Randomness extraction from Bell violation with continuous parametric down conversion

Lijiong Shen

Jianwei Lee   Alessandro Cerè   Le Phuc Thinh

Valerio Scarani   Christian Kurtsiefer

National University of Singapore

Centre for Quantum Technologies

Jean-Daniel Bancal *University of Basel, CH*

Antia Lamas-Linares *Texas Advanced Computing Center, USA*

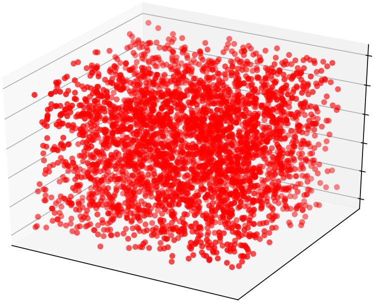
Thomas Gerrits   Adriana E. Lita   Sae Woo Nam

NIST, USA

lijiong.shen@u.nus.edu

Secure private communication requires Randomness

Classical systems cannot guarantee unpredictability

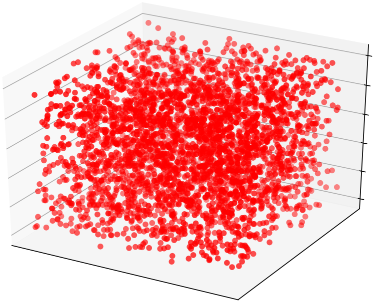


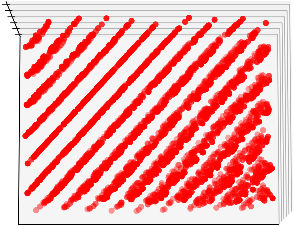
---

https://en.wikipedia.org/wiki/RANDU

Secure private communication requires Randomness

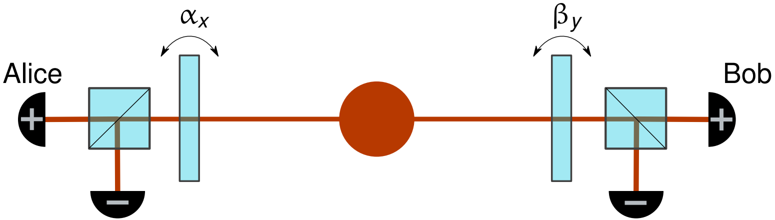
Classical systems cannot guarantee unpredictability





https://en.wikipedia.org/wiki/RANDU

Non-classical correlations certify genuine randomness

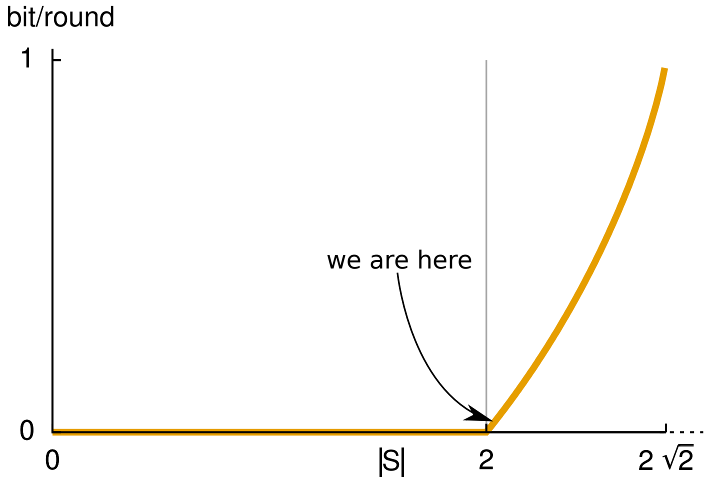


Correlation for measurement settings α_x, β_y

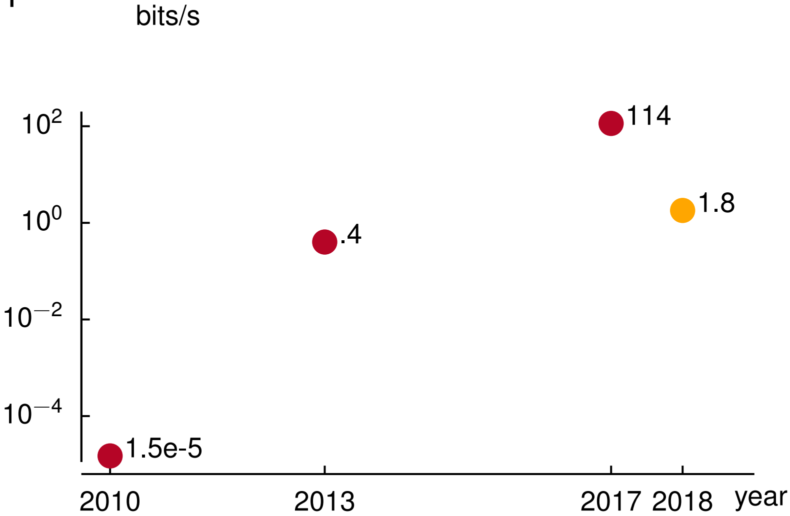
$$E_{x,y} = P(a = b|x, y) - P(a \neq b|x, y)$$

Bell parameter from 4 settings

$$S = E_{00} + E_{01} + E_{10} - E_{11}$$


bit/round
1
0
we are here
0
|S|
2
$2\sqrt{2}$

Our point to the state of the art



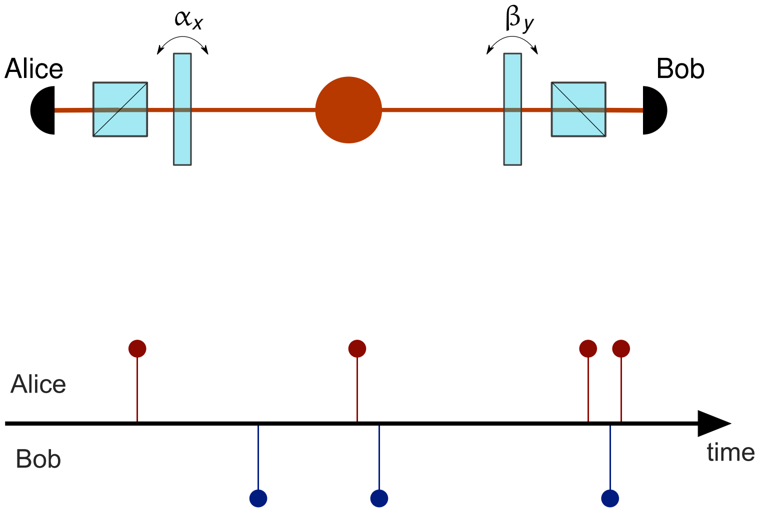
S. Pironio et al., Nature (2010)

B. G. Christensen et al., PRL (2013)

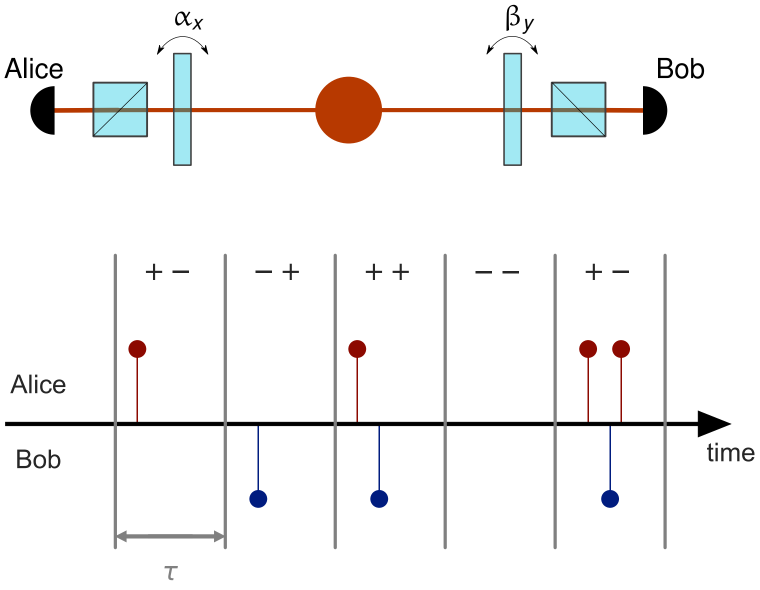
Y.Liu et al., PRL (2018)

P.Bierhorst et al.,Nature(2018)

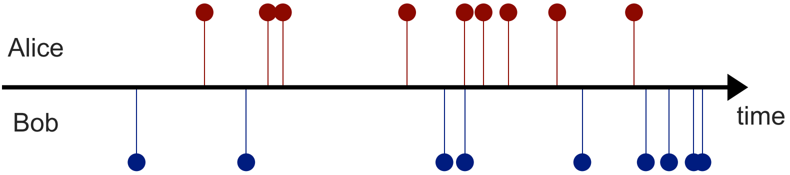
Bell test with CW source and two detectors



Bell test with CW source and two detectors

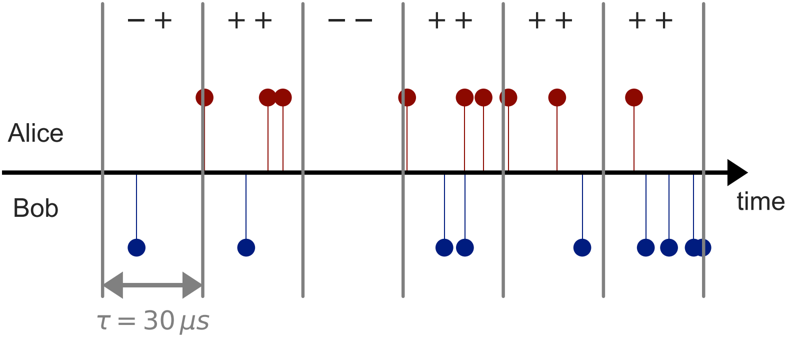


Correlation depends on bin width τ



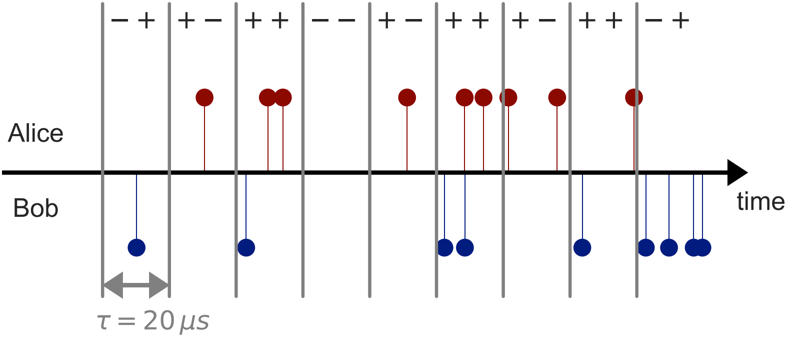
Correlation depends on bin width τ

$$E = \frac{N_{++} + N_{--} - N_{-+} - N_{+-}}{N} = \frac{2}{3}$$

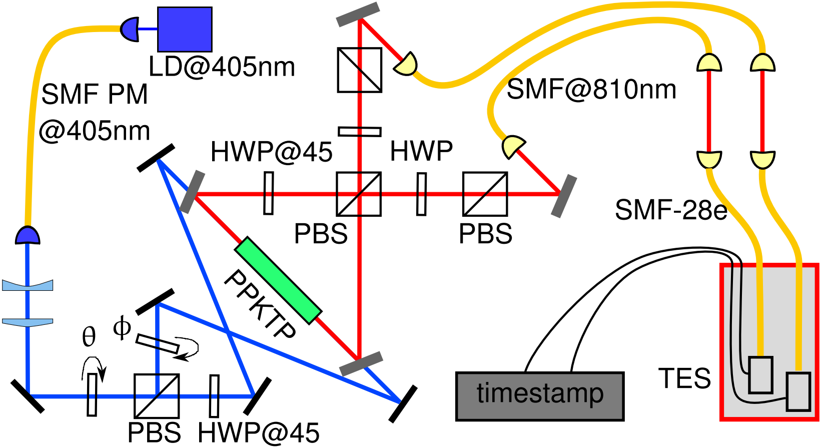


Correlation depends on bin width τ

$$E = \frac{N_{++} + N_{--} - N_{-+} - N_{+-}}{N} = -\frac{1}{9}$$



Experimental setup

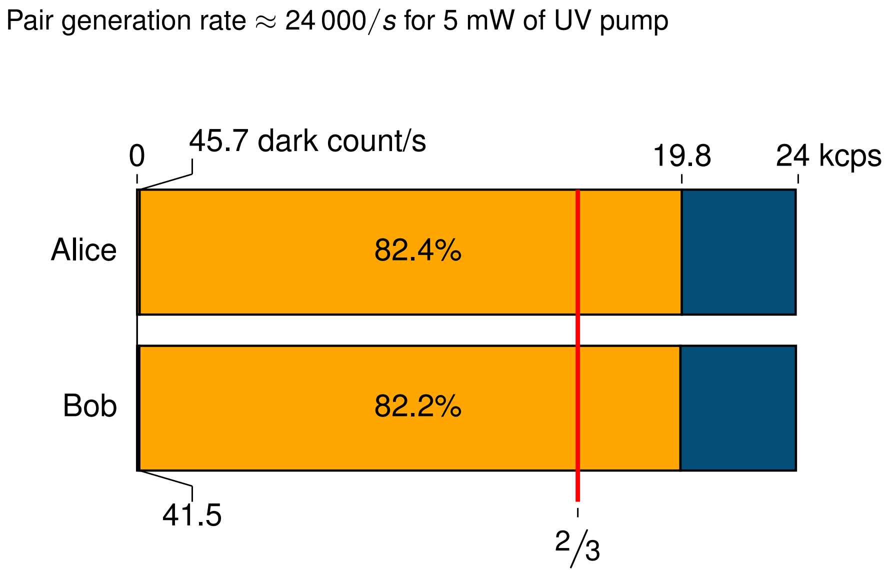


efficiency $> 98\%$

jitter $\approx 170ns$

$$|\psi\rangle = \cos\theta\,|HV\rangle - e^{i\phi}\sin\theta\,|VH\rangle$$

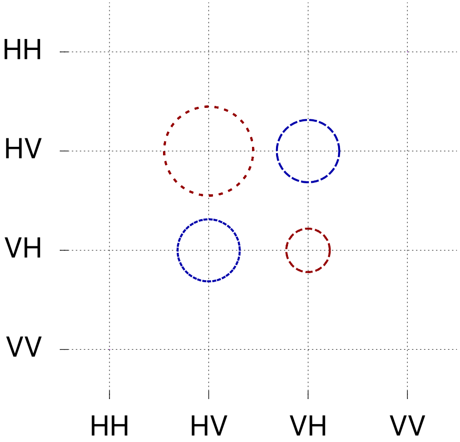
P. H. Eberhard, Phys. Rev.A(1993)



Pair generation rate ≈ 24 000/s for 5 mW of UV pump
45.7 dark count/s
0
19.8
24 kcps
Alice
82.4%
Bob
82.2%
41.5
2/3

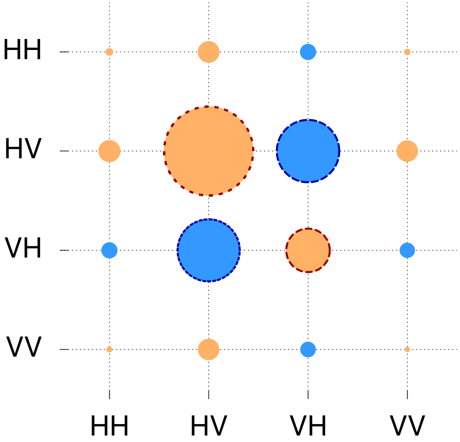
Optimal setting for loophole free Bell test - State

$$|\psi\rangle \approx 0.9\,|HV\rangle - 0.43\,|VH\rangle$$

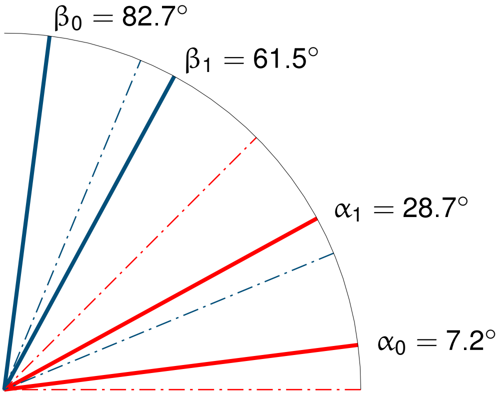


Optimal setting for loophole free Bell test - State

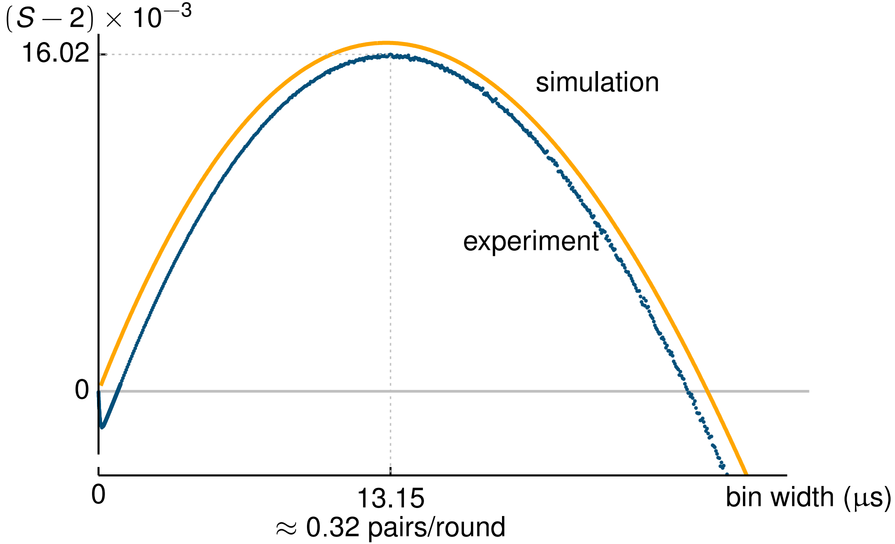
$$|\psi\rangle \approx 0.9\,|HV\rangle - 0.43\,|VH\rangle$$



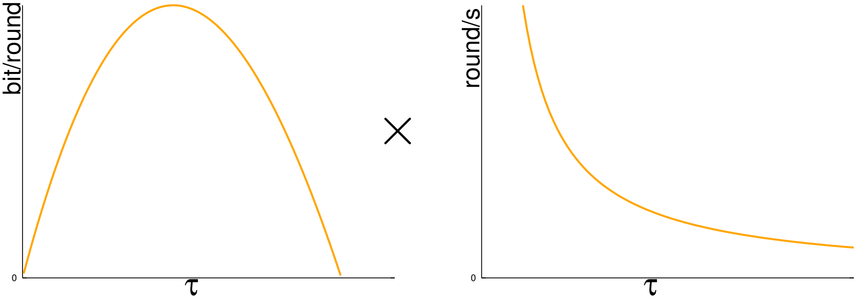
Optimal setting for loophole free Bell test - Projections

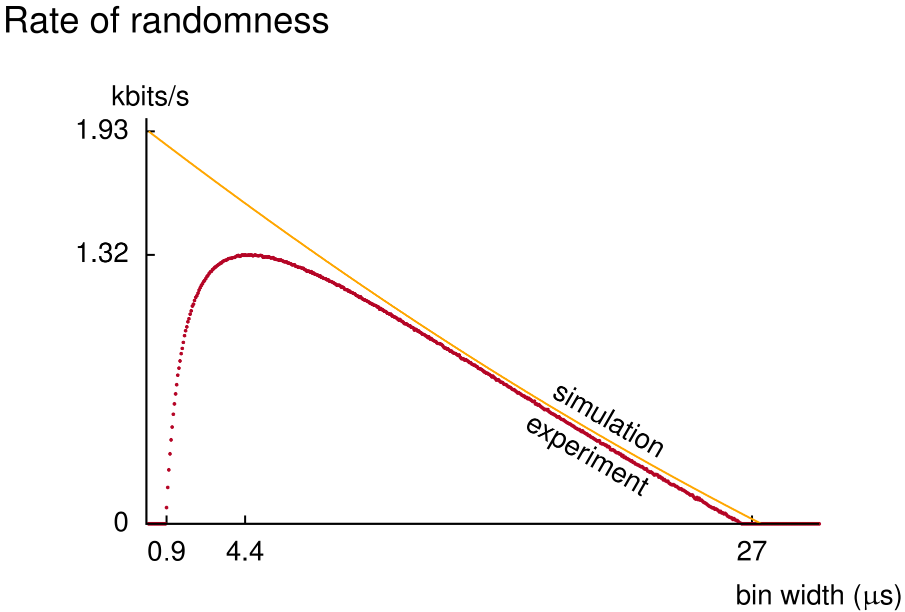


We observe a violation of $S = 2.01602(32)$



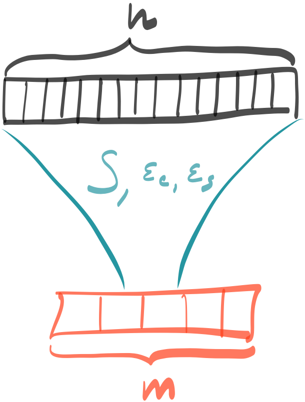
Rate of randomness





Rate of randomness
kbits/s
1.93
1.32
0
0.9
4.4
27
bin width (μs)
simulation
experiment

Finite statistics - Block extraction



$$m = n \cdot \eta_{\rm opt}(\varepsilon_c, \varepsilon_s) + 4 \log \frac{\epsilon_{EX}}{n} - 10$$

We choose

$$\varepsilon_c = \varepsilon_s = 10^{-10}$$

Trevisan extractor based on polynomial hashing with block weak design

In 26 min we generated 617 920 random bits (396 bits/s)

$\Rightarrow$

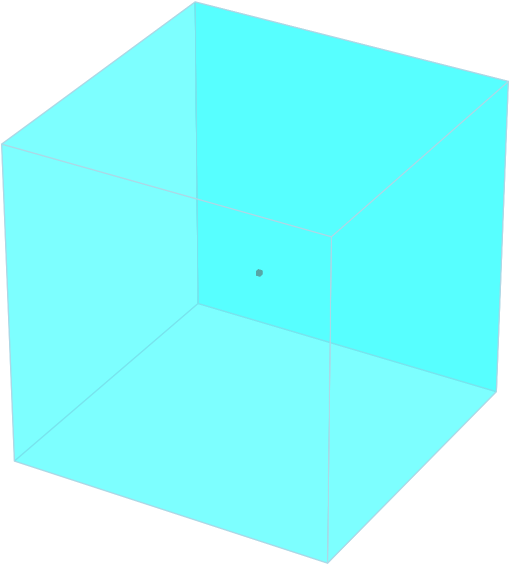
Processing time for 26mins data

26 mins data

$\downarrow$

9 hours processing

Processing time for 10 hours data



10 hours data

↓

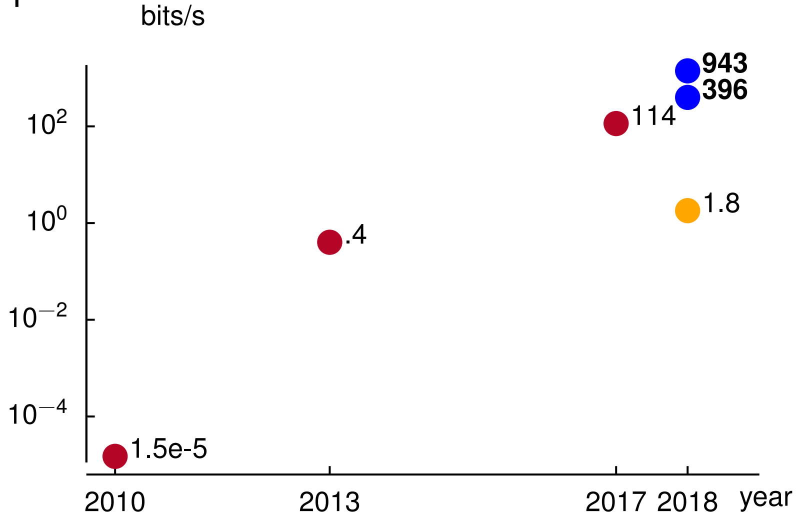
28 years processing

Toeplitz extractor

↓

943 bits/s in few hours

Our point to the state of the art



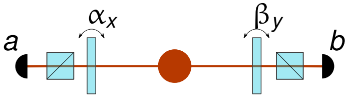
S. Pironio et al., Nature (2010)

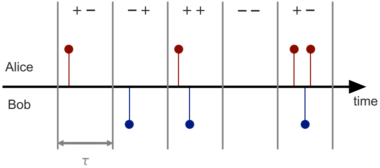
B. G. Christensen et al., PRL (2013)

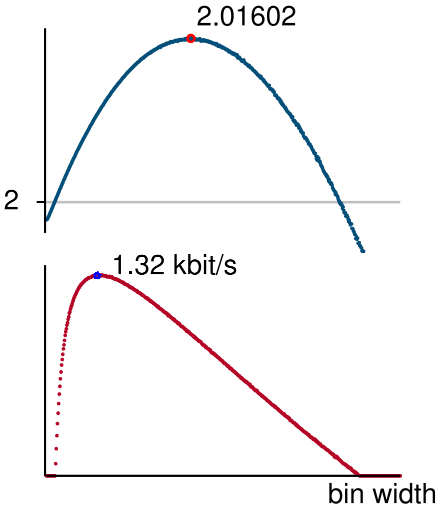
Y.Liu et al., PRL (2018)

P.Bierhorst et al.,Nature(2018)

Conclusion







arXiv:1805.02828

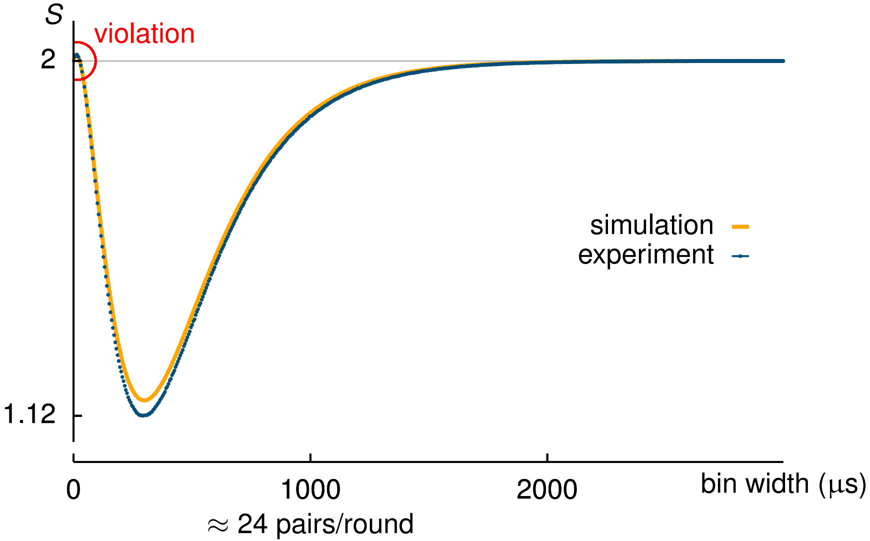
lijiong.shen@u.nus.edu

lijiong.shen@u.nus.edu

SUZHOU

lijiong.shen@u.nus.edu

Observed violation changes with τ



Rate of randomness with finite block size