Bell tests with Entangled Photons – what is left?

AQIS'15 satellite conference
KIAS, Seoul, 28-30 August 2015

Christian Kurtsiefer

Centre for Quantum Technologies

NUS National University of Singapore

Big News on the arXiv:

Quantum Physics

Experimental loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km

B. Hensen, H. Bernien, A.E. Dréau, A. Reiserer, N. Kalb, M.S. Blok, J. Ruitenberg, R.F.L. Vermeulen, R.N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D.J. Twitchen, D. Elkouss, S. Wehner, T.H. Taminiau, R. Hanson

(Submitted on 24 Aug 2015)

For more than 80 years, the counterintuitive predictions of quantum theory have stimulated debate about the nature of reality. In his seminal work, John Bell proved that no theory of nature that obeys locality and realism can reproduce all the predictions of quantum theory. Bell showed that in any local realist theory the correlations between distant measurements satisfy an inequality and, moreover, that this inequality can be violated according to quantum theory. This provided a recipe for experimental tests of the fundamental principles underlying the laws of nature. In the past decades, numerous ingenious Bell inequality tests have been reported. However, because of experimental limitations, all experiments to date required additional assumptions to obtain a contradiction with local realism, resulting in loopholes. Here we report on a Bell experiment that is free of any such additional assumption and thus directly tests the principles underlying Bell's inequality. We employ an event-ready scheme that enables the

Outline

- **Part I**: Implications of closing loopholes in Bell tests

  - Security against blinding attacks & friends in QKD

- **Part II**: Is |S|>2 the only challenge?

  - Tsirelson bound
  - Grinbaum bound

- **Part III**: An alternative way to assess the quantumness of a system

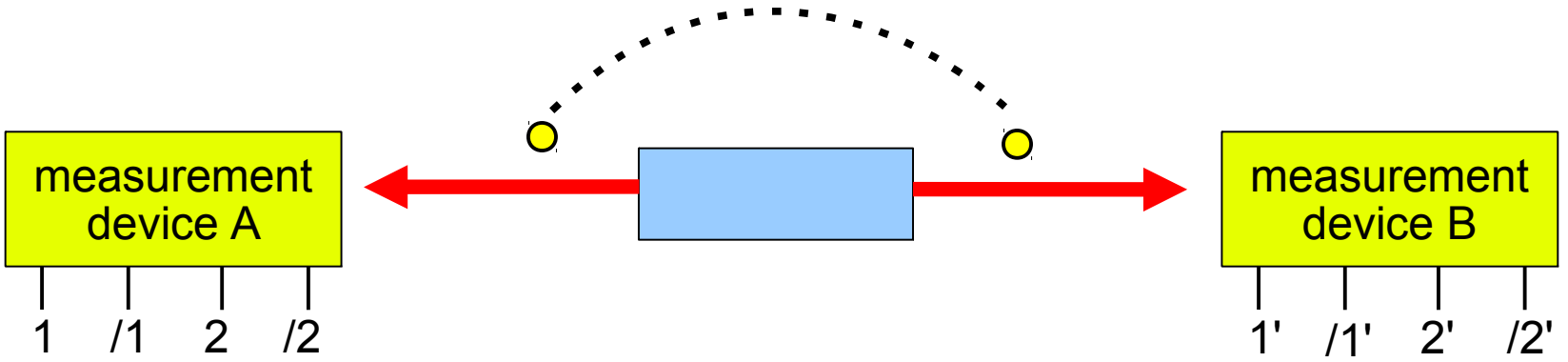
Part I: Bell tests and loopholes

- **History of Bell tests**

1972/74:	Freedman, Clauser: First tests
1981:	Aspect, Grangier, Roger: Choice of measurement
1998:	Weihs et al.: Locality loophole, random choice
2001:	Rowe et al.: Detection loophole with ions
2009:	Ansman et al: Detection loophole in SC qubits
2013:	Giustina et al.: Detection loophole for photons
2015:	Hanson team: All loopholes closed?

Ekert-91/ Device-independent protocol

Basic idea for QKD:



For proper settings 1, 2, 1', 2' and state $|\Psi^-\rangle$ $S = \pm 2\sqrt{2}$

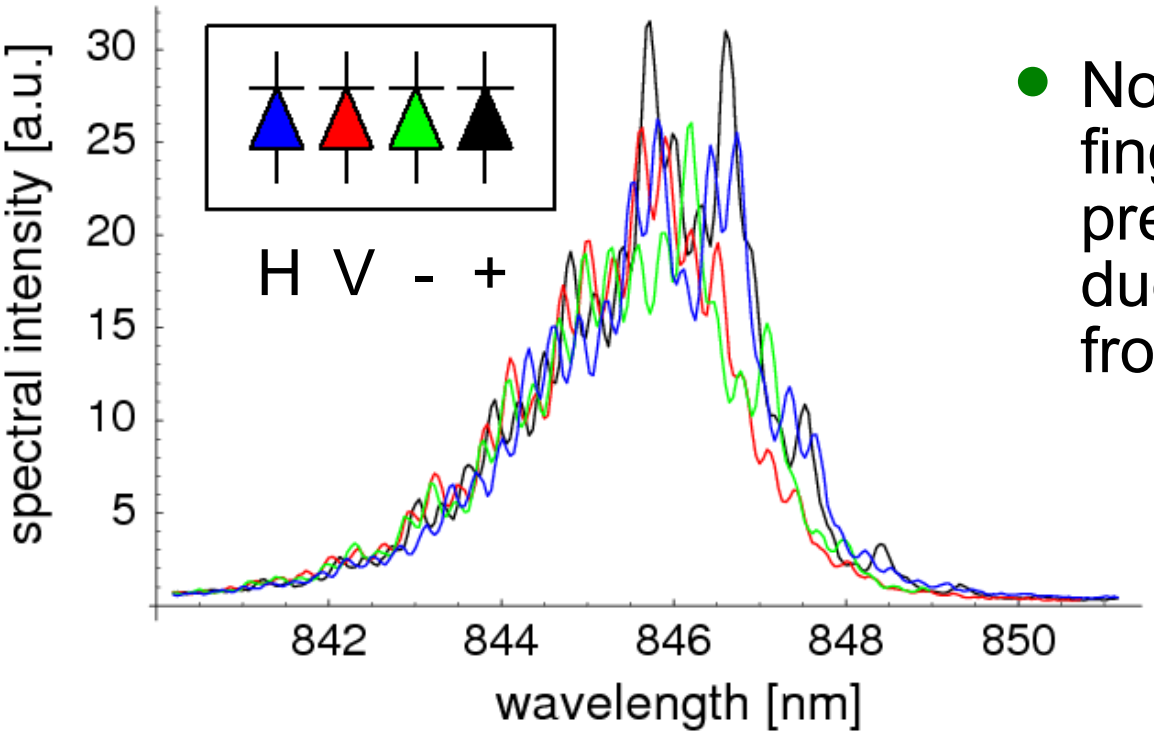
- Estimate quantitatively the knowledge of Eve of raw key between A and B from S:

$$I_E(S) = h\left(1 + \frac{\sqrt{S^2/4 - 1}}{2}\right)$$

- No fingerprint problems of photons due to side channels

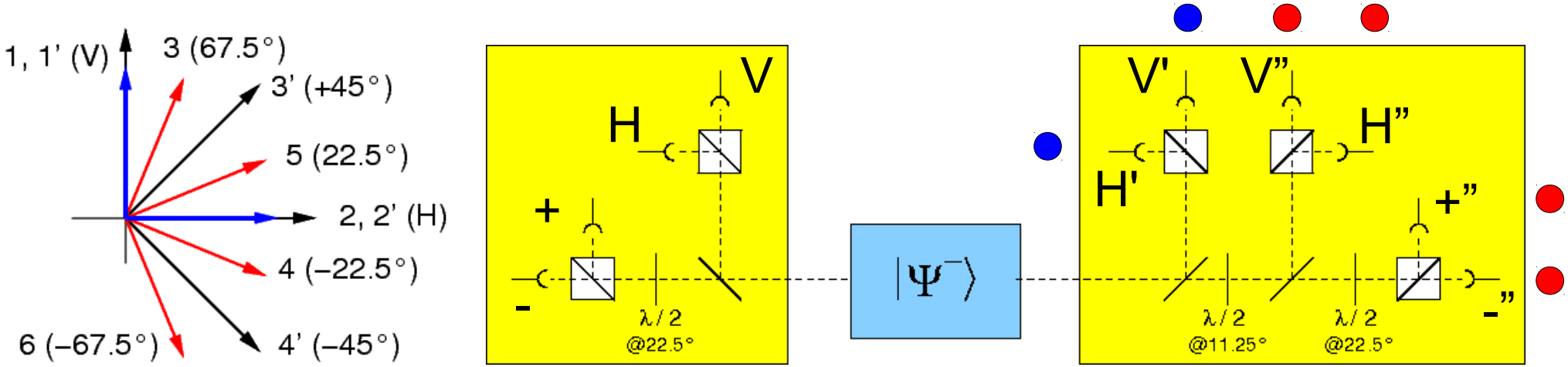
A. Acin, N. Brunner, N. Gisin,S. Massar, S. Pironio, V. Scarani, PRL 98, 230501 (2007)

Secure against (many) side channels...



- No spectral or other fingerprinting in prepare/send protocols due to independence from Hilbert space

Practical implementation

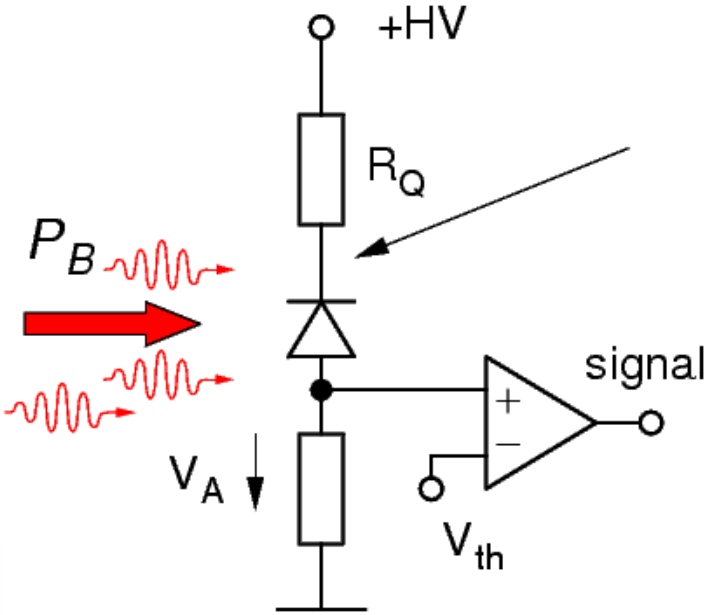


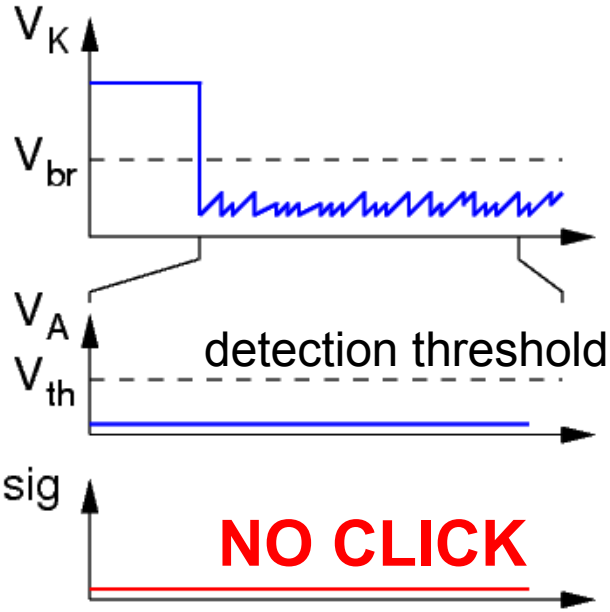
- {H,V; H',V'} coincidences → key generation
- {H,V,+,-;H",V",+",-"} coincidences → CHSH Bell test

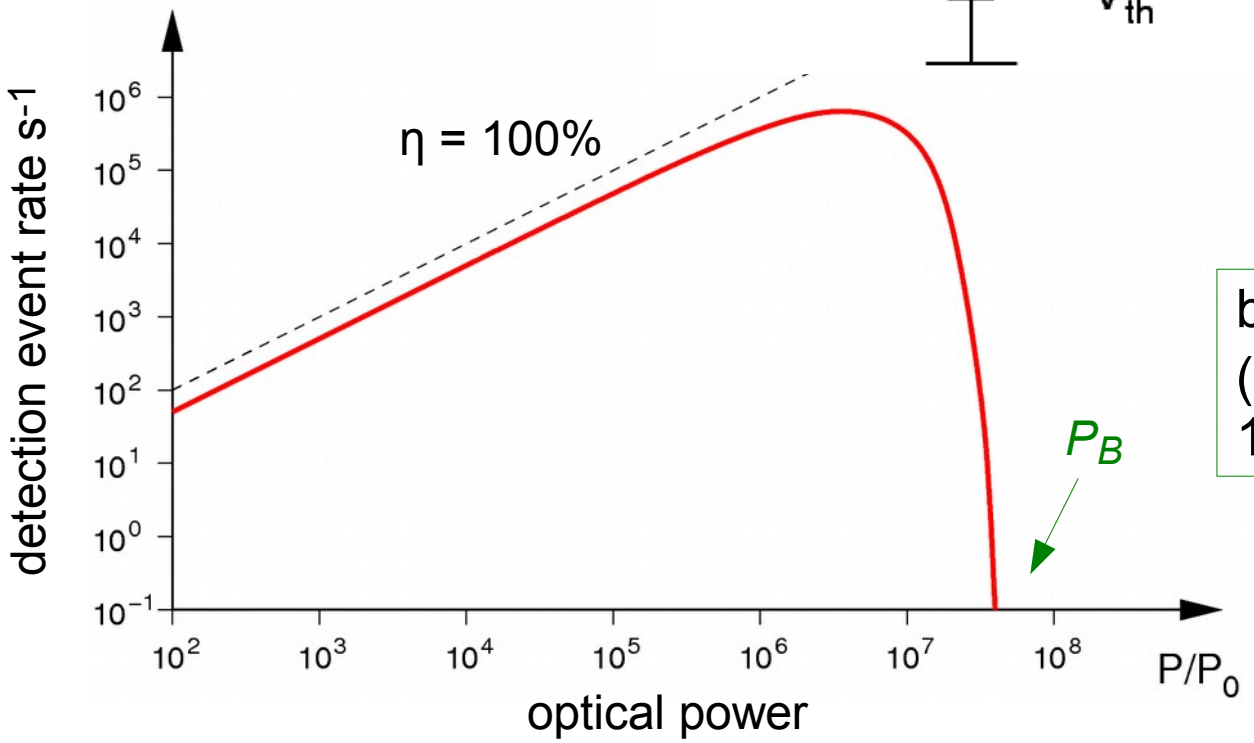
*A. Ling, M. Peoloso, I. Marcikic, V. Scarani, A. Lamas-Linares, CK; PRA **78**, 020301R, 2008*

Detector blinding attack, part 1

APD saturate and
can be blinded



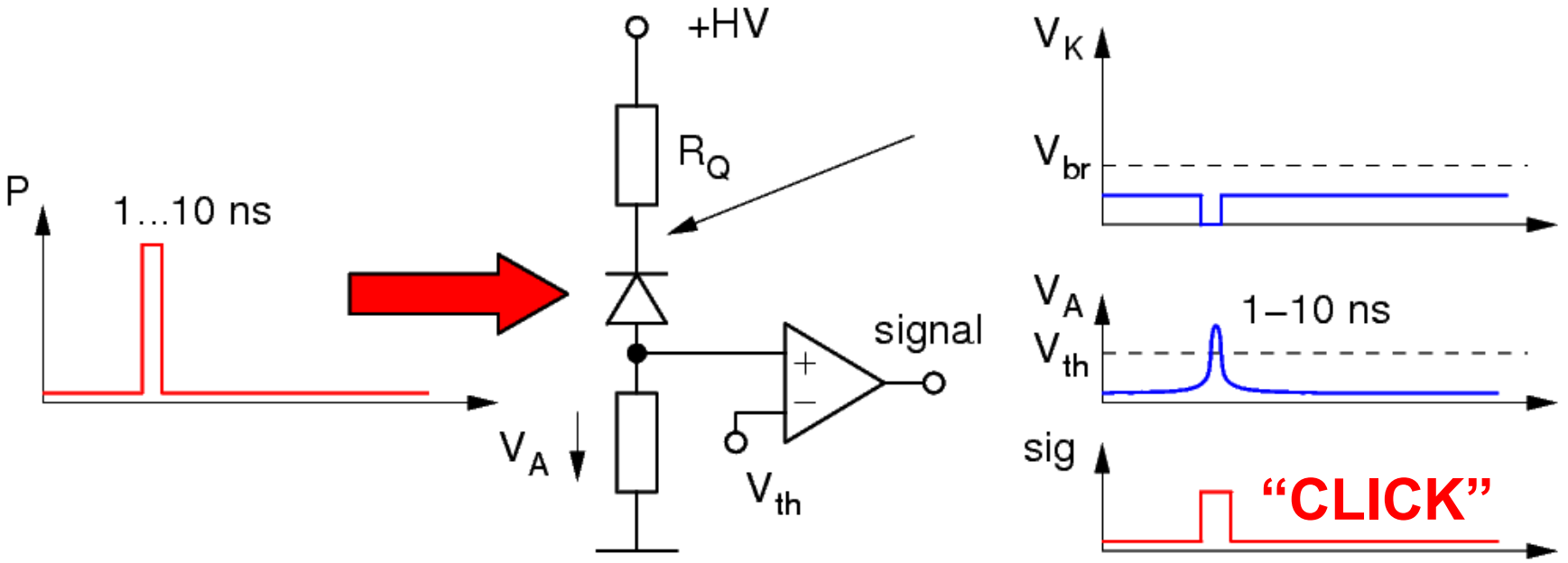




blinding power P_B: 1..10 pW
(corresponding to
10^6-10^7 events / sec)

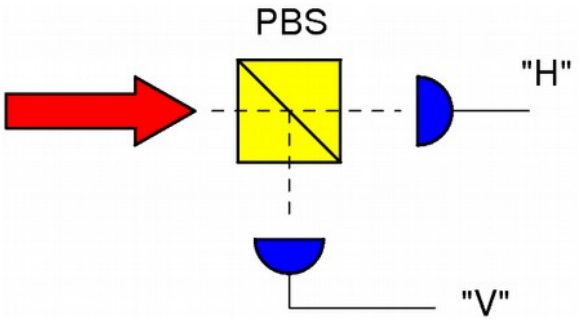
Detector blinding attack, part 2

...and forced to give a signal by bright light pulses:



Avalanche diode operates in PIN / normal amplification regime

Detector blinding attack, part 3

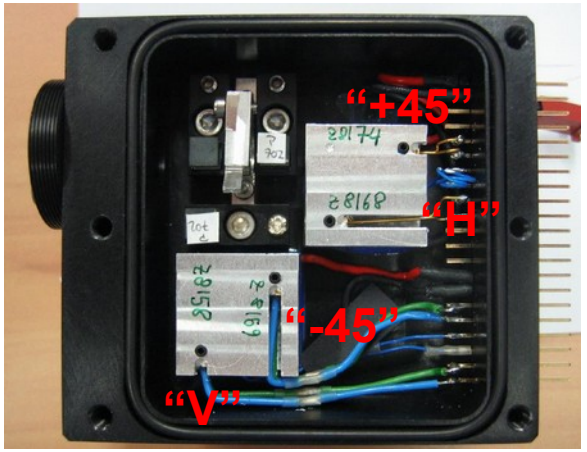


Choose unpolarized / circularly polarized P_1 and different linear polarizations P_2 to fake a 'click'

Light:	**“H” detector:**	**“V” detector:**
>2 P_B	no click	no click
+	click	no click
+	no click	click

Detector blinding attack, part 4

"faked state"



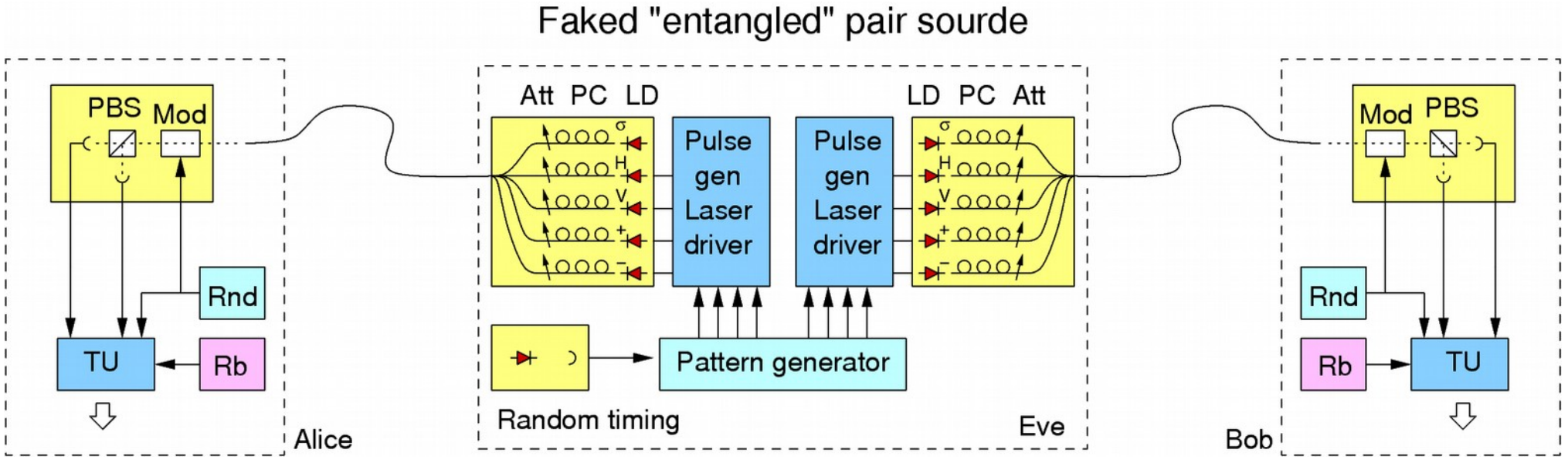
our polarization detector

Light:	"H"	"V"	"+45"	"-45"
>4 P_B	no click	no click	no click	no click
+	click	no click	no click	no click
+	no click	no click	click	no click

- Choose pulse amplitudes above +45 threshold, but below H/V threshold -- ideally 1- √2/2 margin for P_2

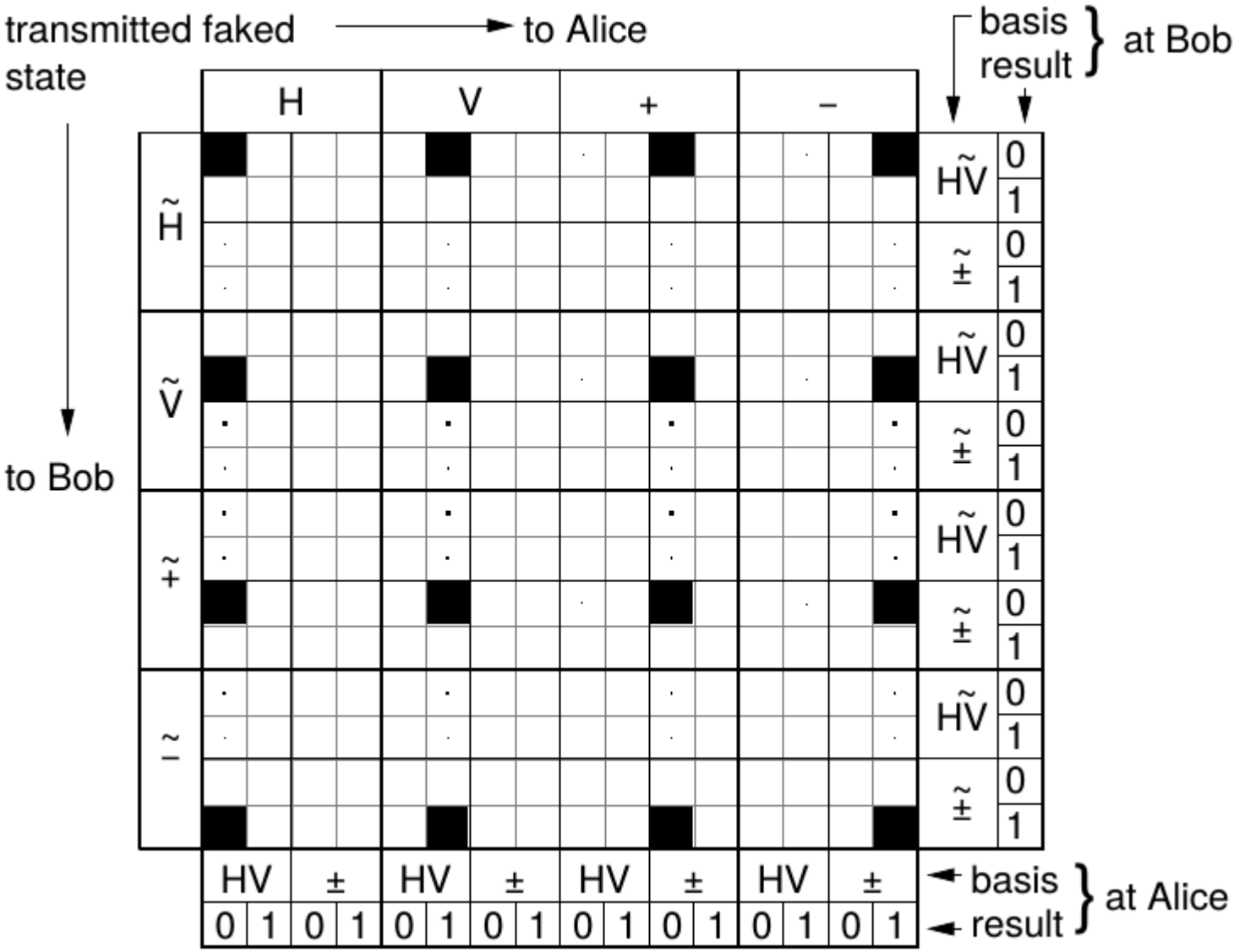
Faking the violation of a Bell inequality

(core part of device-independent QKD protocol)



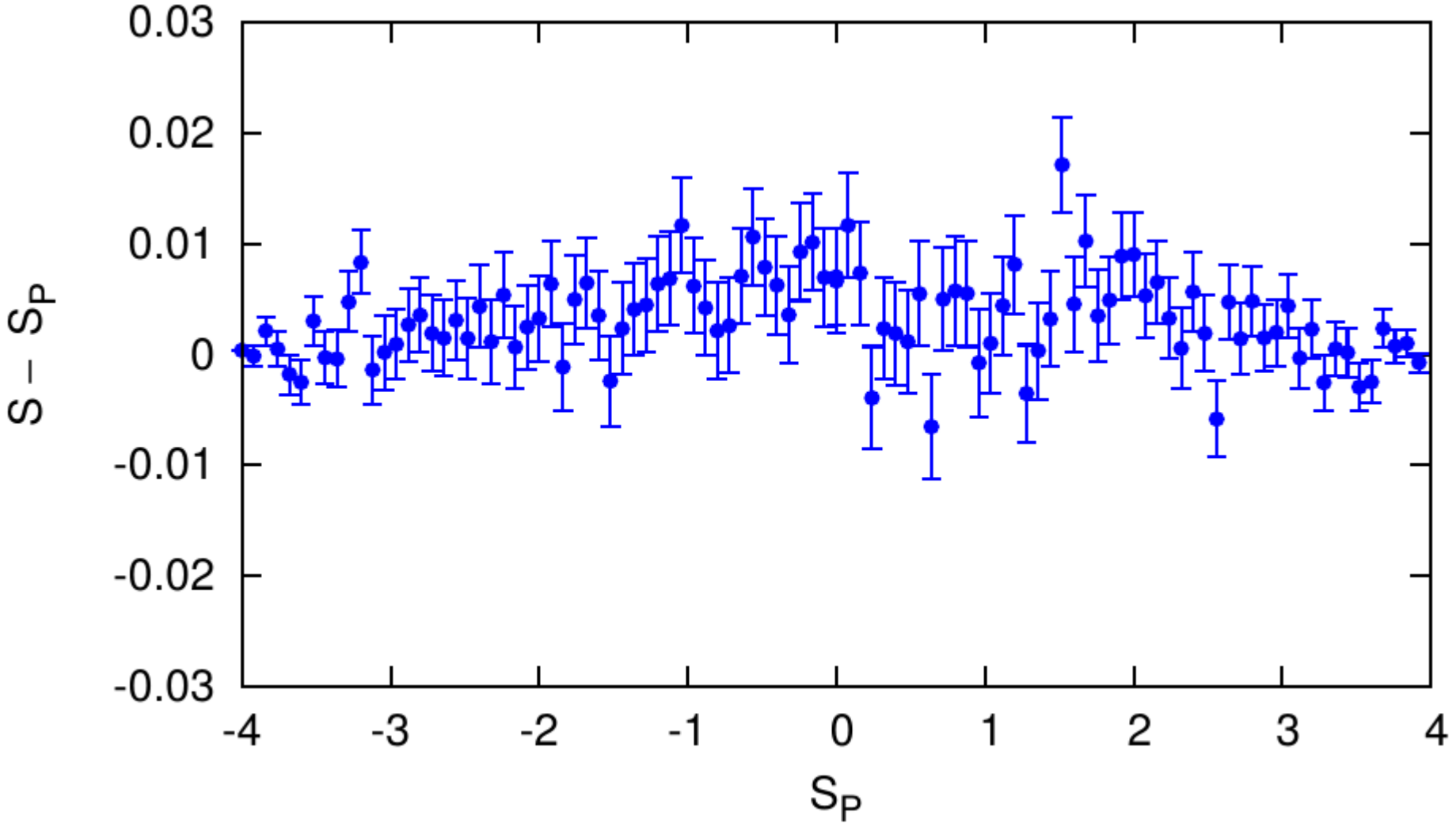
- Alice & Bob will see “programmed” correlations in 25% of the cases (base match on both sides), rest nothing
- Alice and Bob cannot distinguish from lossy line....
- We programmed (and found) CHSH results from S = -4 .... 4 with active choice

"Programming" measurement results



I. Gerhardt et al., Phys. Rev. Lett. ***111,*** *103001 (2011)*

Faked Bell results



How can DI-QKD break down?

- Losses in CHSH are removed by post-selecting pair observations using a fair sampling assumption
- Current pair sources (η = 70%) and detectors (η = 50% for non-cryogenic ones)
- Eve hides behind losses of transmission line. Best guess: optical fiber and ideal (η = 100%) detectors, active base choice: At 0.2dB/km@1550nm, T = 25% for *dist* = 30 km
- Only very short distances possible with current detectors

Can we expect all loopholes closed ?

Individually, they are all closed:

- Freedom of choice / Locality: Photons (Weihs et al. 1998)
- Detection loophole: Ions (Rowe et al. 2001), other systems

Few days ago

~~Probably later this year~~ all in a single experiment:

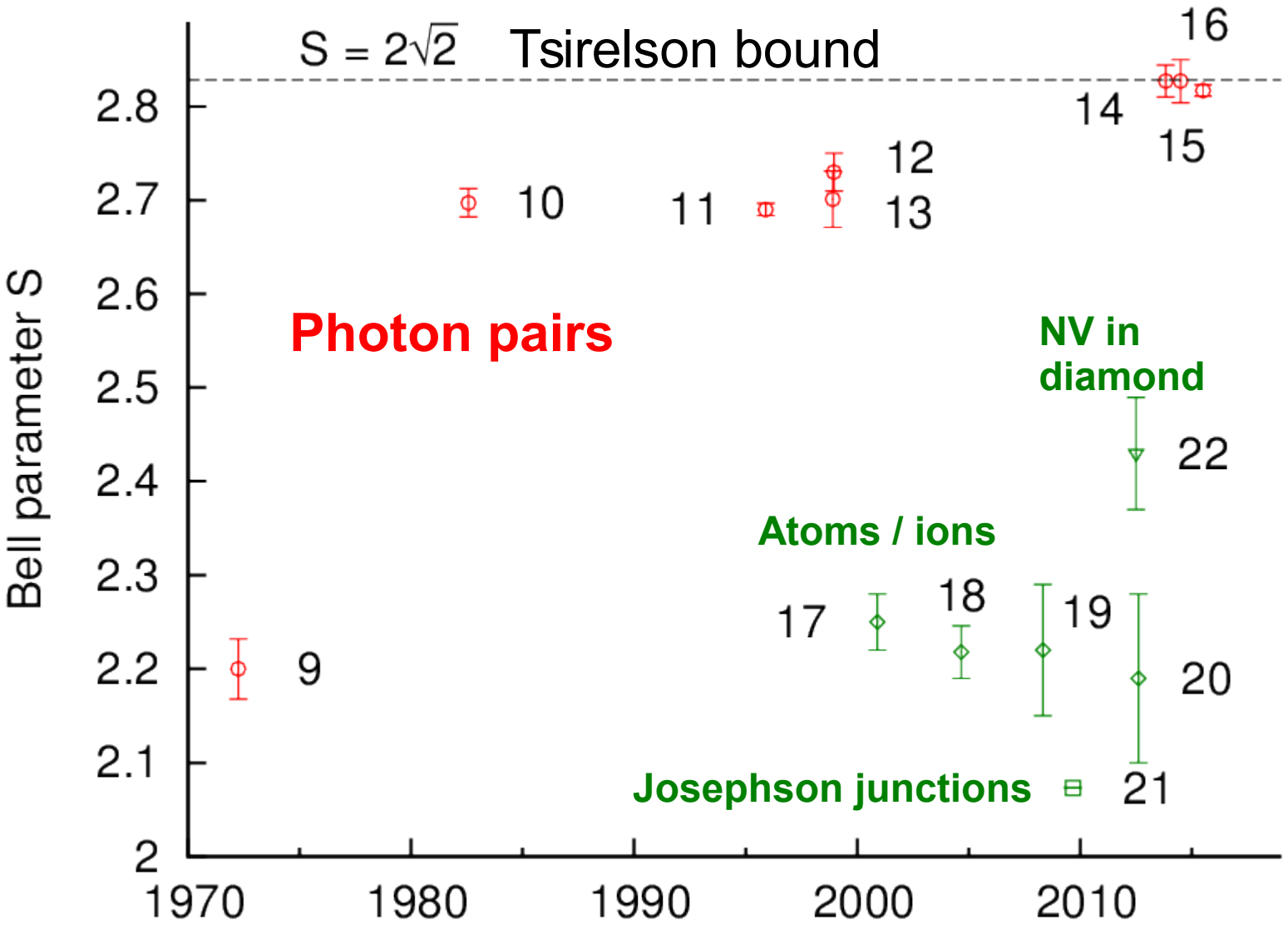
- NV centers in diamond (efficient detection, fast): Delft
- Photonic systems: Vienna, UIUC,...?
- Neutral atoms: Munich

Part II: Tests beyond $|S|<2$

- How well do you refute local variable theories? (higher signal/noise)

- How close can you reach the prediction of quantum physics?

Various Tests so far



Boris Cirel'son, Letters in Mathematical Physics ***4****, 93 (1980)*

Corresponding Photonic References

[9] S.J. Freedman and J.F. Clauser, *Phys. Rev. Lett.* ***28****, 938 (1972)*

[10] A. Aspect, P. Grangier, and G. Roger,
Phys. Rev. Lett. ***47****, 460 (1981)*

[11] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko,
and Y. Shih, *Phys. Rev. Lett.* ***75****, 4337 (1995)*

[12] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger,
Phys. Rev. Lett. ***81****, 5039 (1998)*

[13] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin,
Phys. Rev. Lett. 81, 3563 (1998)

[14] B.G. Christensen, K.T. McCusker, J.B. Altepeter, B. Calkins,
T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam,
N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat,
Phys. Rev. Lett. ***111****, 130406 (2013).*

[15] M. Nawareg, F. Bisesto, V. D'Ambrosio, E. Amselem, F. Sciarrino,
M. Bourennane, and A. Cabello, *arXiv:1311.3495 [quant-ph*]

[16] B.G. Christensen, Y.-C. Liang, N. Brunner, N. Gisin,
and P. G. Kwiat, *arXiv:1506.01649*

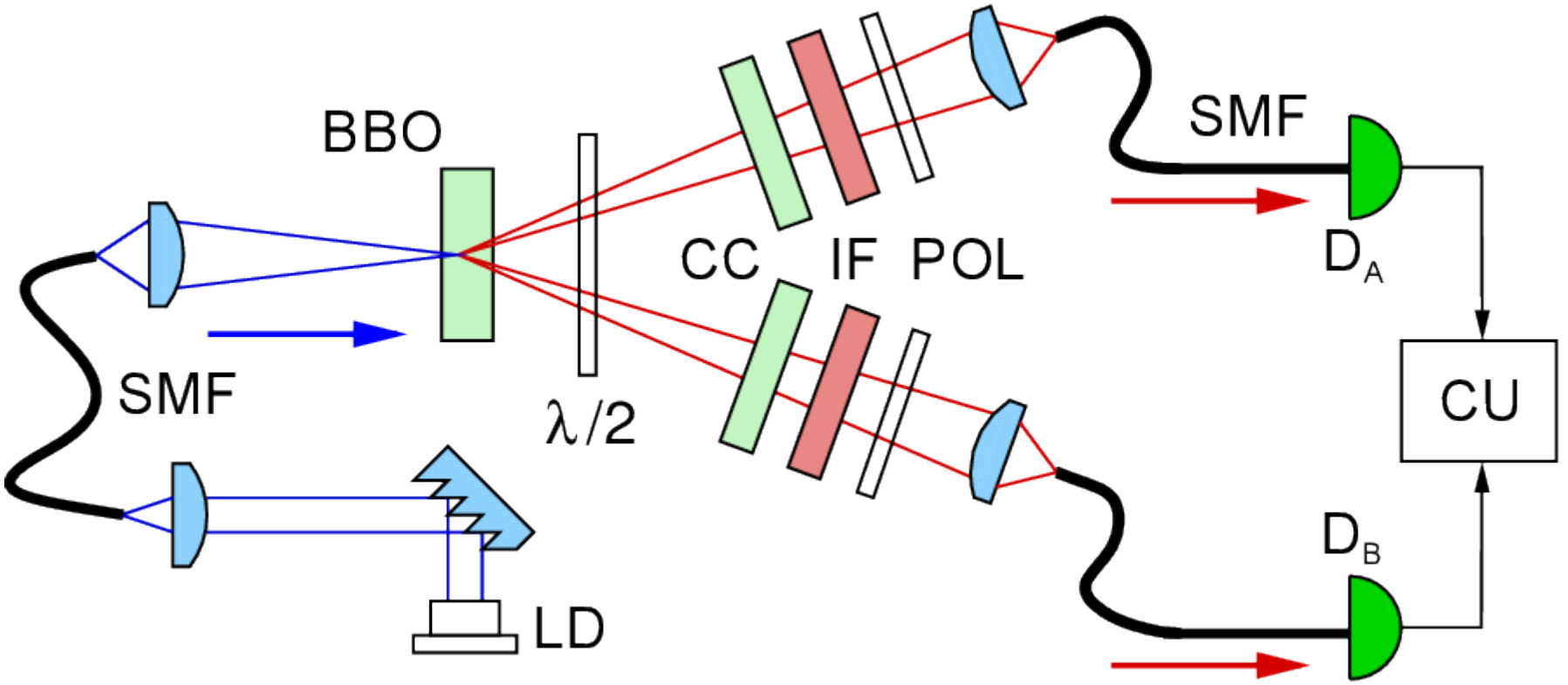
Grinbaum bound

- Assume an observer with limited string complexity
- Provides an alternative “underlying” description to observed phenomena that can be well approximated by Quantum physics in the “critical regime”.
- For binary codes describing bipartite systems, there is “strong evidence” for an upper bound on bipartite correlations”

$$|S| \leq 2.82537 = S_G \quad < \quad 2\sqrt{2} = S_T = 2.828427...$$

Alexei Grinbaum: Quantum Theory as a Critical Regime of Language dynamics Found. Phys. 2015, (doi: 10.1007/s10701-015-9937-y, arXiv:1501:02710)

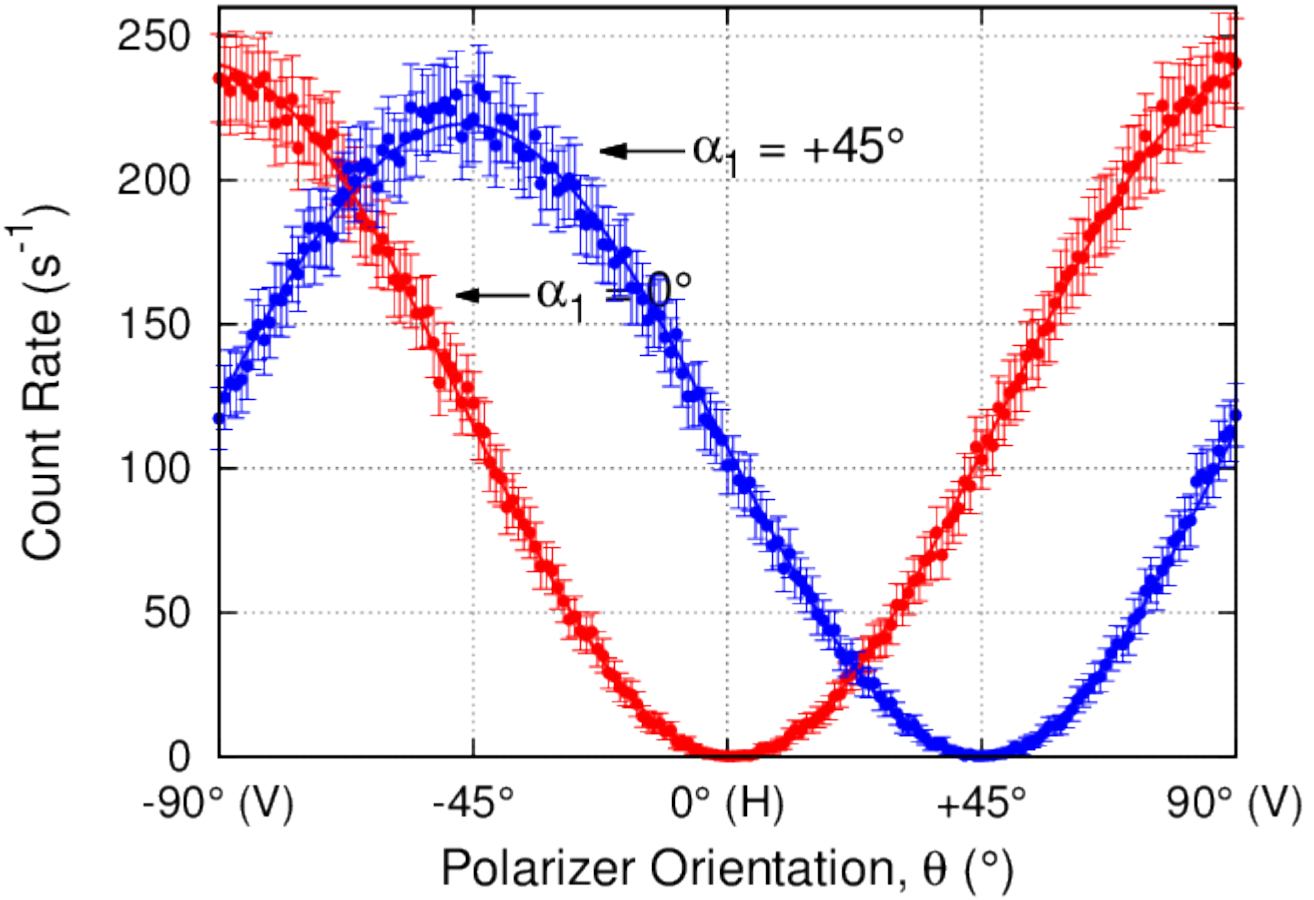
Experimental Setup



- Traditional Kwiat-95 type-II SPDC source
  weak pump, optimized for good balance, ~512 pairs/sec
- Very good polarizaton filters, find optimal measurement angles

Kwiat et al., Phys. Rev. Lett. ***75****, 4337 (1995)*

Visibility of polarization correlation



V_{HV} = 99.9 ± 0.1%

$V_{\pm 45}$ = 99.9 ± 0.1%

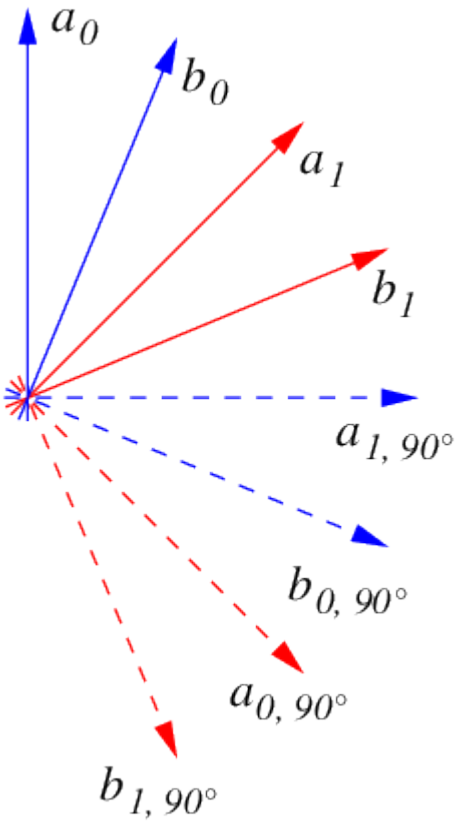
Other experimental details

- Low pump power: P=7mW leads to low accidental coincidences
  r_{coinc} ~ 560 events/sec
  r_{acc} ~ 0.0067±0.0025 events/sec

- Use good film polarization filters (better 1:10^4), low wedge errors

- Optimize setting a_0 / b_0 to minimize impact on detector inefficiencies (we find a_0= 1.9°, b_0=22.9° etc)

Evaluate maximal CHSH Bell violation



- Choose optimal measurement directions $a_{0,\,1}$ and $b_{0,\,1}$ for

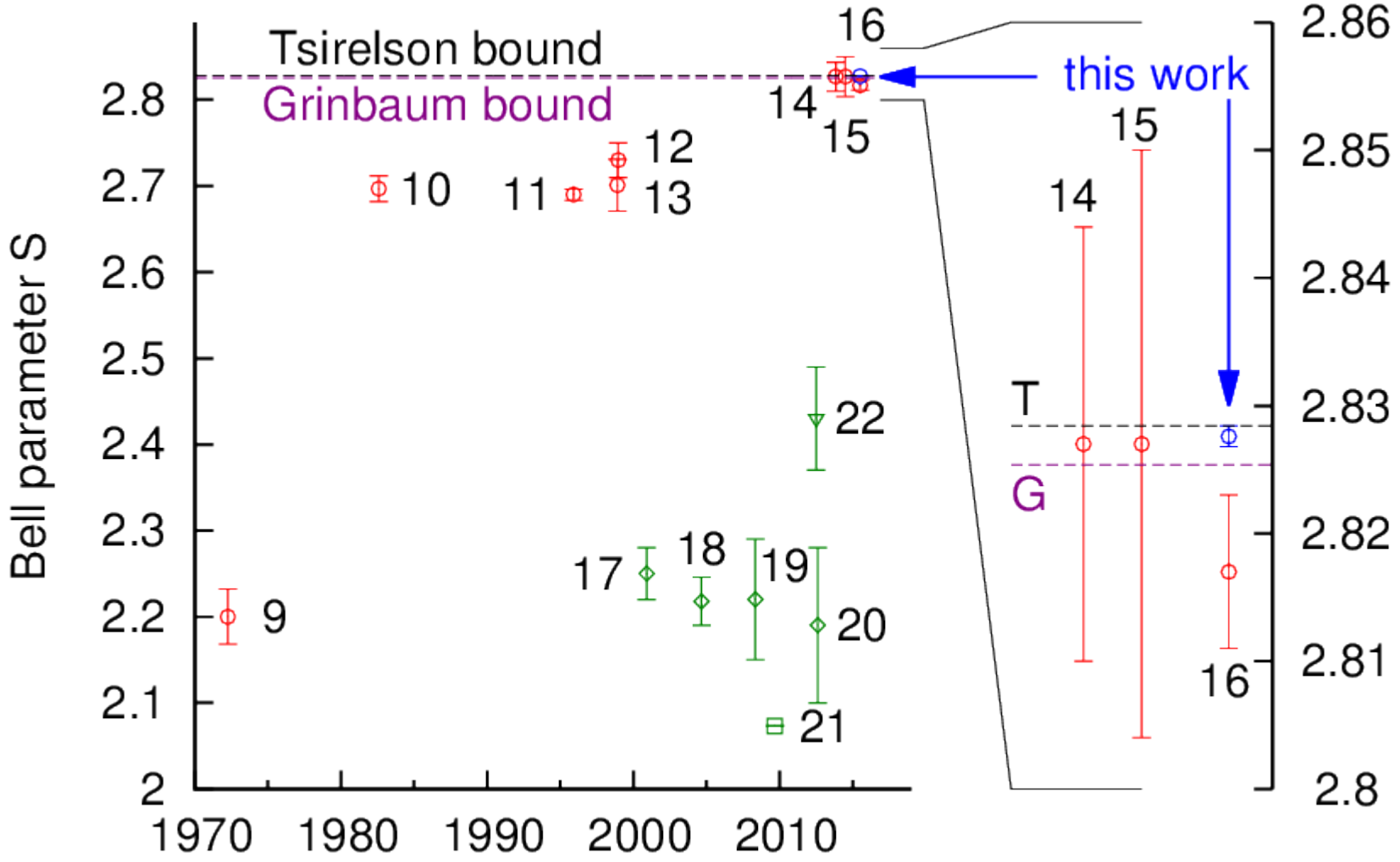
$$S = E(a_0, b_0) + E(a_0, b_1) + E(a_1, b_1) - E(a_1, b_1)$$

- Evaluate correlations E from coincidence events N between different analyzer settings:

$$E(a_0, b_0) \approx \frac{N(a_0, b_0) - N(a_{0,+90^\circ}, b_0) - N(a_0, b_{0,+90^\circ}) + N(a_{0+90^\circ}, b_{0,+90^\circ})}{N(a_0, b_0) + N(a_{0,+90^\circ}, b_0) + N(a_0, b_{0,+90^\circ}) + N(a_{0,+90^\circ}, b_{0,+90^\circ})}$$

- Propagate errors on N into S, assume $\Delta N_i = \sqrt{N_i}$

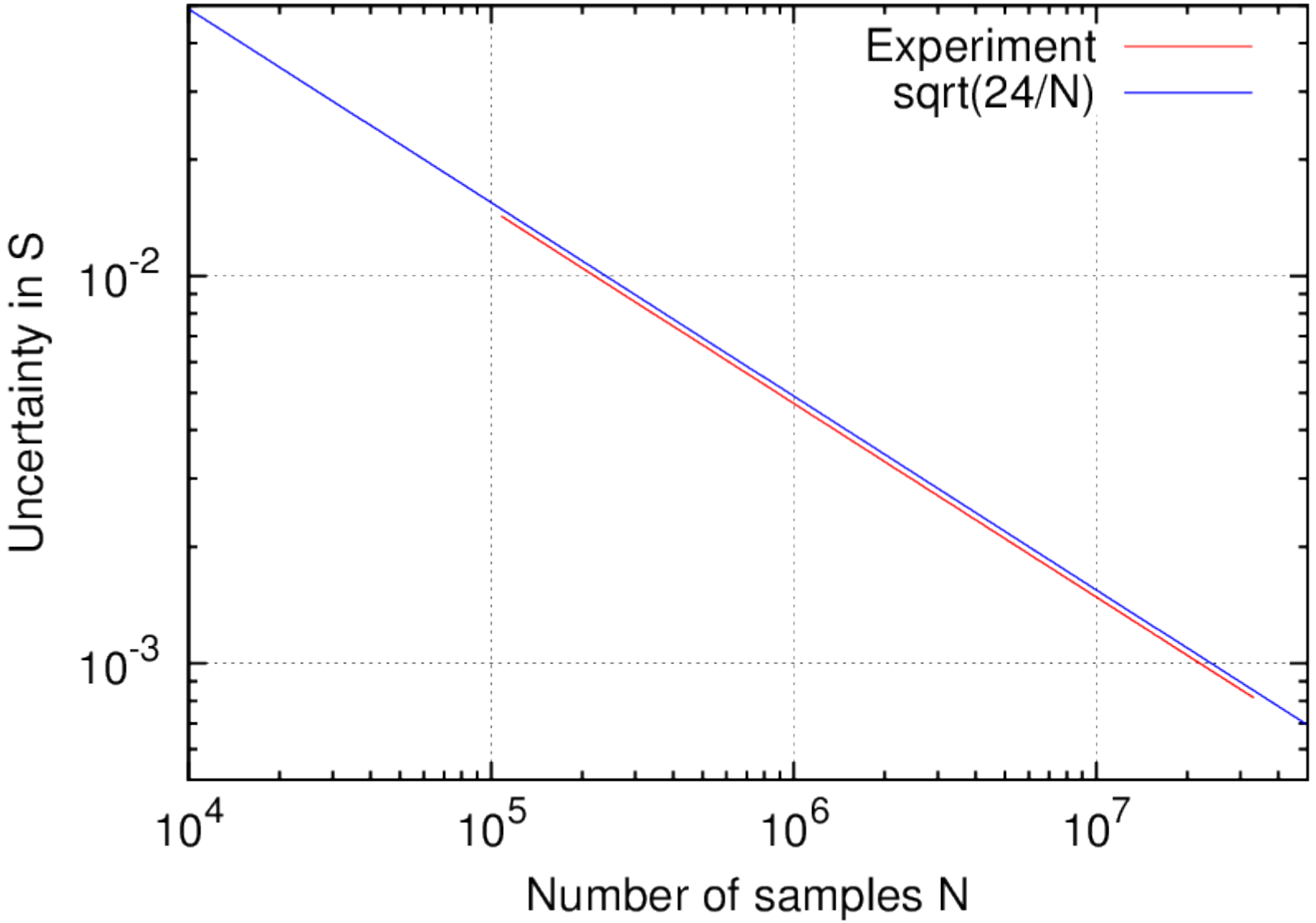
Comparison, with this work



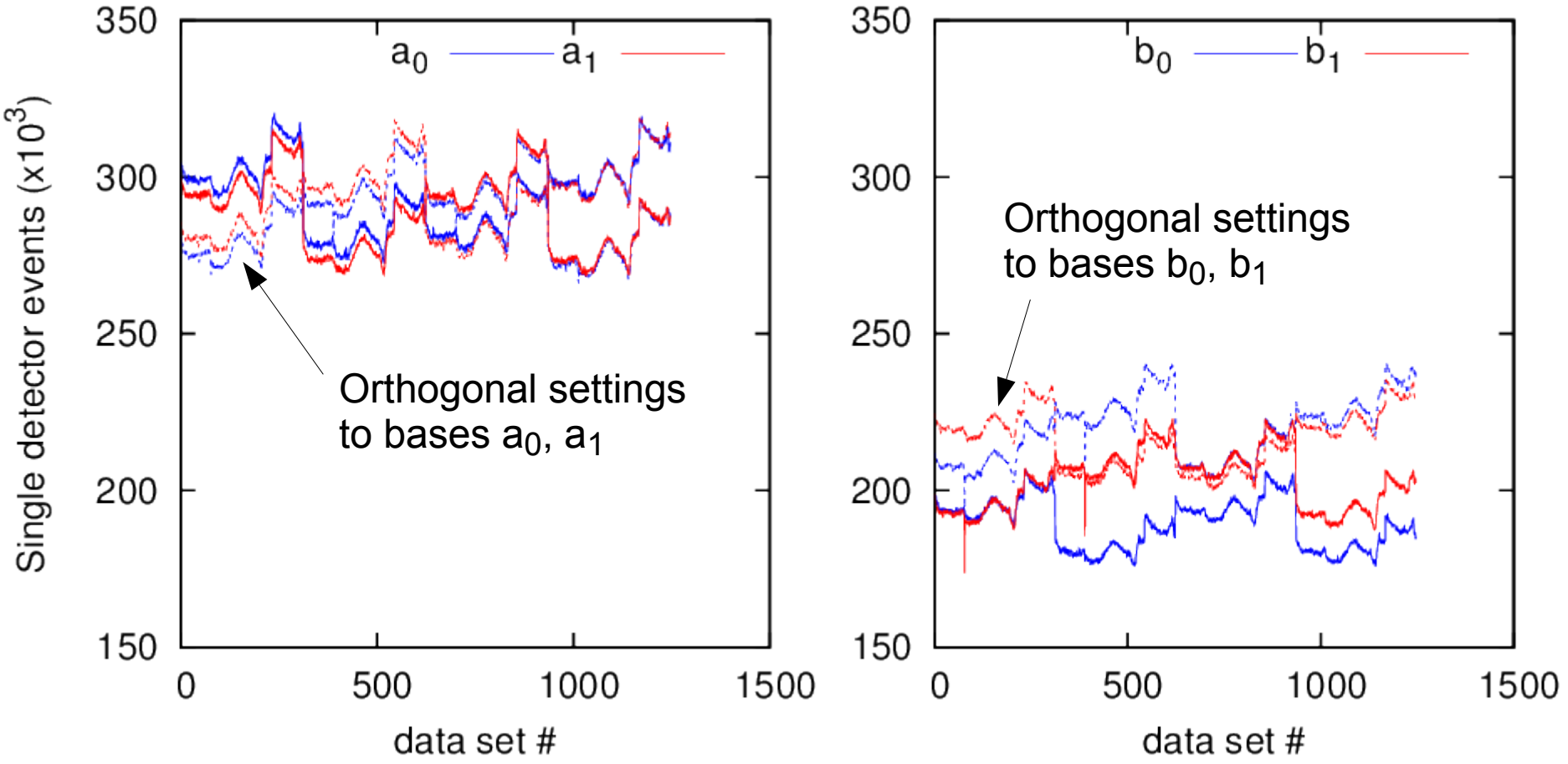
$S = 2.8274 \pm 0.00082$ or $|S - 2\sqrt{2}| = 0.0008 \pm 0.00082$

H.S. Poh, S.K. Joshi, A. Cere, A. Cabello, C.K., arXiv:1506.01865

Do we see really Poisson statistics?



Systematic errors



- Different filter settings result in different detector efficiencies
- These efficiencies drift (slowly) over time (pump freq drift)
- All slow drifts will *lower* the degree of violation

Correcting for different efficiencies?

- Extract different detector efficiencies from single/pair variations
- Correct count rates for efficiencies accordingly

$$S_C = 2.8281 \pm 0.0031$$

Error increase comes from estimating efficiencies of detectors, would not be able to exceed Grinbaum limit statistically significantly:

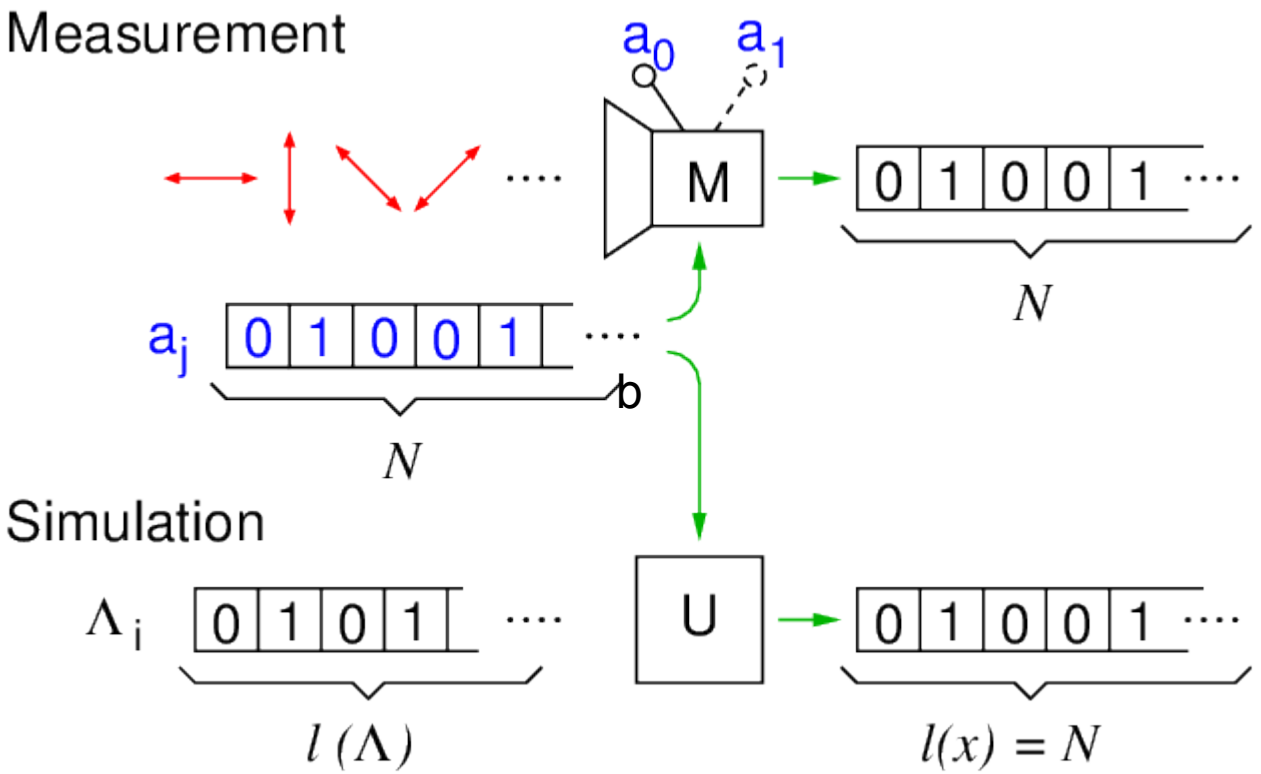
$$S_C - S_G = 0.0027 \pm 0.0031$$

$$S_T - S_C = 0.0003 \pm 0.0031$$

Part III: Compressibility tests

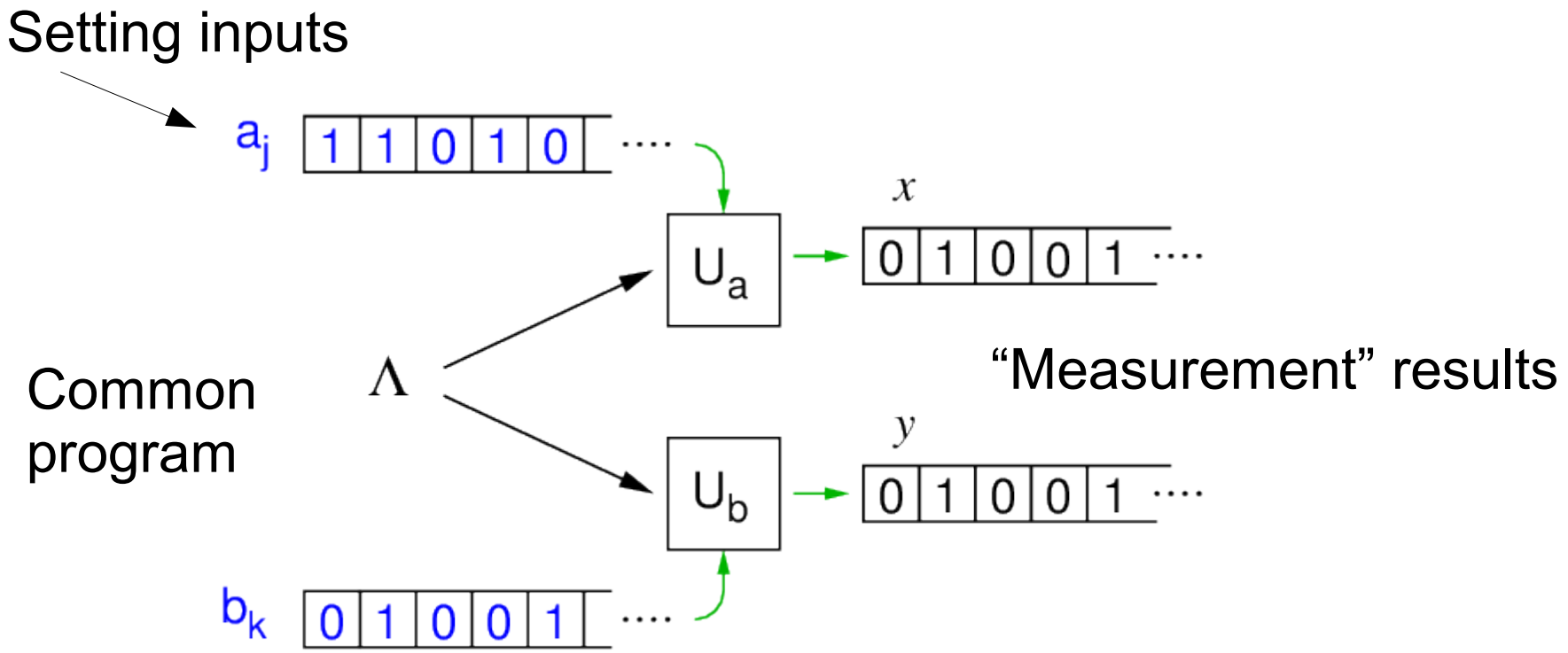
- Consider the physical world as a Turing machine and evaluate correlations via complexity in of measurement results
- Evaluate complexity via Normalized Information Distance
- Approximate NID by normalized compressibility distance (NCD)

Turing model of a simple system



Measurement result is string x of length l

Model of a correlated bipartite system



Information distance

- Normalized information distance between two strings x, y:

$$NID(x,y) = \frac{K(x,y) - min[K(x), K(y)]}{max[K(x), K(y)]}$$

Kolmogorov complexity

Length of shortest program that generates the joint string $(x\ ,\ y)$ (concatenation of x and y)

M. Li, X. Chen, X. Li, B. Ma, P.M.B. Vitàny, IEEE Trans. On Inf. Theory ***50****, 3250 (2004)*

Triangle inequality

- Correlation strings (x, y) for different settings $a_{0,1}$ and $b_{0,1}$:

$$NID(x_{a_0}, y_{b_0}) + NID(x_{a_1}, y_{b_0}) + NID(x_{a_1}, y_{b_1}) \geq NID(x_{a_0}, y_{b_1})$$

- Introduce testable quantity S:

$$S' = NID(x_{a_0}, y_{b_1}) - NID(x_{a_0}, y_{b_0}) - NID(x_{a_1}, y_{b_0}) - NID(x_{a_1}, y_{b_1})$$

- For a physical system that is governed by the Turing model:

$$S' \leq 0$$

Approximate Kolmogorov complexity

- Statistical approach:

$$\langle NID(x,y)\rangle = \frac{H(x,y) - min[H(x), H(y)]}{max[H(x), H(y)]}$$

- Results in an entropic inequality of Braunstein/Caves

S.L. Braunstein, C.M. Caves, Phys. Rev. Lett. ***61,*** *662 (1988)*

- Interpretation and test requires assumption of *identically independently distributed* outputs of the system

Algorithmic approach

- Approximate NID by Normalized Compression Distance

$$NID(x,y) \approx NCD(x,y)$$

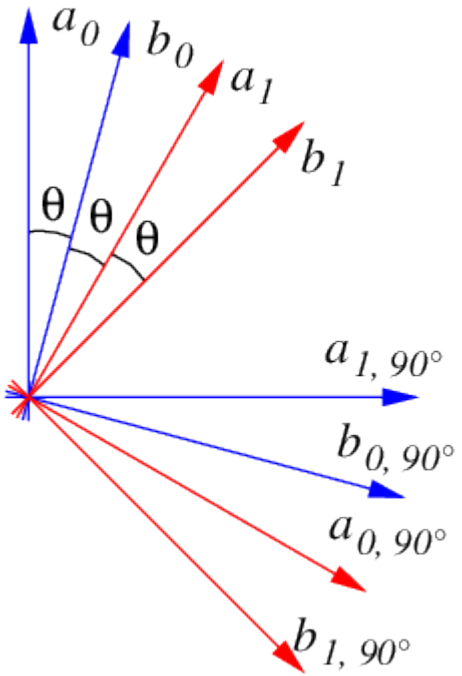
$$NCD(x,y) = \frac{C(x,y) - min[C(x), C(y)]}{max[C(x), C(y)]}$$

Length of compressed outcome strings

- Triangle inequality can be tested experimentally:

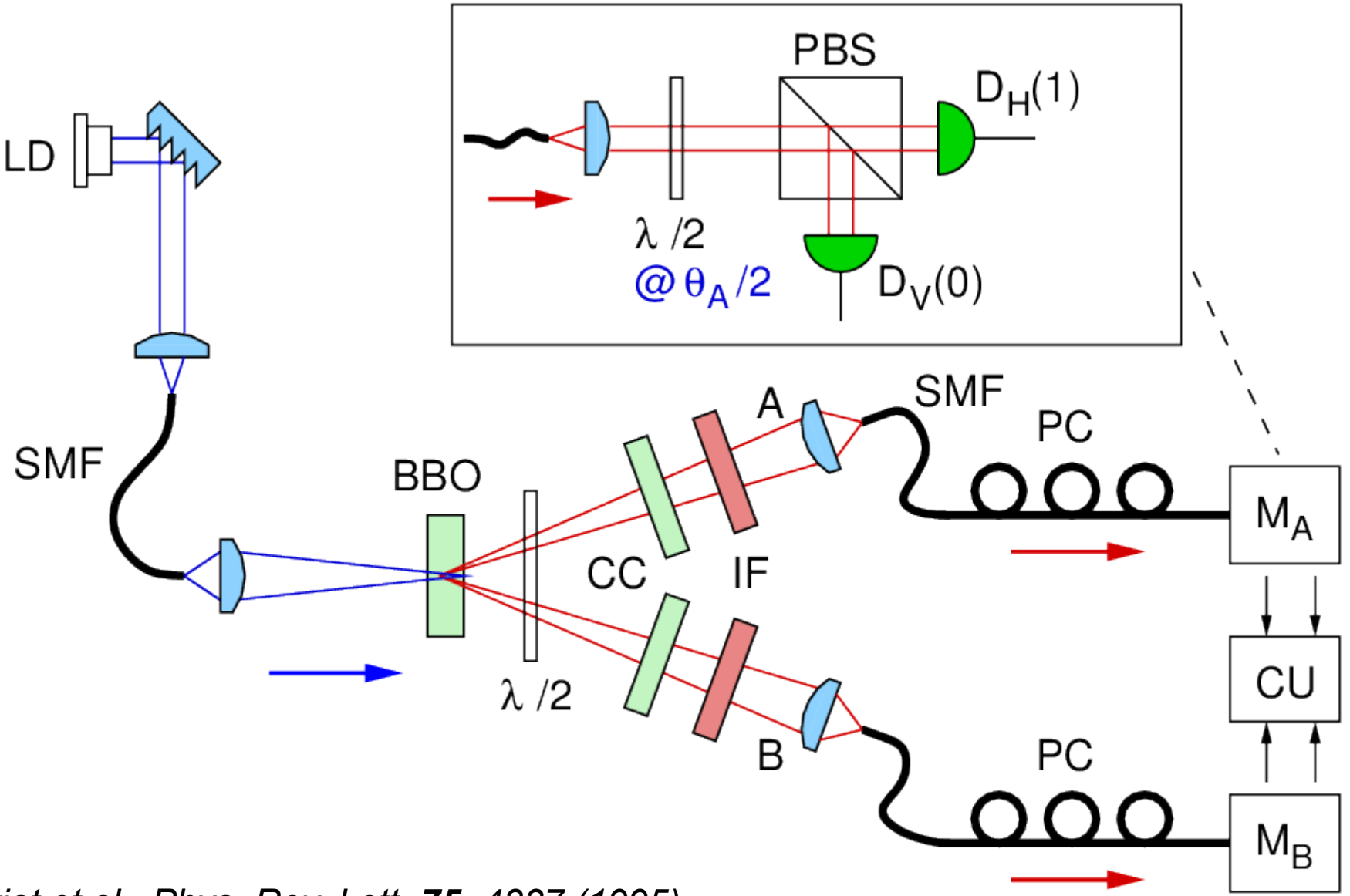
$$S = NCD(x_{a_1}, y_{b_0}) - NCD(x_{a_0}, y_{b_0}) - NCD(x_{a_0}, y_{b_1}) - NCD(x_{a_1}, y_{b_1}) \leq 0$$

What to test?



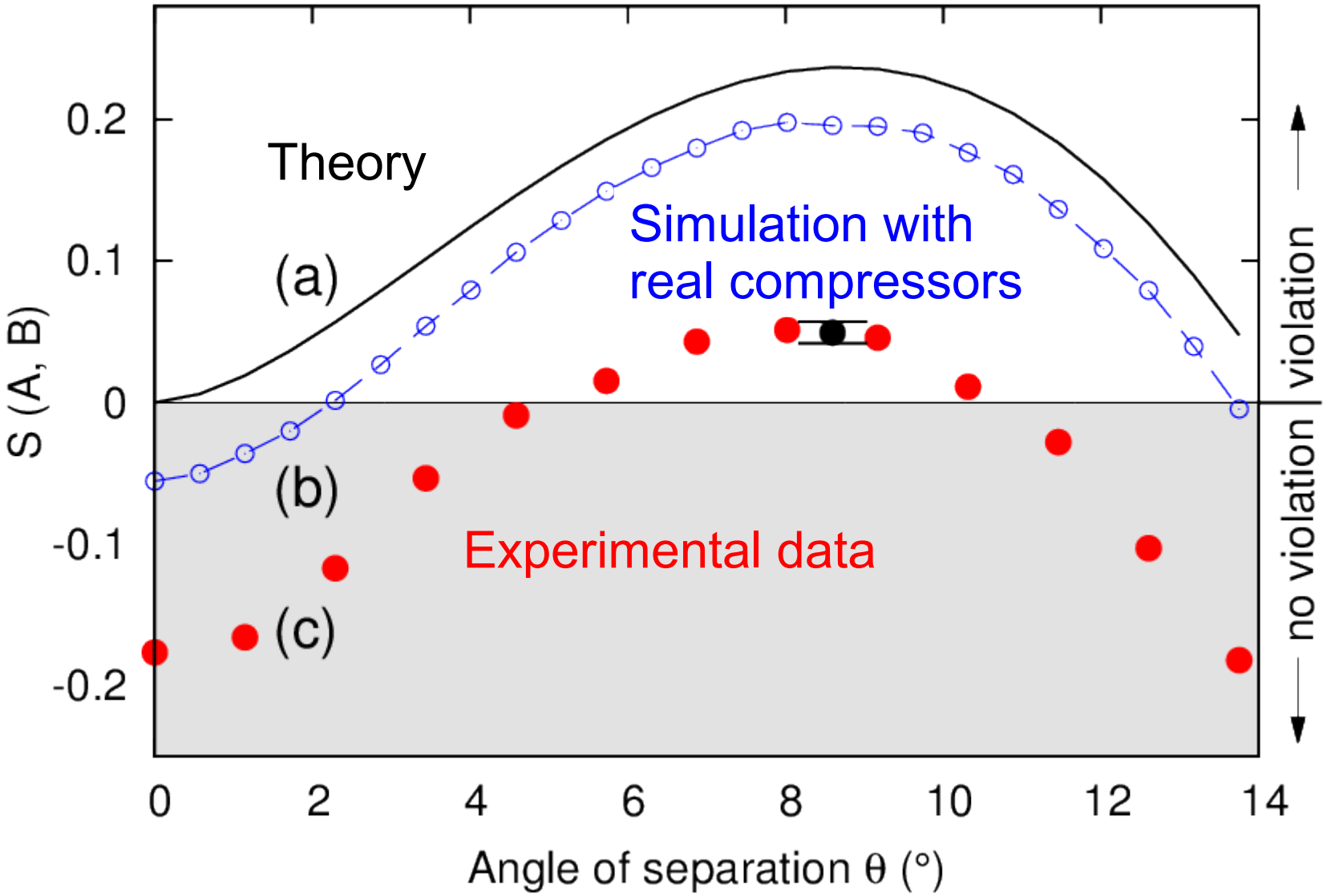
- Choose measurement suitable measurement directions $a_{0,1}$ and $b_{0,1}$
- Optimal angle: θ = 8.6°
- Record joint and single measurement outcomes for both sides, forming strings x and y
- Compress and determine S

Experimental setup



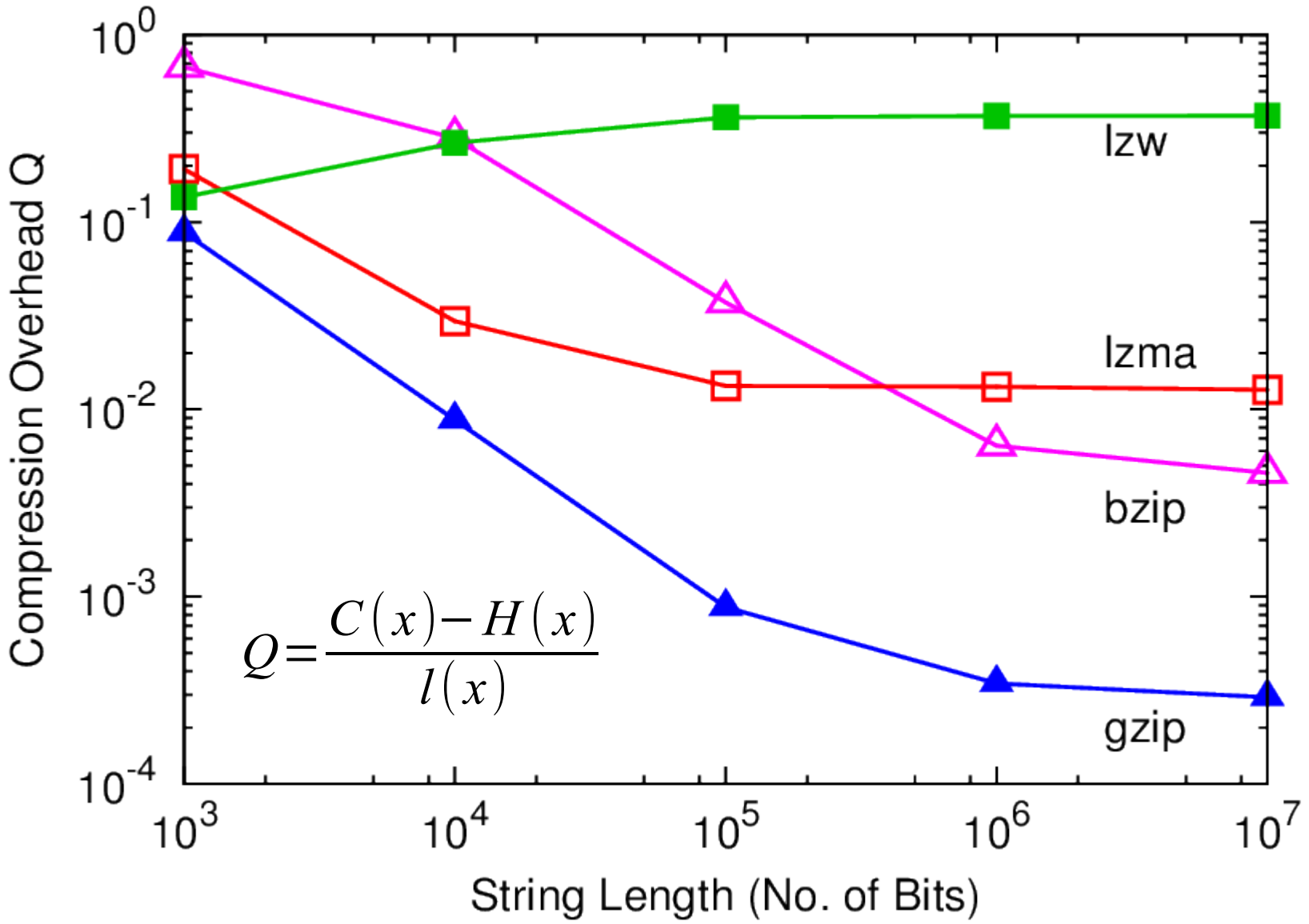
Kwiat et al., Phys. Rev. Lett. ***75****, 4337 (1995)*

Compression results

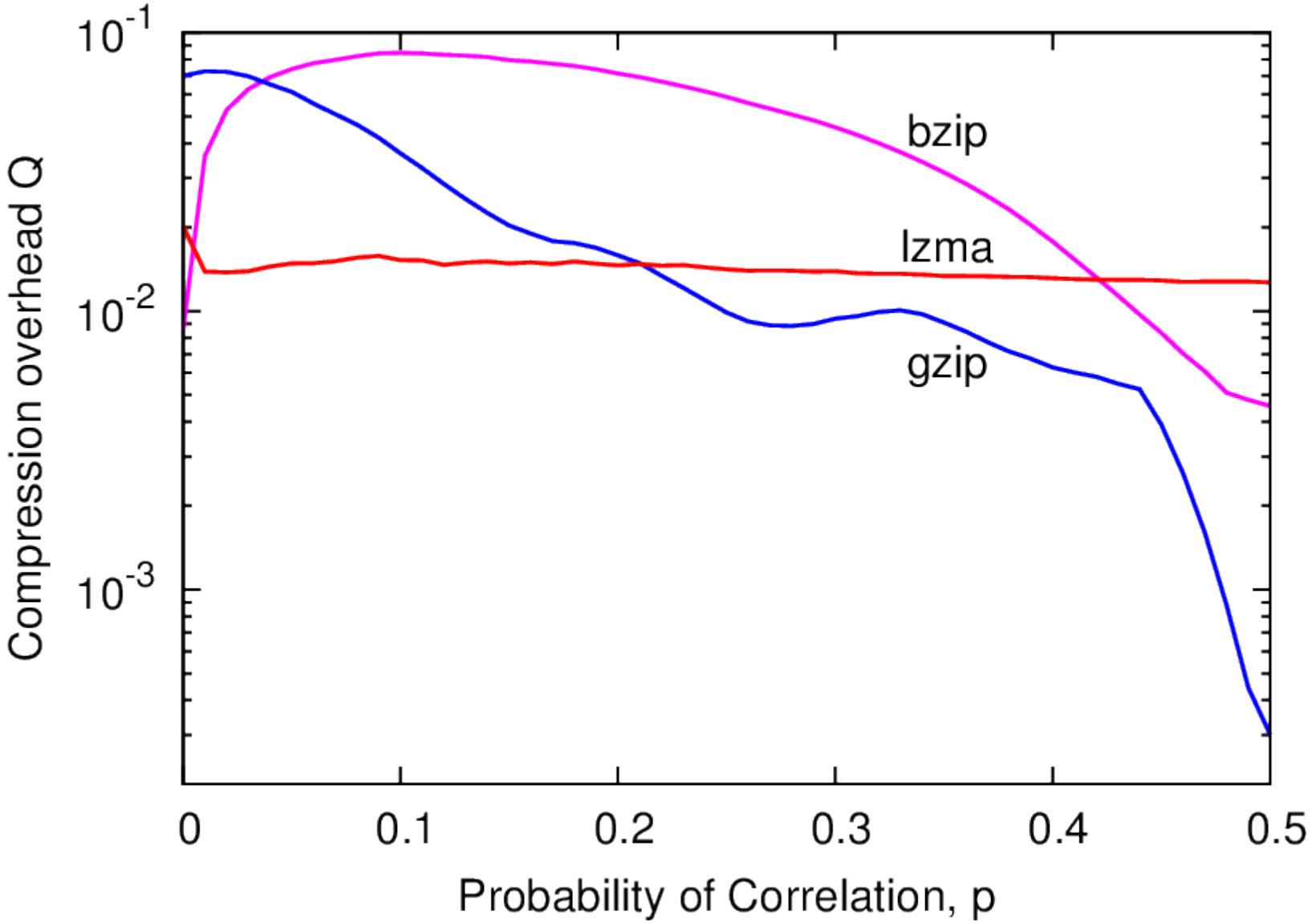


H.S. Poh, M. Marciewicz, P. Kurzynski, A. Cerè, D. Kaszlikowski, C.K, arXiv: 1504:03126

Performance of real compressors



Compression uniformity



Summary

- Closing loopholes in Bell tests is REALLY important for quantum key distribution

- Experimental evidence that Tsirelson's Bound can be reached, alternative Grinbaum model seems refuted/refutable

- Other measures for entanglement may not need iid assumption and can use information assessing tools like compressors

Thank you!

http://www.qolah.org

Part I:
Ilja Gerhardt
Qin Liu
Antia Lamas-Linares
Vadim Makarov
Antia Lamas-Linares
Valerio Scarani

Part II+ III:
Poh Hou Shun
Siddarth K. Joshi
Marcin Markiewicz
Paweł Krzyński
Dagomir Kaszlikowski
Adan Cabello
Alessandro Cerè

C.K.