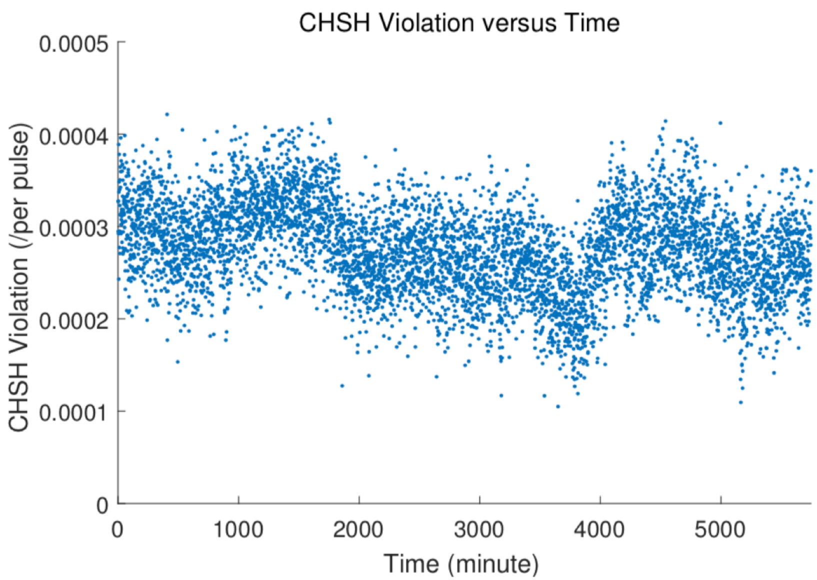
$$R'_m = \begin{pmatrix} R_l^0 & R_l^1 & \cdots & R_l^{k-1} \end{pmatrix} \quad T_{m\times n} = \begin{pmatrix} T_{m\times l}^0 & T_{m\times l}^1 & \cdots & T_{m\times l}^{k-1} \end{pmatrix} \quad V_n = \begin{pmatrix} V_l^0 \\ V_l^1 \\ \vdots \\ V_l^{k-1} \end{pmatrix}$$

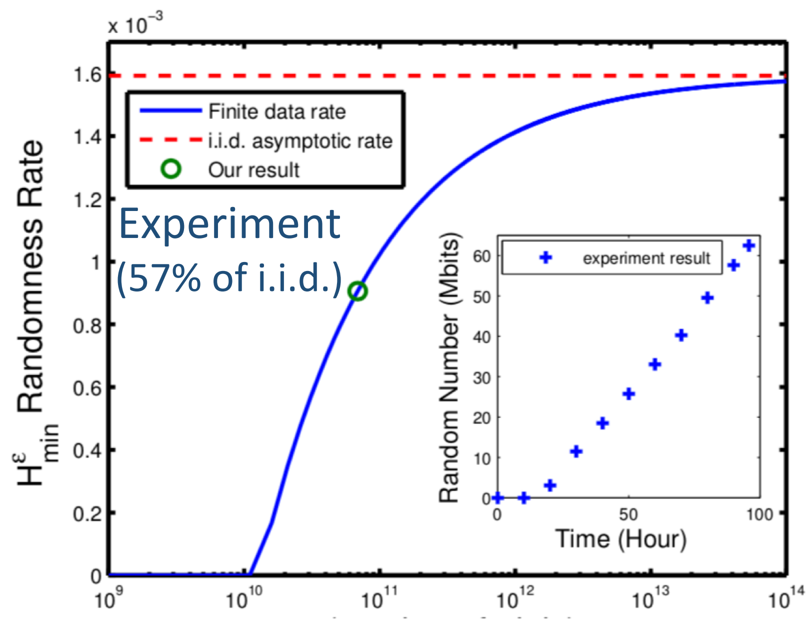
Grouped FFT Acceleration

IV. Result

DIQRNG Experiment -- Result

- $n = 6.895{\times}10^{10}$ experimental trials in 95.77 hours.
- CHSH violation $\bar{J} = 2.757{\times}10^{-4}$
- Final random bits $6.2469{\times}10^{7}$ or $181.2\ bps$ with uniformity within 10^{-5}





DIQRNG Experiment -- Result

- Hypothesis test (p-value) of local realism

  The null hypothesis: The experimental results are explainable by local realism.

  p value: the max probability according to local realism that the statistic takes a value as extreme as the observed one.

  - Prediction-based-ratio (PBR)

  Upper bound of the p-value w/o i.i.d.

  $$\boxed{P_{LR} = 10^{-204792}}$$

  The small p value strongly reject LHV.

- Hypothesis test of no signaling

  $$\boxed{P_{NS} = 1}$$

  No evidence of anomalous signaling

- Passes NIST uniformity test

Statistical tests	P value	Proportion	Result
Frequency	0.17828	1.000	Success
BlockFrequency	0.73992	0.983	Success
CumulativeSums	0.25360	1.000	Success
Runs	0.13469	1.000	Success
LongestRun	0.67178	1.000	Success
Rank	0.04872	1.000	Success
FFT	0.77276	0.967	Success
NonOverlappingTemplate	0.08440	0.990	Success
OverlappingTemplate	0.63712	1.000	Success
Universal	0.96430	0.983	Success
ApproximateEntropy	0.37814	0.983	Success
RandomExcursions	0.22430	0.990	Success
RandomExcursionsVariant	0.50920	0.991	Success
Serial	0.10250	1.000	Success
LinearComplexity	0.13469	1.000	Success

Outlook

- DI-Random Number Expansion
- DI-Random Number Amplification
- Looking for Device-Independent Protocols

Shanghai Branch, University of Science and Technology of China:
Yang Liu, Ming-Han Li, Jian-Yu Guan, Bing Bai, Wen-Zhao Liu, Cheng Wu, Jun Zhang, Jingyun Fan, Qiang Zhang, Jian-Wei Pan

Tsinghua University:
Qi Zhao, Xiao Yuan, Xiongfeng Ma

Shanghai Institute of Microsystem and Information Technology:
Weijun Zhang, Hao Li, Lixing You, Zhen Wang

NTT Basic Research Laboratories
Yanbao Zhang, W. J. Munro

National Key R&D Program of China

Thank You!