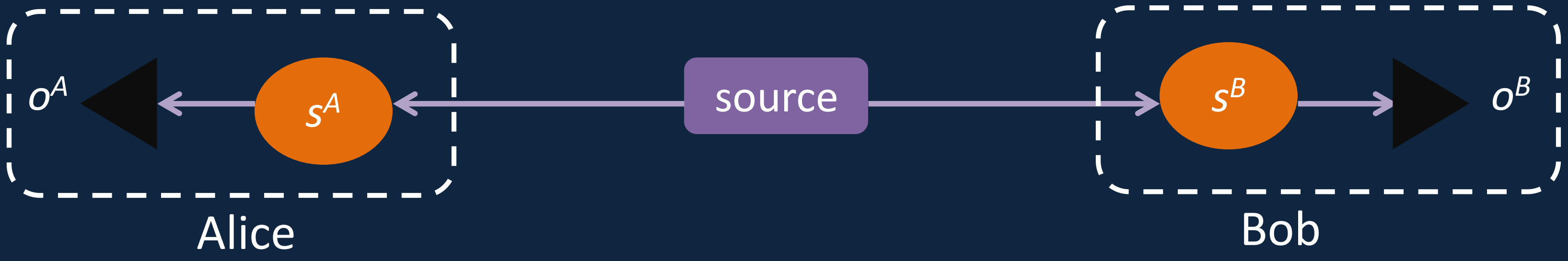
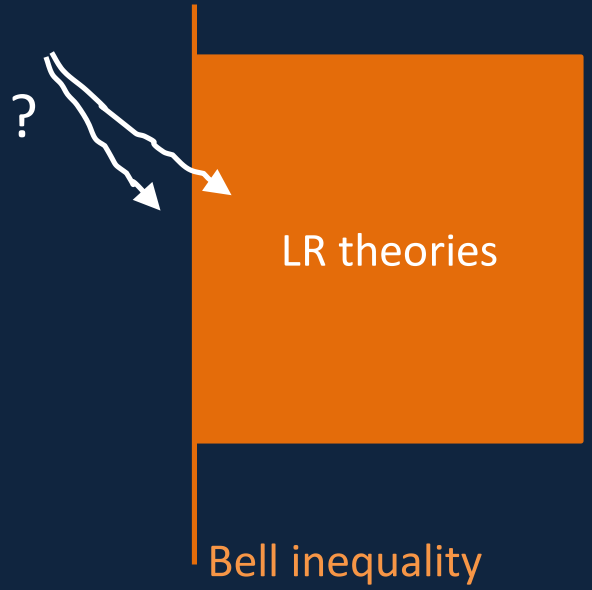
A Strong Loophole-Free Test of Local Realism





arXiv:1511.03189 [quant-ph]

Lynden K. Shalm, Evan Meyer-Scott, Bradley G. Christensen, Peter Bierhorst, Michael A. Wayne, Martin J. Stevens, Thomas Gerrits, Scott Glancy, Deny R. Hamel, Michael S. Allman, Kevin J. Coakley, Shellee D. Dyer, Carson Hodge, Adriana E. Lita, Varun B. Verma, Camilla Lambrocco, Edward Tortorici, Alan L. Migdall, Yanbao Zhang, Daniel R. Kumor, William H. Farr, Francesco Marsili, Matthew D. Shaw, Jeffrey A. Stern, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Thomas Jennewein, Morgan W. Mitchell, Paul G. Kwiat, Joshua C. Bienfang, Richard P. Mirin, Emanuel Knill, and Sae Woo Nam

Outline

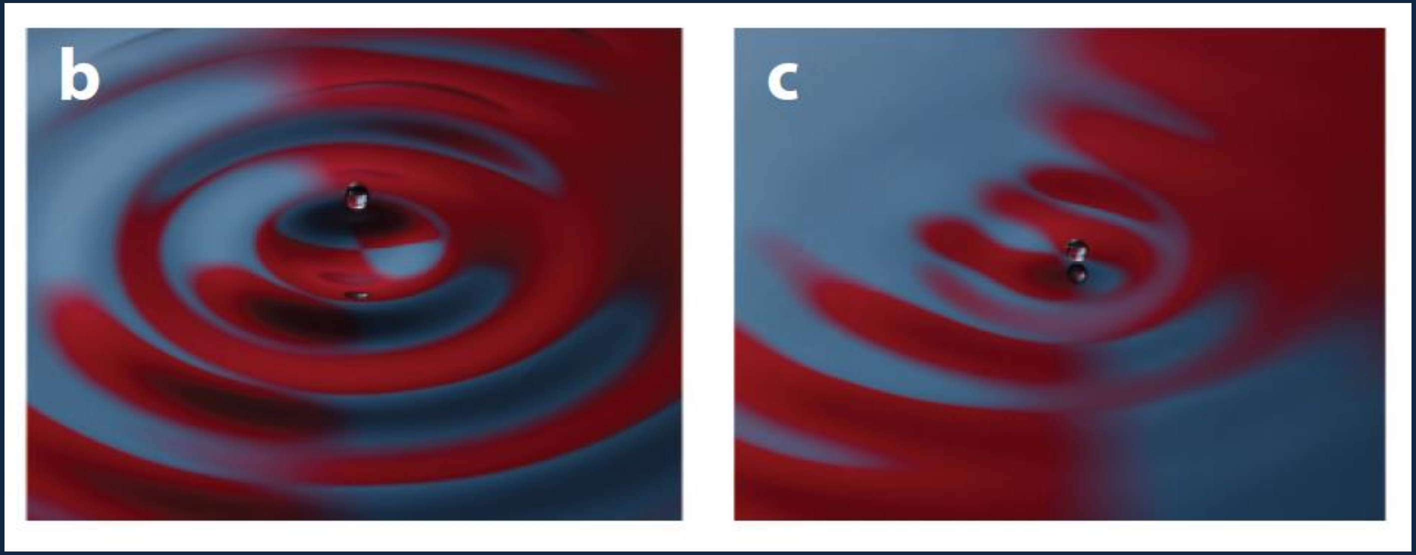
- Introduction to tests of LR
  - History lesson: hidden variables and LR
  - Bell inequalities
- Hypothesis test of LR
  - P-values for LR
- Experiments
  - Requirements and loopholes
  - Past experiments
  - Our experiment
- Computing our p-values
- Randomness expansion

History Lesson

- In 1920’s some physicists thought that quantum theory was very strange.
  - Superposition!
  - Entanglement!
  - “Spooky actions!”
  - Randomness! (not even respectable randomness like in statistical mechanics)

Hidden Variables

- Maybe all of this strangeness could be fixed with "hidden variables".
- If we knew the hidden variables, we would be able to predict the outcomes of all measurements with certainty.
- The quantum randomness would be respectable.
- In 1927 de Broglie invented the pilot wave theory [*J. Phys. Radium*].



[images from Bush, Ann. Rev. Fluid Mech., 2015]

Hidden Variables

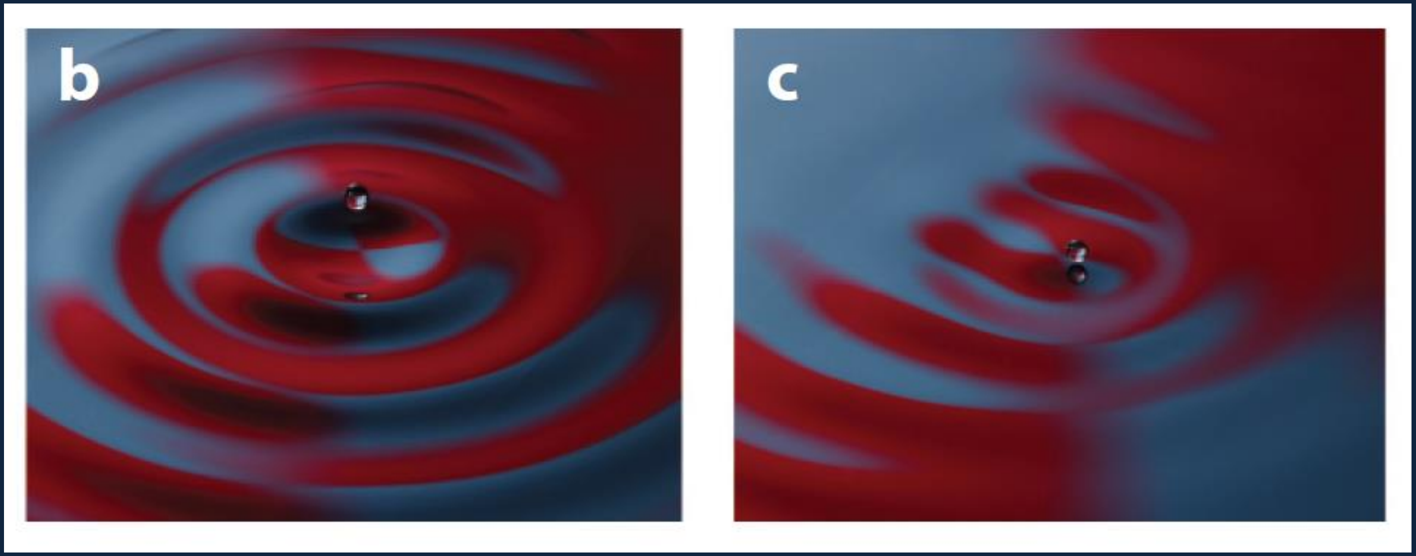
- Maybe all of this strangeness could be fixed with “hidden variables”.
- If we knew the hidden variables, we would be able to predict the outcomes of all measurements with certainty.
- The quantum randomness would be respectable.
- In 1927 de Broglie invented the pilot wave theory [*J. Phys. Radium*].
- In 1952 David Bohm completed the pilot wave theory [*Phys. Rev.*].
- Bohm’s theory gives exactly the same measurable predictions as standard non-relativistic quantum theory.

Hidden Variables

- Maybe all of this strangeness could be fixed with "hidden variables".
- If we knew the hidden variables, we would be able to predict the outcomes of all measurements with certainty.
- The quantum randomness would be respectable.
- In 1927 de Broglie invented the pilot wave theory [*J. Phys. Radium*].
- In 1952 David Bohm completed the pilot wave theory [*Phys. Rev.*].
- Bohm's theory gives <u>**EXACTLY THE SAME MEASURABLE PREDICTIONS**</u> as standard non-relativistic quantum theory.

Hidden Variables

- de Broglie's and Bohm's hidden variables are non-local.



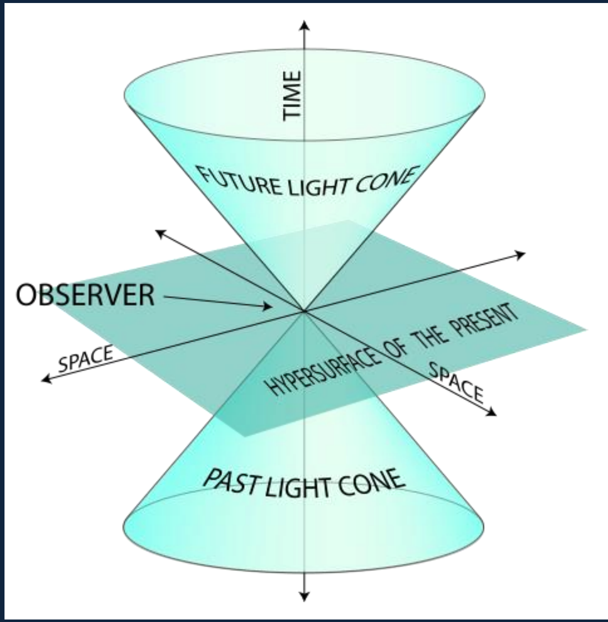
  - Hidden location of particle can change instantly because of distant events.
  - Hidden particle can travel faster than light.

Hidden Variables

- Bell wrote:
  - Bohm of course was well aware of these features of his scheme, and has given them much attention. However, it must be stressed that, to the present writer's knowledge, there is no *proof* that *any* hidden variable account of quantum mechanics *must* have this extraordinary character. It would therefore be interesting, perhaps, to pursue some further "impossibility proofs". [*Rev. Mod. Phys.*, 1966]
- Need a mathematical formulation.

Local Realism

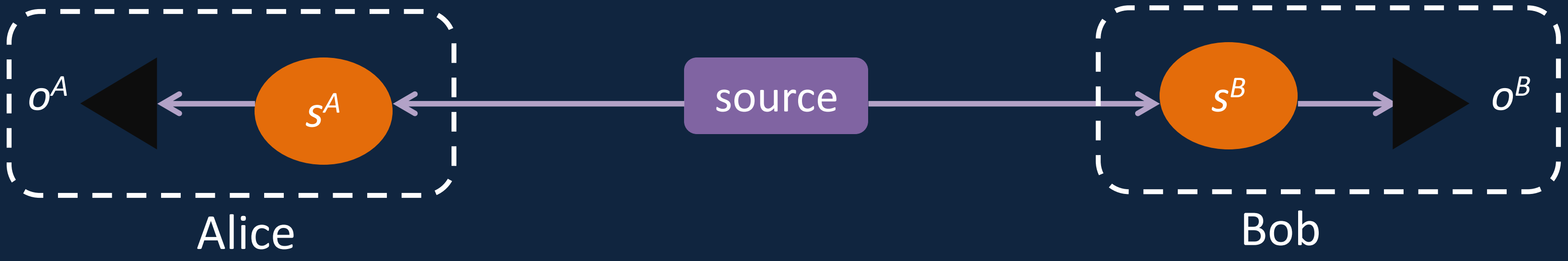
- Realism: all systems have pre-existing values for all possible measurements.
  - even incompatible measurements.
- Local realism: pre-existing values depend only on events in the past lightcone of the system.
- Classical physics obeys LR.
- Does quantum physic obey LR?



[Image source: K. Aainsqatsi at Wikipedia]

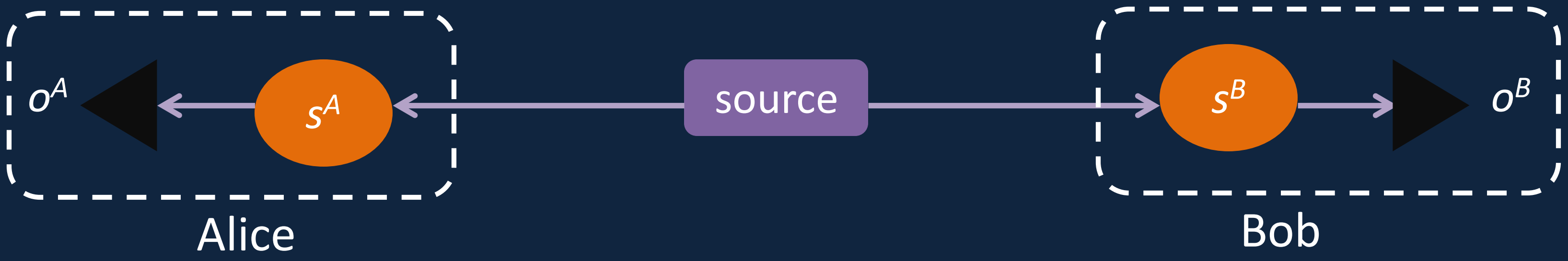
Bell's Inequalities

- Bell's thought experiment:



- Alice and Bob randomly choose measurements $s^A \in \{a, a'\}$ and $s^B \in \{b, b'\}$.
- They get outcomes o^A, $o^B \in \{0,+\}$.
- LR constrains $P(o^A, o^B \mid s^A, s^B)$.
- Bell found an inequality that is obeyed by all LR $P(o^A, o^B \mid s^A, s^B)$, but is violated by some entangled quantum systems [*Physics,* 1964].

Bell's Inequalities

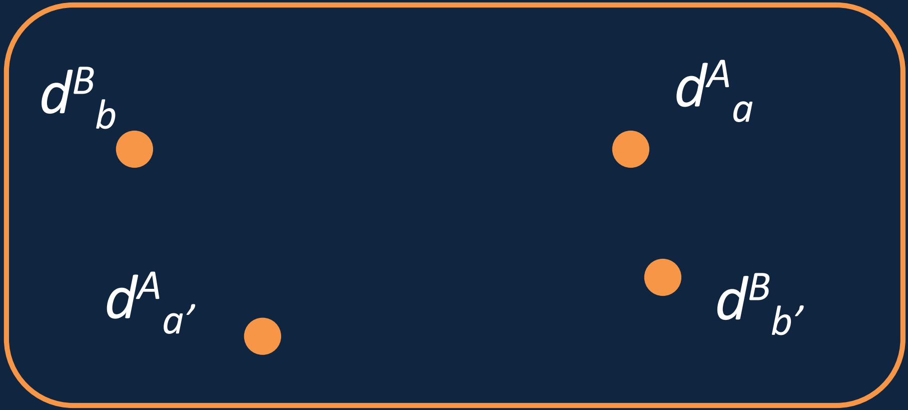


- A marginal problem:
  - LR outcome random variables $d^A{}_a$, $d^A{}_{a'}$, $d^B{}_b$, $d^B{}_{b'}$.
  - Physicists measure marginals
    - $P(d^A{}_a, d^B{}_b \mid a, b)$
    - $P(d^A{}_a, d^B{}_{b'} \mid a, b')$
    - $P(d^A{}_{a'}, d^B{}_b \mid a', b)$
    - $P(d^A{}_{a'}, d^B{}_{b'} \mid a', b')$
  - Are these compatible with $P(d^A{}_a, d^B{}_b, d^A{}_{a'}, d^B{}_{b'}, s^A, s^B)$?
  - If "no", LR is false.

Distance-Based Bell Inequalities

- Use triangle inequality to construct Bell inequalities: [Shumacher, *PRA*, 1991]
- Deterministic LR model gives outcomes for all settings
  - $d_{\mathrm{LR}}=(d^A{}_a, d^A{}_{a'}, d^B{}_b, d^B{}_{b'})$

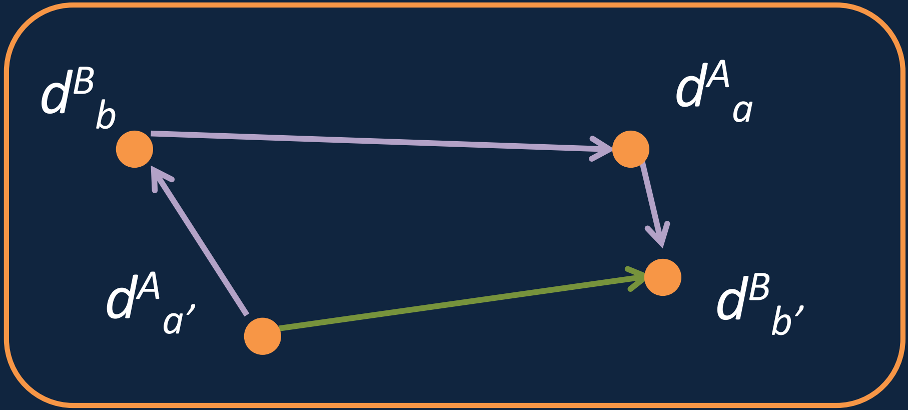
LR outcome space



Distance-Based Bell Inequalities

- Use triangle inequality to construct Bell inequalities: [Shumacher, *PRA*, 1991]
- Deterministic LR model gives outcomes for all settings
  - $d_{\mathrm{LR}}=(d^A{}_a, d^A{}_{a'}, d^B{}_b, d^B{}_{b'})$

LR outcome space



- Pseudo-distance: $l(x,y)$ obeys triangle inequality

$$\underbrace{l(d^A{}_{a'},d^B{}_b) + l(d^B{}_b,d^A{}_a) + l(d^A{}_a,d^B{}_{b'})}_{\longrightarrow} - \underbrace{l(d^A{}_{a'},d^B{}_{b'})}_{\longrightarrow} \geq 0$$

Distance-Based Bell Inequalities

- $I(d^A{}_{a'}, d^B{}_{b}) + I(d^B{}_{b}, d^A{}_{a}) + I(d^A{}_{a}, d^B{}_{b'}) - I(d^A{}_{a'}, d^B{}_{b'}) \geq 0$

- $d_{\mathrm{LR}}=(d^A{}_a, d^A{}_{a'}, d^B{}_b, d^B{}_{b'})$ is hidden, but for any $\mathrm{P}(d_{\mathrm{LR}})$

$$\mathrm{E}[I(d^A{}_{a'}, d^B{}_{b})] + \mathrm{E}[I(d^B{}_{b}, d^A{}_{a})] + \mathrm{E}[I(d^A{}_{a}, d^B{}_{b'})] - \mathrm{E}[I(d^A{}_{a'}, d^B{}_{b'})] \geq 0$$

Bell Inequality

– A constraint that the global distribution places on the marginals.

Distance-Based Bell Inequalities

- $E[l(d^A{}_{a'}, d^B{}_b)] + E[l(d^B{}_b, d^A{}_a)] + E[l(d^A{}_a, d^B{}_{b'})] - E[l(d^A{}_{a'}, d^B{}_{b'})] \geq 0$

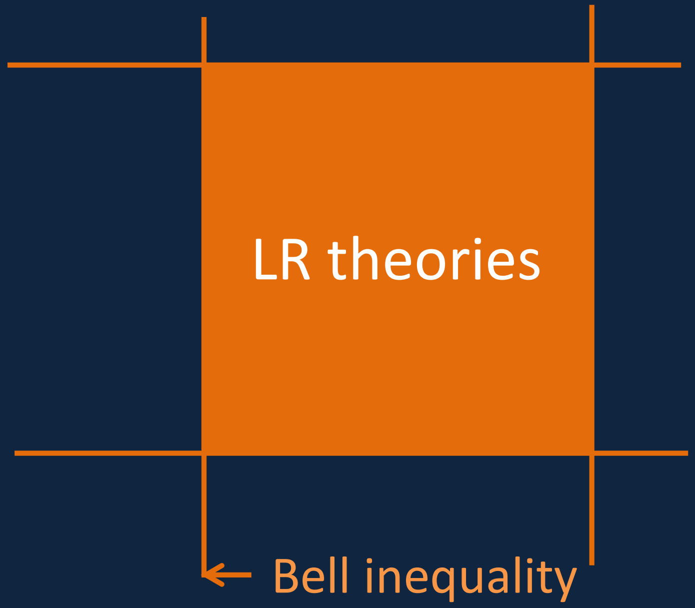
- Example: outcomes $d^X{}_c \in \{-1,1\}$
  - $l(x,y) = ½|y-x| \rightarrow$ CHSH Inequality [Clauser et al., *PRL*, 1969]

    $E[o^A o^B | a,b] + E[o^A o^B | a,b'] + E[o^A o^B | a',b] - E[o^A o^B | a',b'] \leq 2$

- Many other possibilities:
  - Other pseudo-distance functions $l(x,y)$
  - Only constraint: $l(x,y)$ obeys triangle inequality

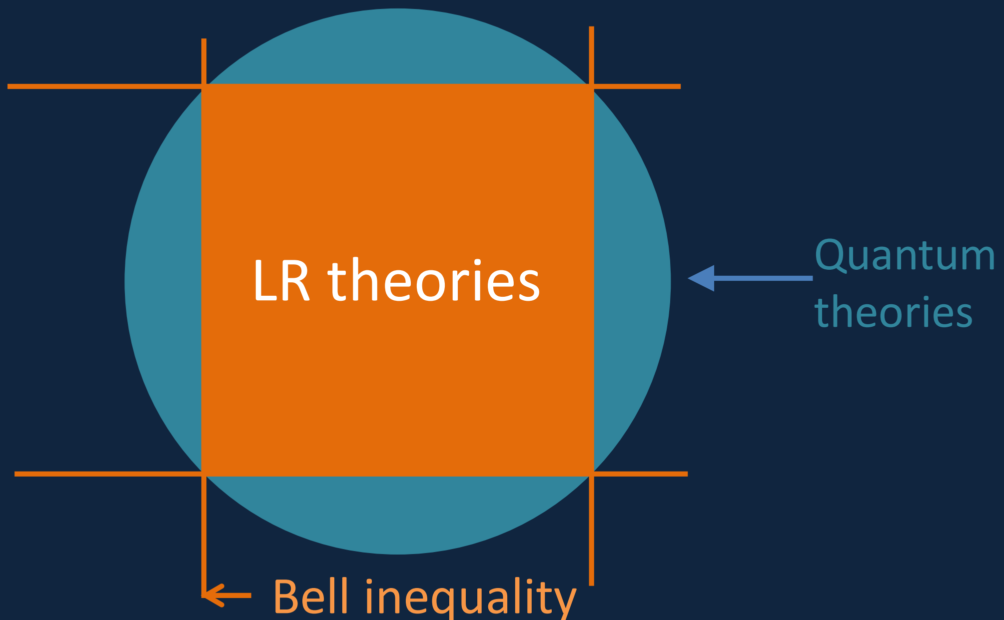
LR Polytope

- All the Bell inequalities make a polytope



LR Polytope

- All the Bell inequalities make a polytope.
- Quantum theories allow stronger correlations.

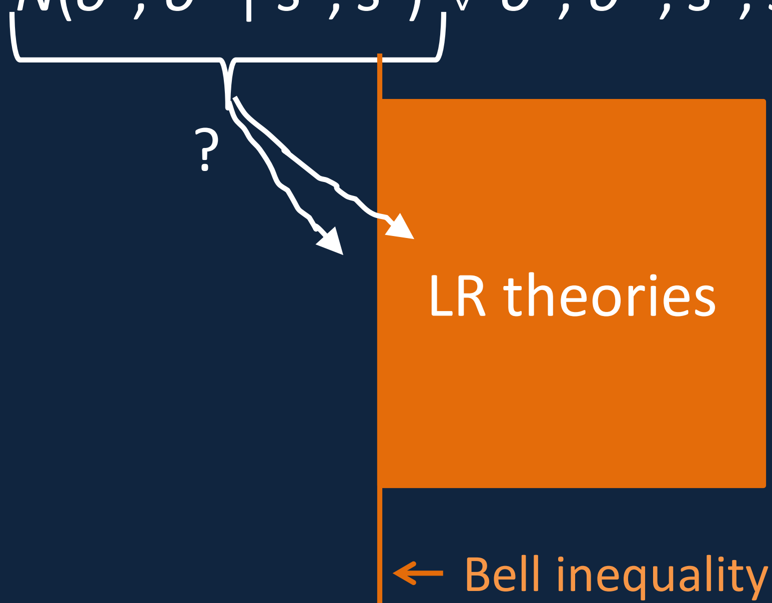


Outline

- Introduction to tests of LR
  - History lesson: hidden variables and LR
  - Bell inequalities
- Hypothesis test of LR
  - P-values for LR
- Experiments
  - Requirements and loopholes
  - Past experiments
  - Our experiment
- Computing our p-values
- Randomness expansion

Hypothesis Test of Local Realism

- Does quantum theory obey LR? **NO**
- Does reality obey LR?
- Do experiment.
- Get counts $N(o^A, o^B \mid s^A, s^B)\ \forall\ o^A, o^B, s^A, s^B$.

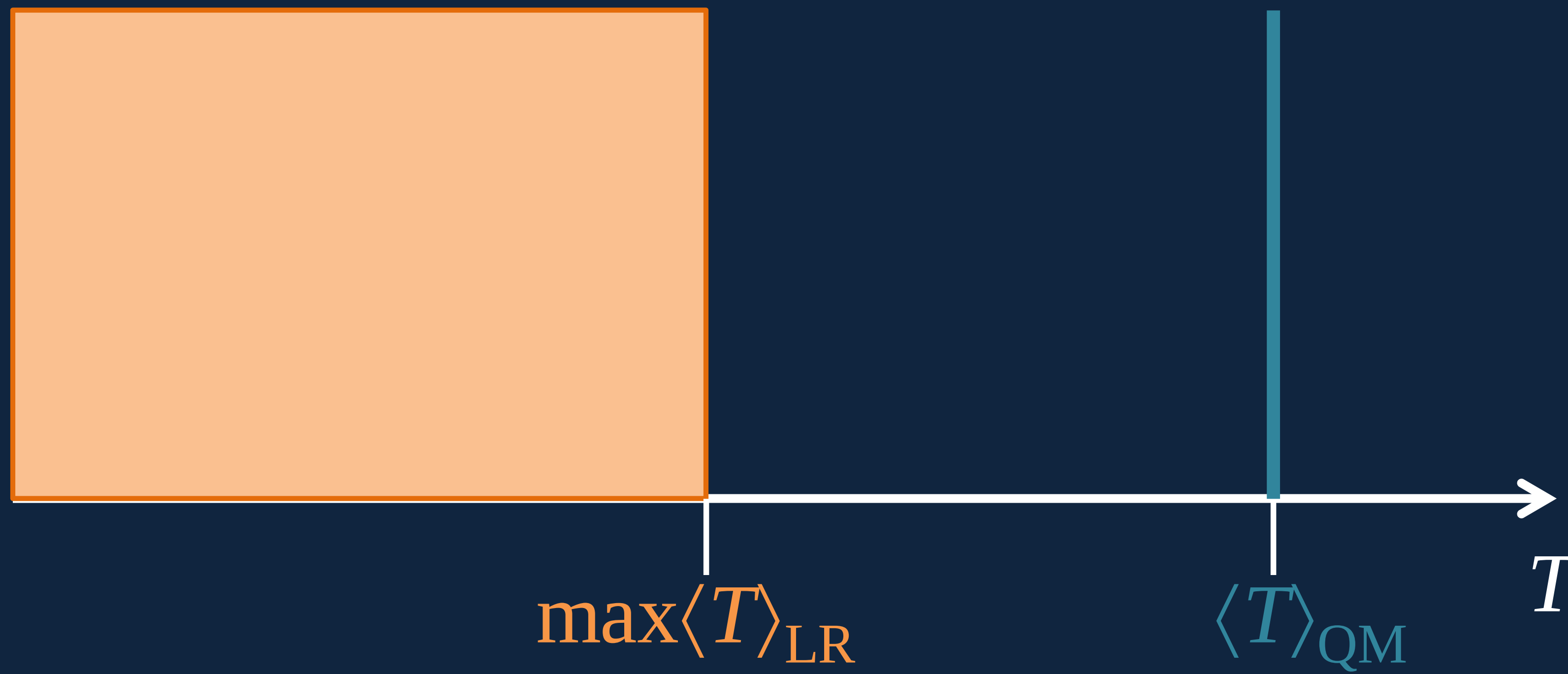


- How certain are we that our counts were not caused by an LR system? Use statistics!

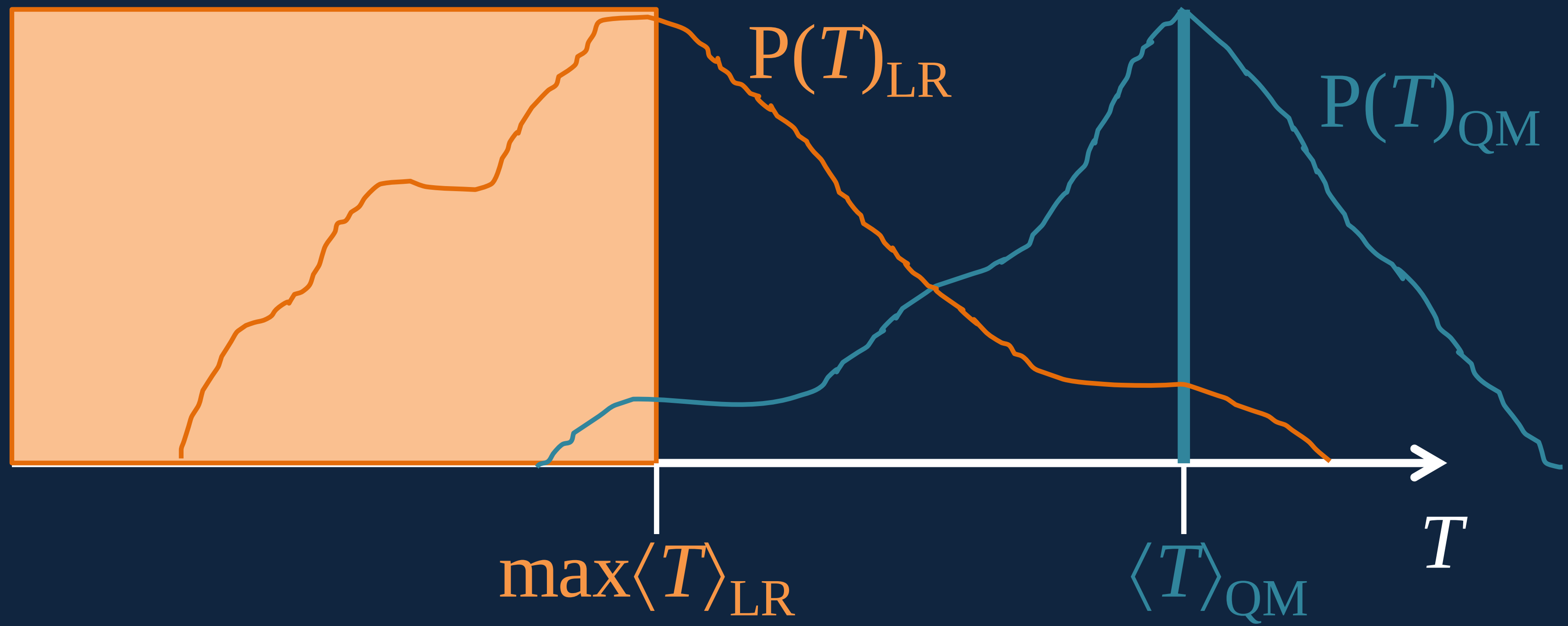
Hypothesis Test of Local Realism

- Test of LR as a Hypothesis Test:
  - Null Hypothesis H_0: "Experiment obeys LR & X & Y…"
  - Do n trials; get results $(o_1,o_2,\ldots,o_n)$
  - Compute test statistic: $T_{\text{obs}}(o_1,o_2,\ldots,o_n)$
  - P-value = $\sup_{\text{LR}}[P_{\text{LR}}(T \geq T_{\text{obs}})]$
  - Smaller p-value is stronger evidence against H_0.
- How to compute p-values for LR tests?
  - Gill [quant-ph/0301059]; Zhang, Glancy, and Knill's PBR [arXiv:1108.2468, 1303.7464]; Bierhorst [1311.3605, 1311.3605]; Kofler et al. [1411.4787]; Elkouss and Wehner [1510.07233].

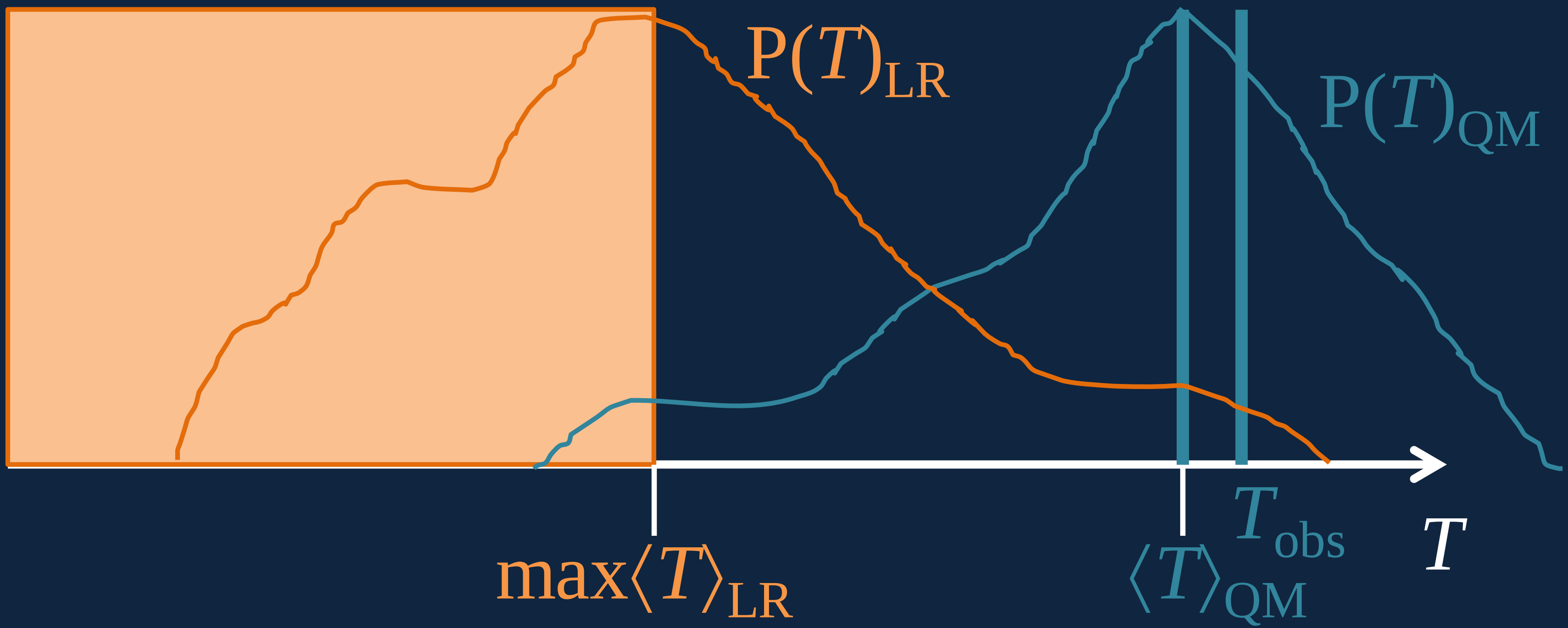
P-value Cartoon



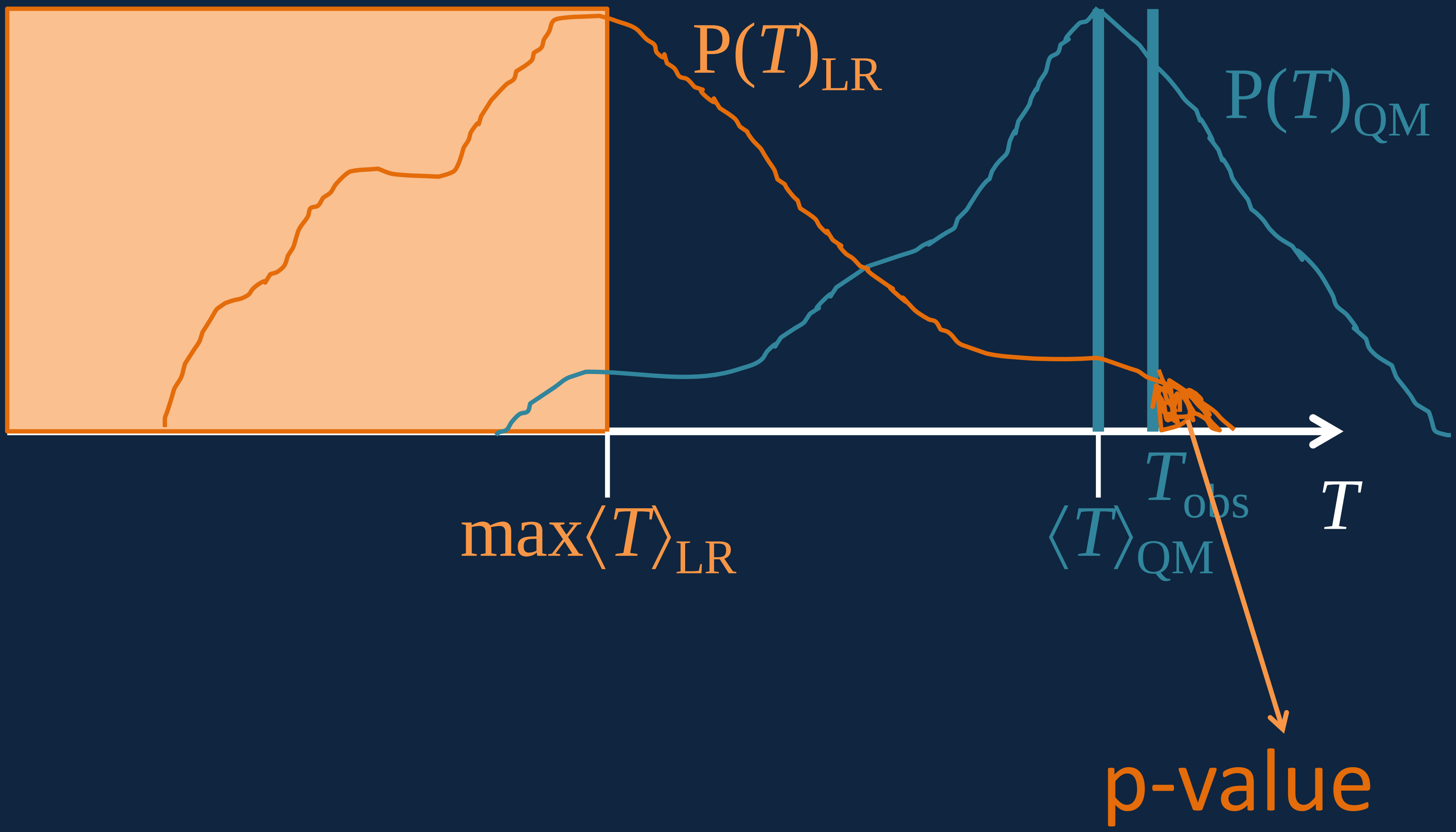
P-value Cartoon



P-value Cartoon



P-value Cartoon



Outline

- Introduction to tests of LR
  - History lesson: hidden variables and LR
  - Bell inequalities
- Hypothesis test of LR
  - P-values for LR
- Experiments
  - Requirements and loopholes
  - Past experiments
  - Our experiment
- Computing our p-values
- Randomness expansion

Experiments and Loopholes

- Experiments need:
  - Well defined trials
    - Choose random setting, get outcomes
  - Independence of choices
  - Isolation of measurement stations
    - Spacelike separation of choices from remote measurement.
  - High efficiency transmission and measurements
    - $\eta > 2/3$
  - High fidelity entangled particles
  - Rigorous analysis
    - without assuming i.i.d. and normal distribution

Experiments and Loopholes

- Experiments are not perfect.
- Loophole: way that LR system can violate a Bell inequality in an experiment.
  - Experiment does not meet requirements.
  - Assumptions that can’t be verified
    - About device
    - During analysis

Past Experiments

- Many past experiments – all had loopholes.
- Loopholes have closed as technology improved:

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

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

A. Aspect, P. Grangier, and G. Roger, *Phys. Rev. Lett.* **49**, 91 (1982).

A. Aspect, J. Dalibard, and G. Roger, *Phys. Rev. Lett.* **49**, 1804 (1982).

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

M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, *Nature* **409**, 791 (2001).

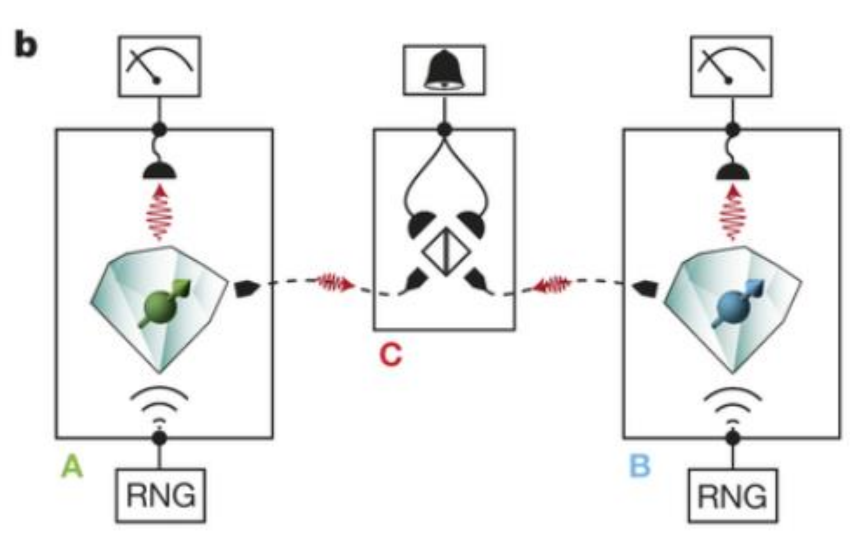
T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X.-S. Ma,T. Herbst, L. Ratschbacher, A. Fedrizzi, N. K. Langford, T. Jennewein, and A. Zeilinger, *Proc. Nat. Acad. Sci. USA* **107**, 19708 (2010).

M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger, *Nature* **497**, 227 (2013)

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).

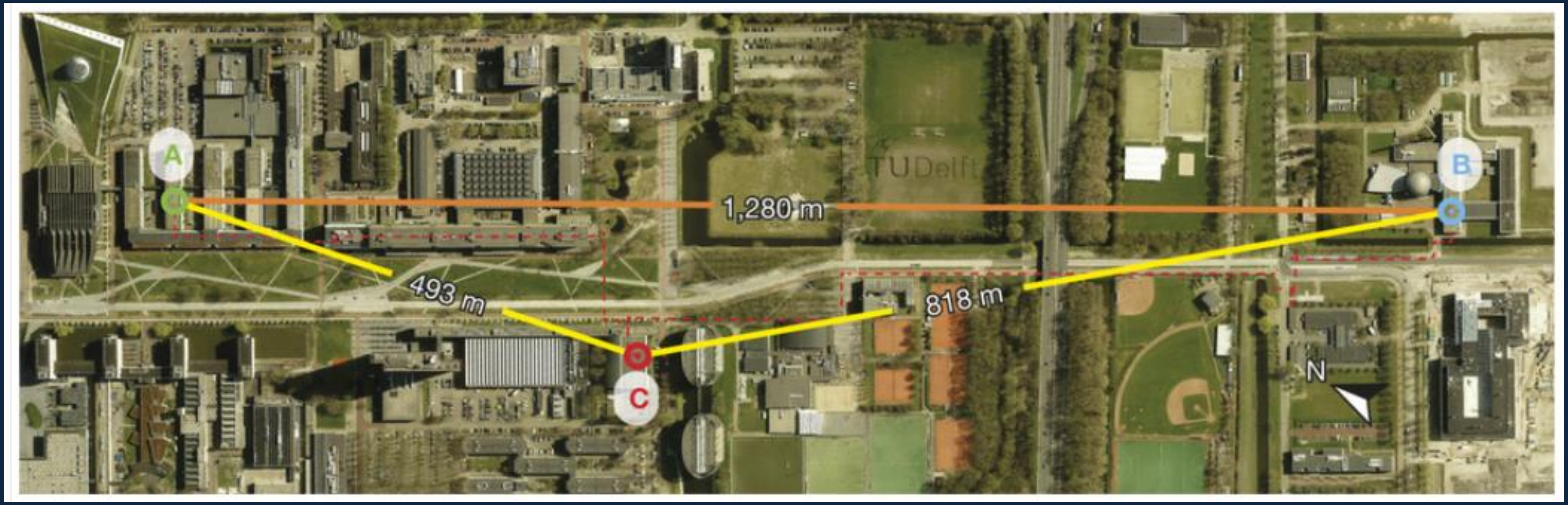
3 New Experiments

- In 2015, 3 “loophole free” experiments were performed
- B. Hensen, and others, “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres” *Nature*. At TU Delft.
  - P-value = 0.039.



3 New Experiments

- In 2015, 3 “loophole free” experiments were performed
- B. Hensen, and others, “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres” *Nature*. At TU Delft.
  - P-value = 0.039.



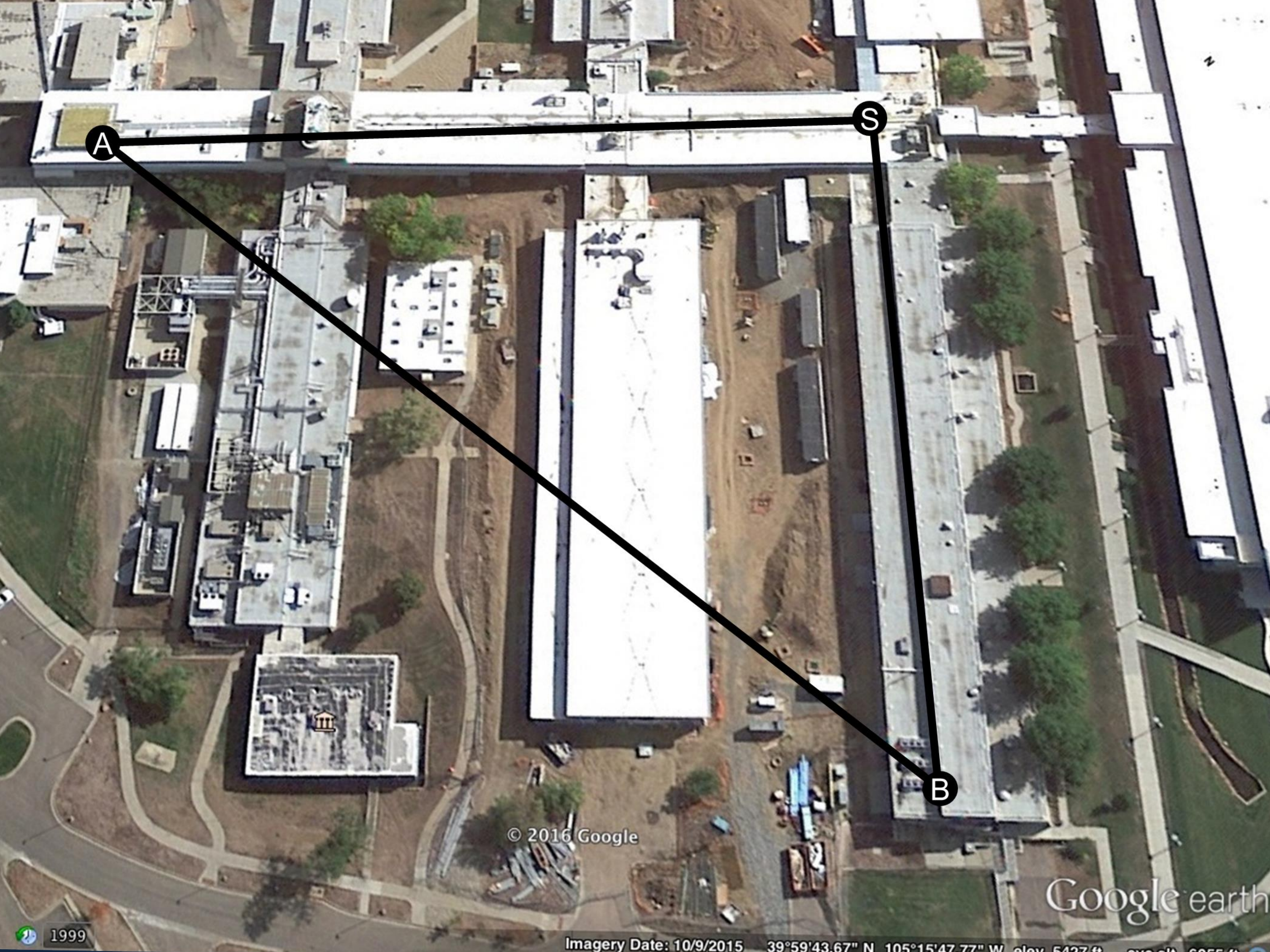
3 New Experiments

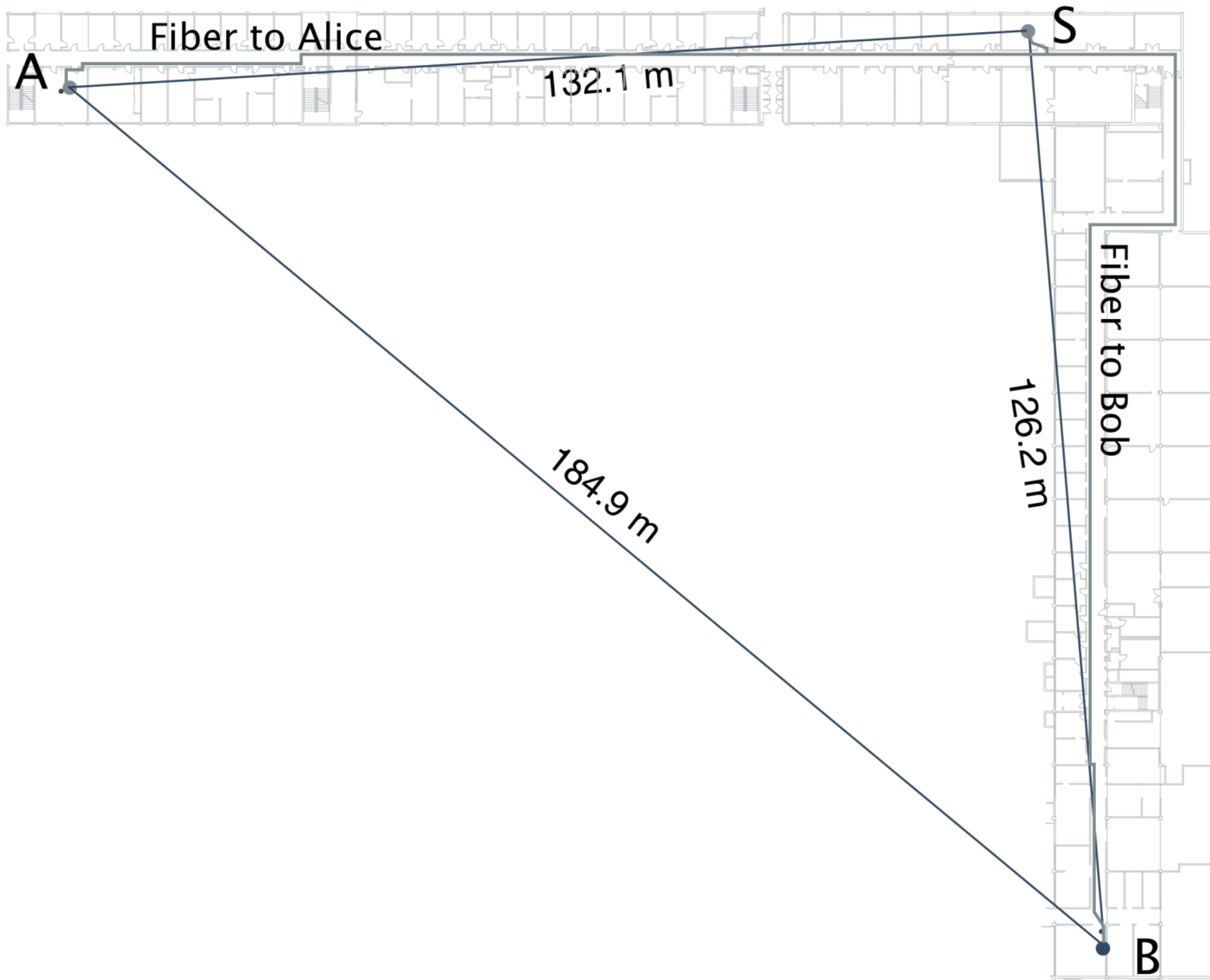
- In 2015, 3 “loophole free” experiments were performed
- B. Hensen, and others, “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres” *Nature*. At TU Delft.
  - P-value = 0.039.
- M. Giustina and others, “Significant-Loophole-Free Test of Bell’s Theorem with Entangled Photons” *Phys. Rev. Lett.* At University of Vienna.
  - P-value = 3.74×10^{-31}.

3 New Experiments

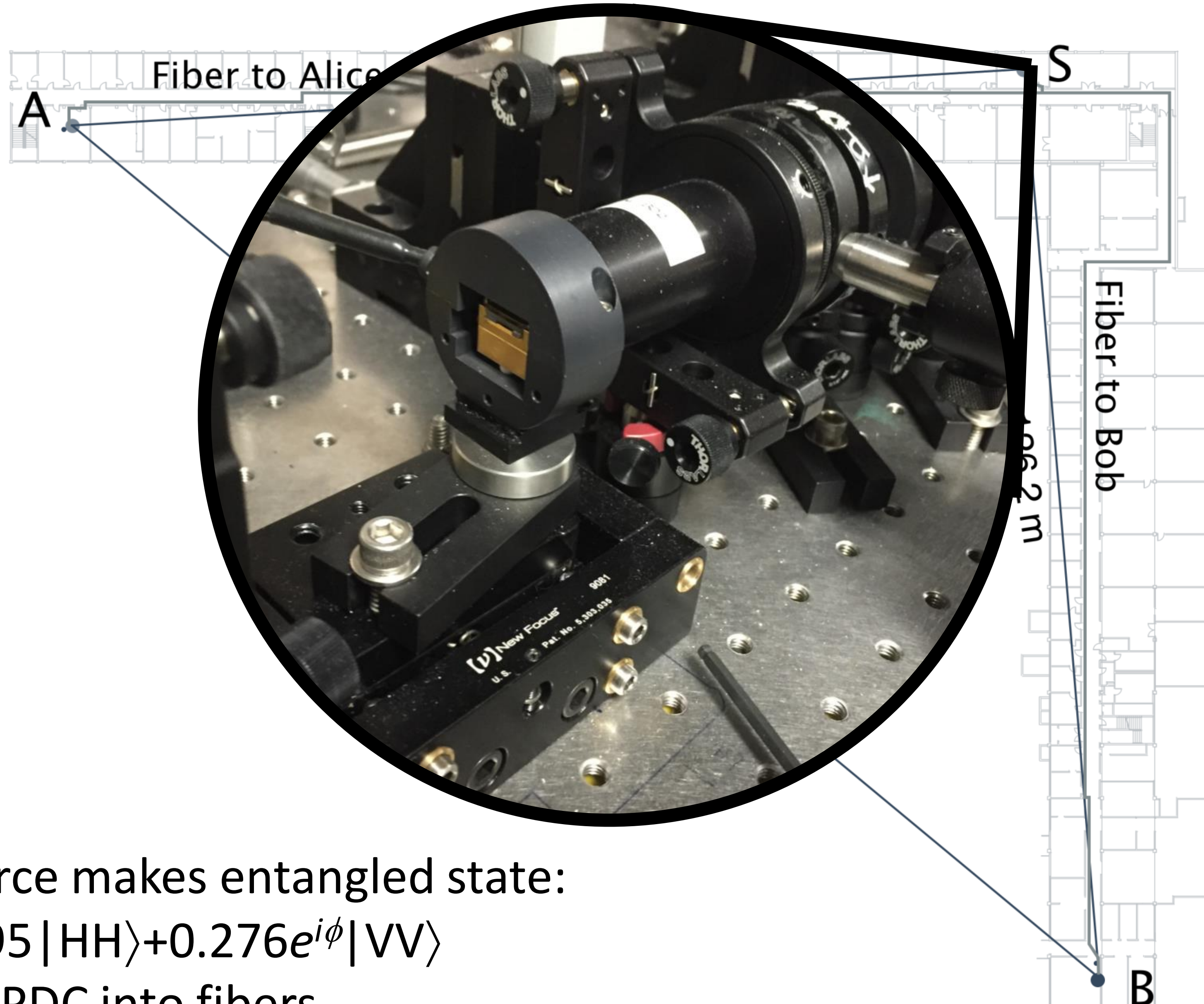
- In 2015, 3 “loophole free” experiments were performed
- B. Hensen, and others, “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres” *Nature*. At TU Delft.
  - P-value = 0.039.
- M. Giustina and others, “Significant-Loophole-Free Test of Bell’s Theorem with Entangled Photons” *Phys. Rev. Lett.* At University of Vienna.
  - P-value = 3.74×10^{-31}.
- K. Shalm and others, “Strong Loophole-Free Test of Local Realism” *Phys. Rev. Lett.* At NIST-Boulder.
  - P-value = 2.3×10^{-7}.

Our Experiment

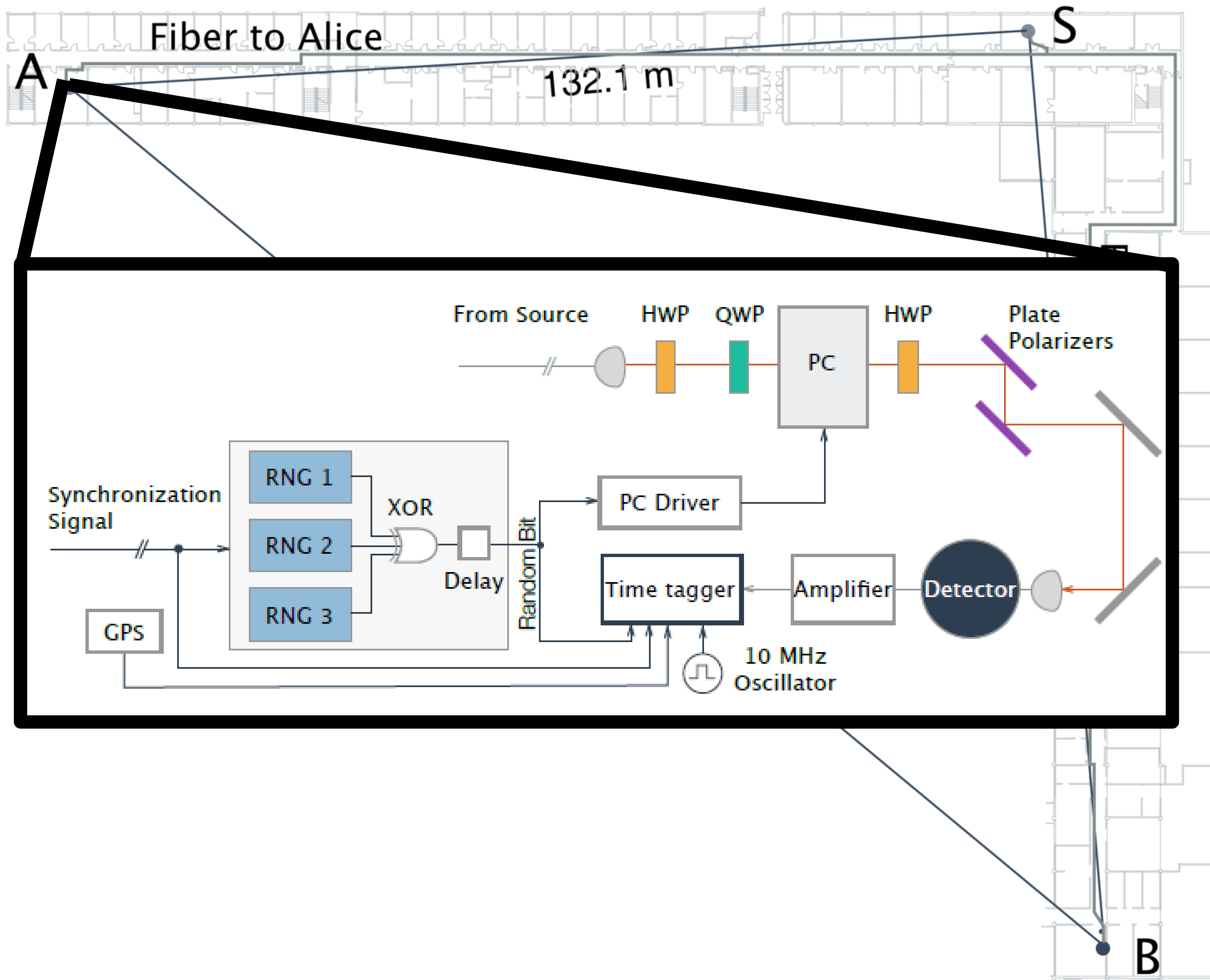

A
S
B
© 2016 Google
Google earth
1999
Imagery Date: 10/9/2015
39°59'43.67" N



Fiber to Alice
A
S
132.1 m
184.9 m
126.2 m
Fiber to Bob
B

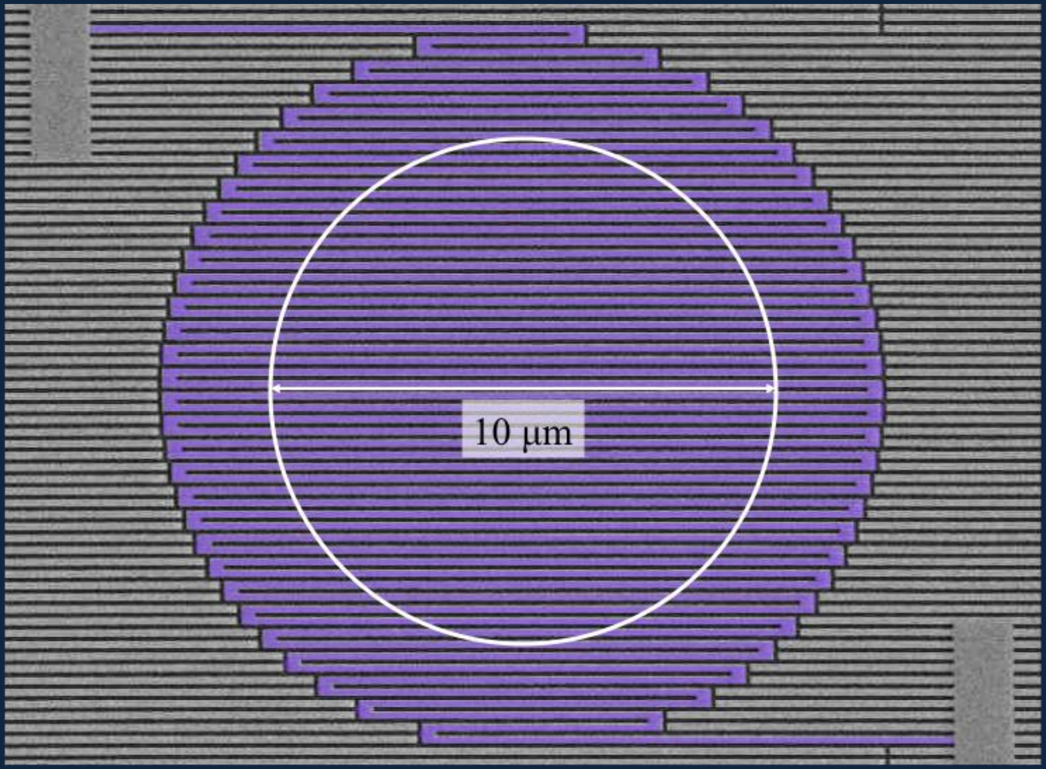


Source makes entangled state:
$0.995|HH\rangle + 0.276 e^{i\phi}|VV\rangle$
by SPDC into fibers.

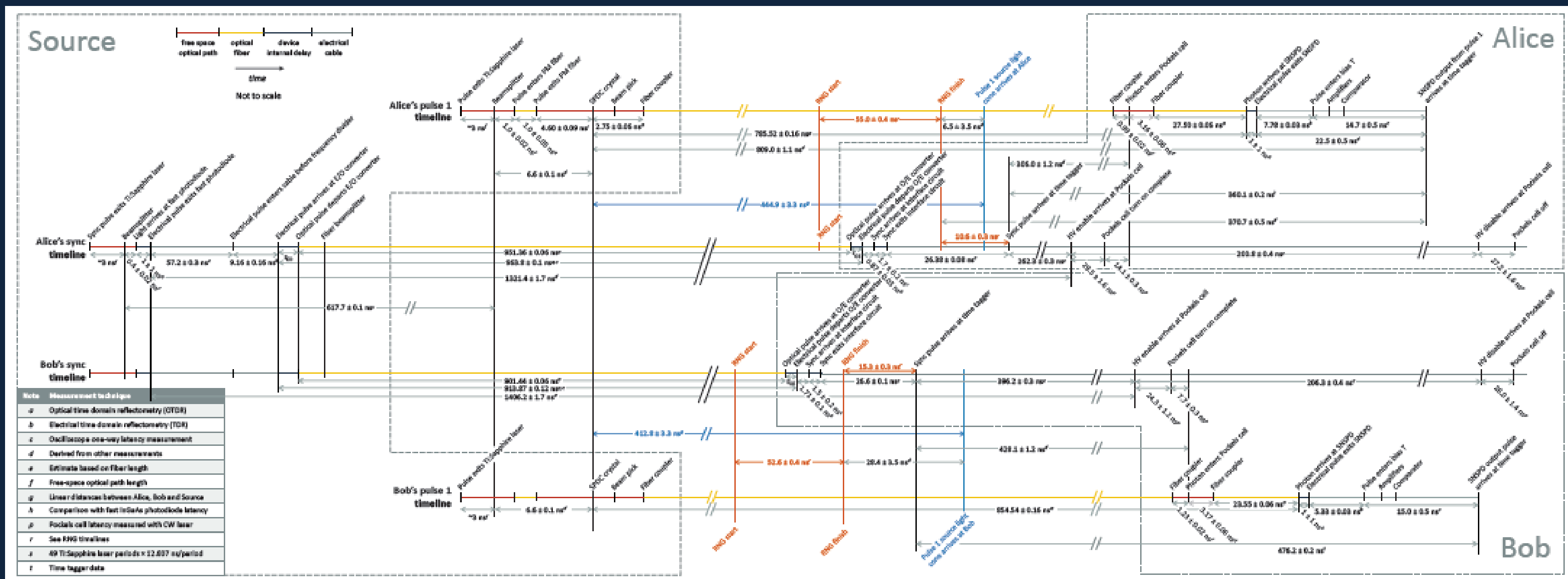

Fiber to Alice
A
S
132.1 m
B
From Source
HWP
QWP
PC
HWP
Plate
Polarizers
Synchronization
Signal
RNG 1
RNG 2
RNG 3
XOR
Delay
Random Bit
PC Driver
Time tagger
Amplifier
Detector
GPS
10 MHz
Oscillator

Superconducting Nanowire Single Photon Detector

- Detector efficiency ~ 90 %
- Total transmission and detection efficiency ~ 75 %
- Latency ~ 1±1 ns, Jitter ~150 ps. [Marsili and others, arXiv:1209.5774]

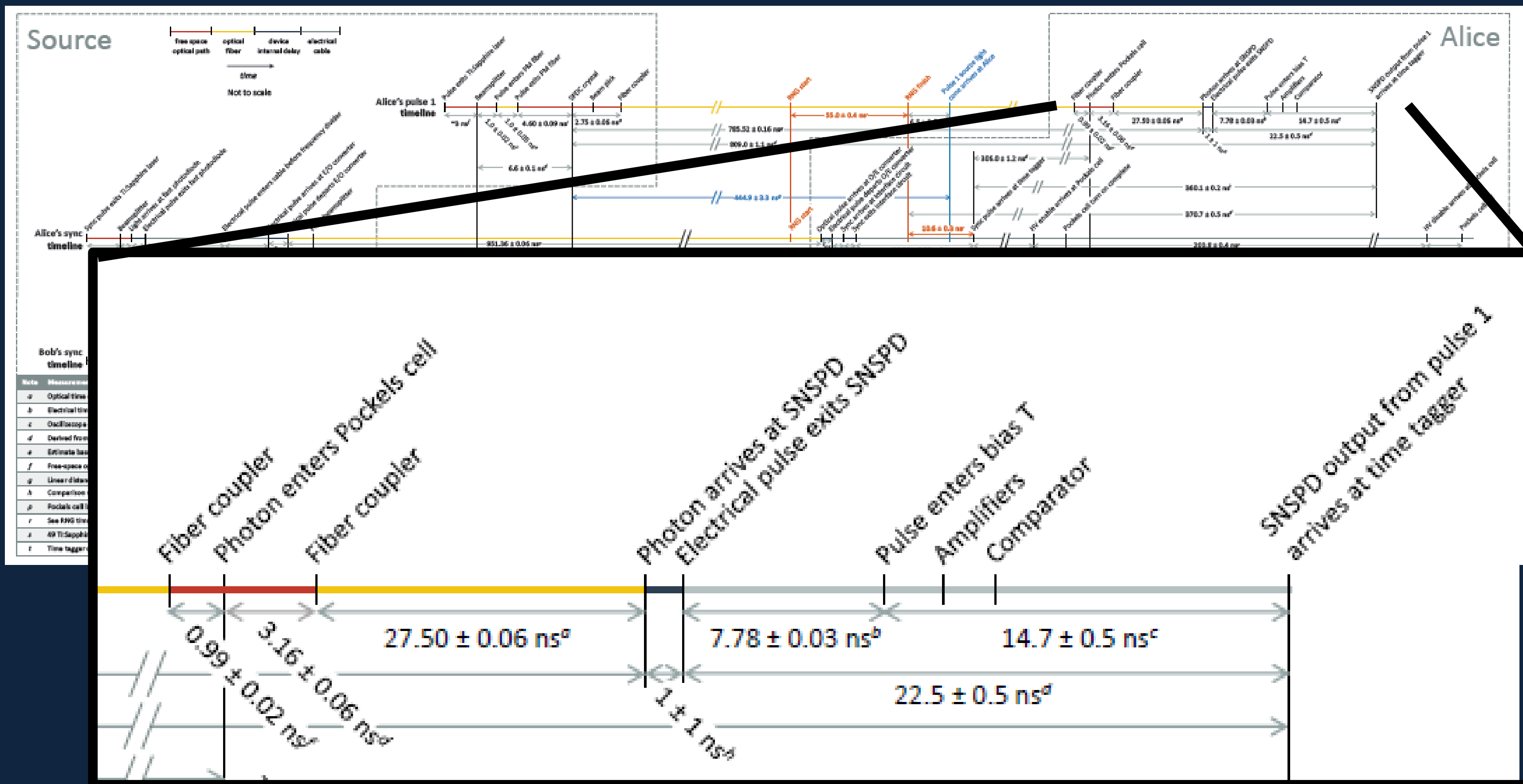


Timing



Source
Alice
Bob
Alice's pulse 1 timeline
Alice's sync timeline
Bob's sync timeline
Bob's pulse 1 timeline

Timing



Source
Alice
Fiber coupler
Photon enters Pockels cell
Fiber coupler
Photon arrives at SNSPD
Electrical pulse exits SNSPD
Pulse enters bias T
Amplifiers
Comparator
SNSPD output from pulse 1 arrives at time tagger
0.99 ± 0.02 ns
3.16 ± 0.06 ns
27.50 ± 0.06 ns
7.78 ± 0.03 ns
14.7 ± 0.5 ns
22.5 ± 0.5 ns
1 ± 1 ns

Outline

- Introduction to tests of LR
  - History lesson: hidden variables and LR
  - Bell inequalities
- Hypothesis test of LR
  - P-values for LR
- Experiments
  - Requirements and loopholes
  - Past experiments
  - Our experiment
- Computing our p-values
- Randomness expansion

How We Compute P-values

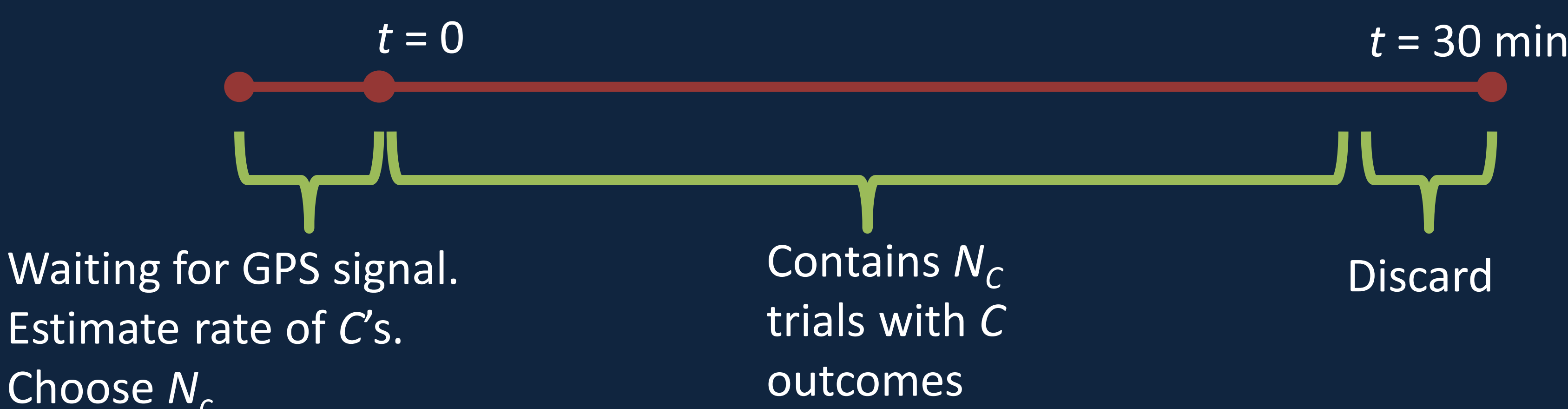
- Define “trial”:
  - Fixed time window after synch pulse arrives at Alice and Bob.
  - When they are ready.
  - Measurement choices.
  - Detector click times.
- Convert detection timetags to 0/+ outcomes
  - “0” if no photons detected
  - “+” if any photons detected

Binomial Method

- See Bierhorst [arXiv:1312.2999].
- For the CH inequality:
  - $P(++|\mathrm{ab}) \leq P(+0|\mathrm{ab'}) + P(0+|\mathrm{a'b}) + P(++|\mathrm{a'b'})$
  - Does not include 00 terms – less sensitive to failed downconversion.
- Consider subsequence of trials with outcomes C = {++ab, +0ab’, 0+a’b, ++a’b’}.
- If ++ab $\rightarrow$ HEADS, otherwise TAILS.
- Under optimal LR model, coin flips have binomial distribution with $P(\mathrm{HEADS}) = ½$.
- P-value = probability to get at least observed # of HEADS using a fair coin.

Binomial Method

- For valid p-values, we must choose a stopping criterion in advance.
- Actual experiment was done for fixed amount of time.
- Warning: # of C={++ab, +0ab’, 0+a’b, ++a’b’} outcomes is random.
- Use initial data to estimate rate of C outcomes.
- Choose N_C to be analyzed from remainder of data.



Binomial Method

- For “Classical XOR 3” data set:
- Total trials = 182,137,032
- N_c = 12,127
- # of HEADS = 6,378
- p-value = 5.85×10^{-9}

RNG Bias Correction

- What if RNGs have bias: $P(\mathrm{a}) \neq P(\mathrm{a'}) \neq ½$ or $P(\mathrm{b}) \neq P(\mathrm{b'}) \neq ½$?
- How should we adjust p-values?
- Define excess predictability bound
  - $\varepsilon = 2 \max[P(\mathrm{a}), P(\mathrm{a'}), P(\mathrm{b}), P(\mathrm{b'})] - 1$
- Under the optimal LR theory, $\varepsilon \neq 0$ allows
  - P(HEADS) $\leq \frac{1}{2} + \frac{\varepsilon}{1+\varepsilon^2}$.
  - If $\varepsilon \leq 3\times10^{-3}$, p-value $\leq 2.3\times10^{-7}$,

P-value: Best Practice

- P-value: Given a test statistic, the p-value is the probability, according to null hypothesis, of observing a test statistic value as or more extreme than the observed value.

- For probability statement to hold, one must
  – Commit to analysis method.
  – Choose stopping rule.
  – Take data.
  – Compute p-value.
  – Publish p-value (whatever it is).

P-value: What We Did

- Took several data sets.
- Chose good stopping rules in advance.
- Tried different analysis methods.
  - PBR [Zhang, Glancy, Knill, arXiv:1108.2468]
  - Binomial
  - Adjusted trail duration
- In supplementary material, we gave a big table of p-values.

TABLE S-I. Table of p-values testing LR.

02-54 (first run), $N_{\mathrm{Total}} = 203,629,242$				
Pulses	6	5-7	4-8	3-9
N_χ Cut Point	2528	7659	12753	17854
N_S	1263	3842	6460	9057
$\epsilon = 0$ p-value	.5238	.3920	.0708	.0263
$\epsilon = .0001$	.5278	.3987	.0739	.0280
$\epsilon = .001$	.5637	.4605	.1067	.0473
$\epsilon = .01$	.8566	.9300	.7848	.7685
03-43 (second run), $N_{\mathrm{Total}} = 107,032,197$				
Pulses	6	5-7	4-8	3-9
N_χ Cut Point	1213	3678	6192	8668
N_S	618	1893	3190	4471
$\epsilon = 0$ p-value	.2638	.0388	.0087	.0017
$\epsilon = .0001$	.2661	.0399	.0091	.0018
$\epsilon = .001$	.2871	.0502	.0132	.0030
$\epsilon = .01$	.5259	.2906	.2110	.1422
19-45 (third run), $N_{\mathrm{Total}} = 182,560,876$				
Pulses	6	5-7	4-8	3-9
N_χ Cut Point	2455	7304	11891	16648
N_S	1246	3692	6016	8465
$\epsilon = 0$ p-value	.2337	.1776	.0996	.0148
$\epsilon = .0001$	.2368	.1821	.1035	.0157
$\epsilon = .001$	.2652	.2256	.1433	.0274
$\epsilon = .01$	.6043	.7837	.8151	.6564
Classical XOR 1, $N_{\mathrm{Total}} = 178,781,131$				
Pulses	6	5-7	4-8	3-9
N_χ Cut Point	2332	7108	11917	16684
N_S	1179	3617	6034	8503
$\epsilon = 0$ p-value	.3023	.0691	.0847	.0065
$\epsilon = .0001$	.3057	.0714	.0881	.0070
$\epsilon = .001$	.3368	.0944	.1239	.0130
$\epsilon = .01$	.6730	.5806	.7908	.5390
Classical XOR 2, $N_{\mathrm{Total}} = 177,785,896$				
Pulses	6	5-7	4-8	3-9
N_χ Cut Point	2384	7120	11921	16690
N_S	1215	3616	6087	8546
$\epsilon = 0$ p-value	.1784	.0942	.0105	
$\epsilon = .0001$	.1809	.0970	.0111	.0010
$\epsilon = .001$	.2050	.1257	.0183	.0022
$\epsilon = .01$	.5219	.6451	.4504	.3013
Classical XOR 3, $N_{\mathrm{Total}} = 182,137,032$				
Pulses	6	5-7	4-8	3-9
N_χ Cut Point	2376	7211	12127	16979
N_S	1257	3800	6378	8820
$\epsilon = 0$ p-value	.0025	2.44×10^{-6}	5.85×10^{-9}	2.03×10^{-7}
$\epsilon = .0001$	.0025	2.64×10^{-6}	6.66×10^{-9}	2.33×10^{-7}
$\epsilon = .001$	.0033	5.40×10^{-6}	2.08×10^{-8}	7.73×10^{-7}
$\epsilon = .01$	.0331	.0020	2.31×10^{-4}	.0069

P-value What We Did

- Took several data sets.
- Chose good stopping rules in advance.
- Tried different analysis methods.
  - PBR [Zhang, Glancy, Knill, arXiv:1108.2468]
  - Binomial
  - Adjusted trial duration
- In supplementary material, gave a giant table of p-values.
  - Informative, but difficult to interpret.
  - How to combine into a single p-value? ¯_(ツ)_/¯
- Abstract says "p-values as low as 5.9×10^{-9}".

P-value What We Did

- Rigor of p-values is slightly weakened by exploratory analysis.
  - Typical of most physics experiments.
  - # of analysis decisions is not very large.
  - Most important analysis decisions were made on training data sets.

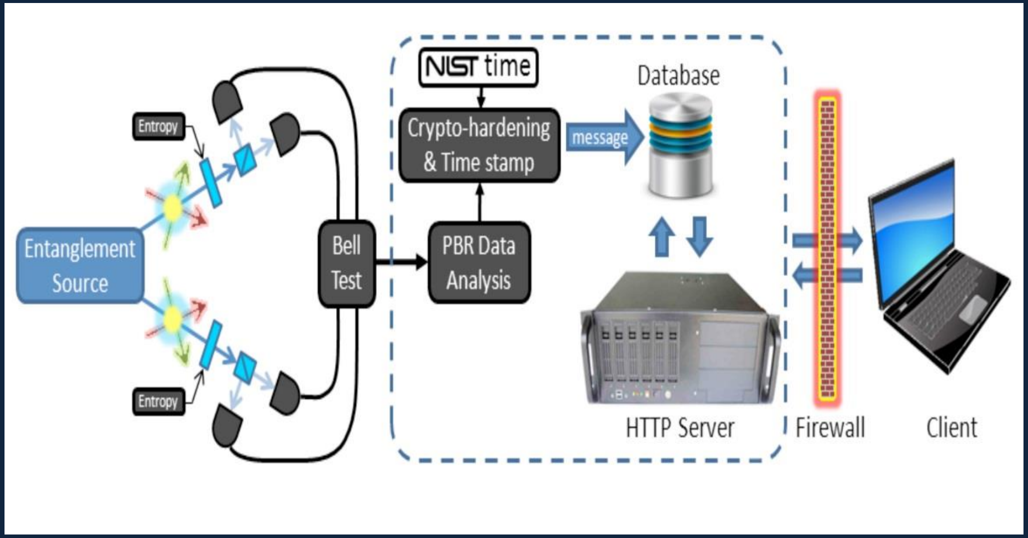
- Hopefully our p-values are small enough that they still provide good evidence against LR.

Outline

- Introduction to tests of LR
  - History lesson: hidden variables and LR
  - Bell inequalities
- Hypothesis test of LR
  - P-values for LR
- Experiments
  - Requirements and loopholes
  - Past experiments
  - Our experiment
- Computing our p-values
- Randomness expansion

Randomness Expansion

- Secure randomness generation
  - For NIST random beacon



  - Broadcasts 512 bits every minute for public use.

Randomness Expansion

- Secure randomness generation
  - Let’s use a test of local realism as the entropy source!
  - Why?
  - An LR system has hidden variables that predict measurement outcomes.
  - A hacker is like a hidden variable.
  - If we can reject LR, we reject hackers’ ability to predict.

Randomness Expansion

- Peter Bierhorst, Lynden K. Shalm, Alan Mink, Stephen Jordan, Yi-Kai Liu, Andrea Rommal, Scott Glancy, Bradley Christensen, Sae Woo Nam, and Emanuel Knill
- Theory project: lower-bound min-entropy as a function of Bell inequality violation.
  – Needed protocol robust to noisy experiment that barely violates.
- Software project: extract unbiased bits from Bell test output.
  – Trevisan extractor
  – Fixed and optimized code of Mauerer, Portmann, and Scholz (arXiv:1212:.0520).

Randomness Expansion

- We made 256 random bits, uniform to within 0.001:

1011000000101000101000011010100111001010110000111001
0100111011111001101101100010011110100101010100101001
1001011011100110001010010000100001011000100100101111
1100110010000001111111000111011110001111011011110110
00110010000111010100110010010101000011110101010100

FAQ

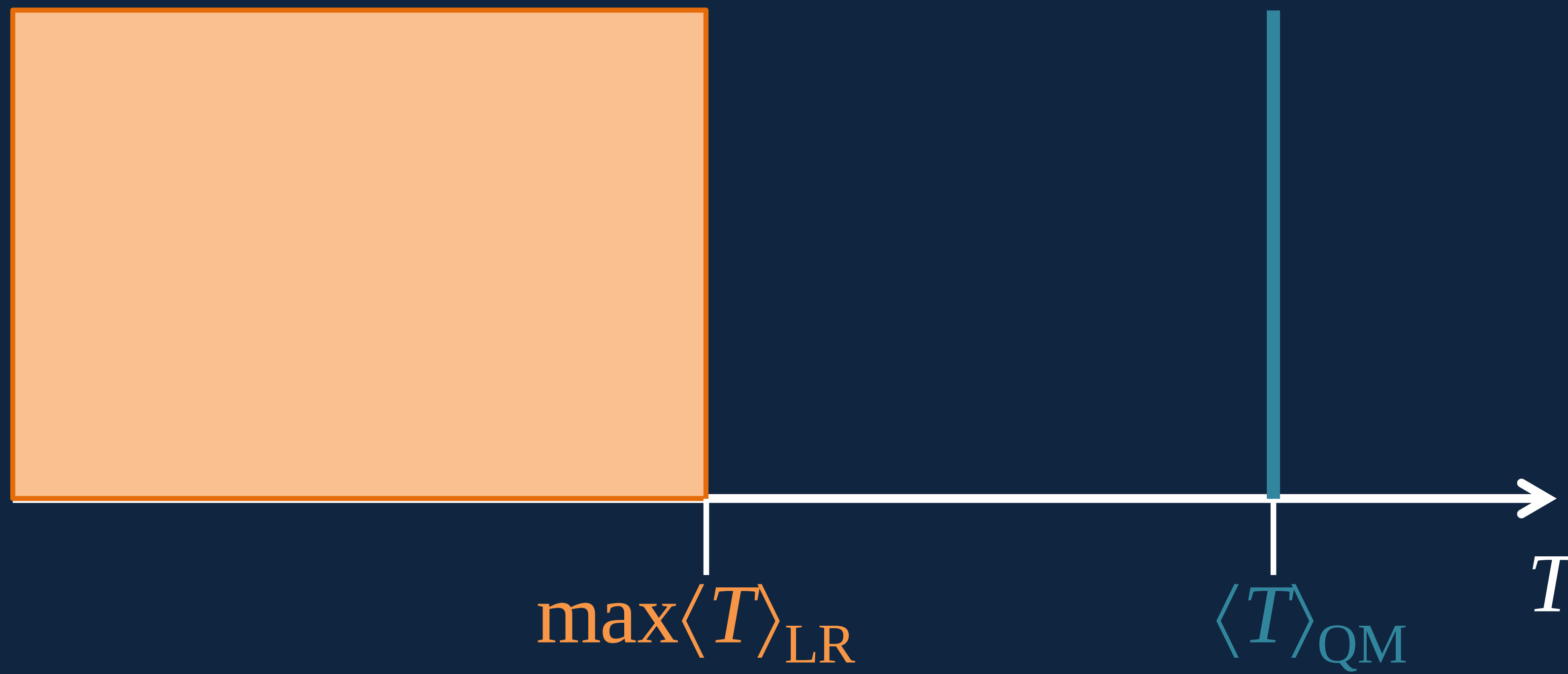
- No loopholes at all? Really?
- Have you thought of doing a Bayesian analysis?
- So, now we will never have to hear about tests of LR ever again!
- Didn’t you use random numbers to make random numbers?
- If nature is not local-realistic, what is it?

Bonus Slides

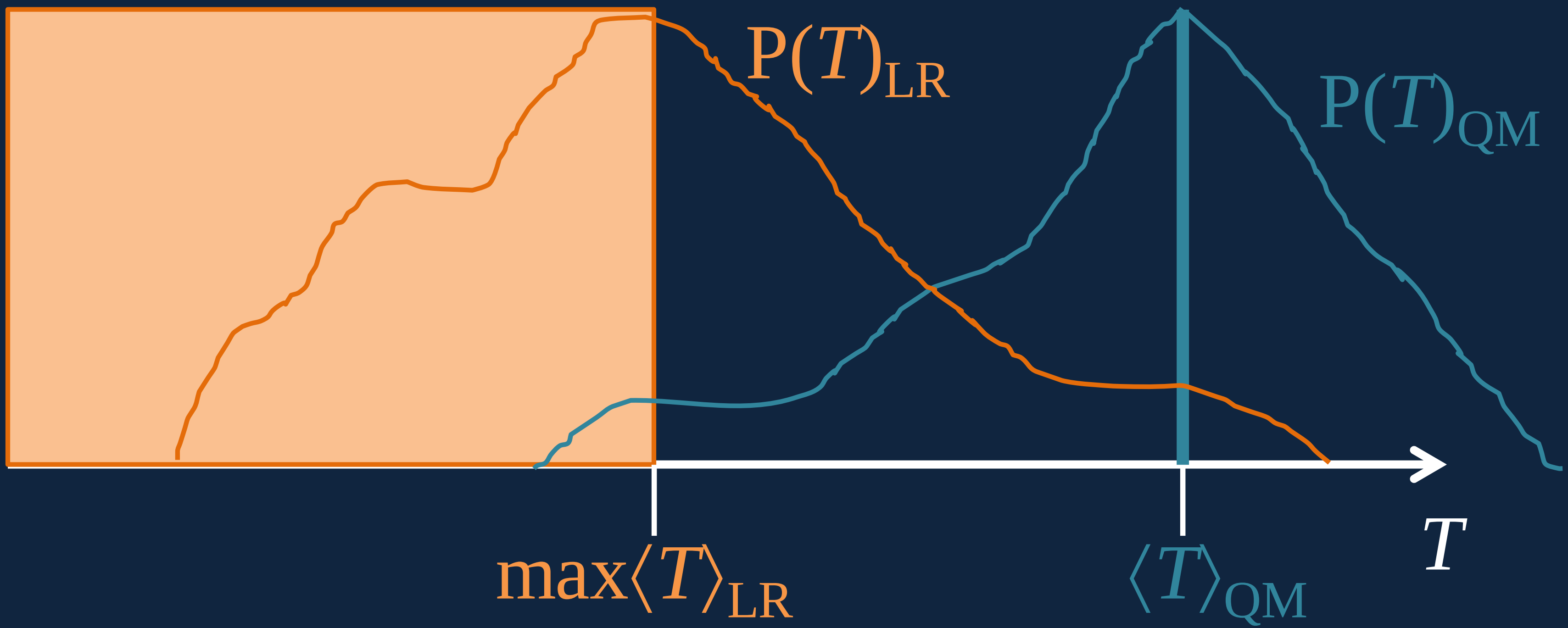
Lynden K. Shalm,[1] Evan Meyer-Scott,[2] Bradley G. Christensen,[3] Peter Bierhorst,[1] Michael A. Wayne,[3,4] Martin J. Stevens,[1] Thomas Gerrits,[1] Scott Glancy,[1] Deny R. Hamel,[5] Michael S. Allman,[1] Kevin J. Coakley,[1] Shellee D. Dyer,[1] Carson Hodge,[1] Adriana E. Lita,[1] Varun B. Verma,[1] Camilla Lambrocco,[1] Edward Tortorici,[1] Alan L. Migdall,[4,6] Yanbao Zhang,[2] Daniel R. Kumor,[3] William H. Farr,[7] Francesco Marsili,[7] Matthew D. Shaw,[7] Jeffrey A. Stern,[7] Carlos Abellán,[8] Waldimar Amaya,[8] Valerio Pruneri,[8,9] Thomas Jennewein,[2,10] Morgan W. Mitchell,[8,9] Paul G. Kwiat,[3] Joshua C. Bienfang,[4,6] Richard P. Mirin,[1] Emanuel Knill,[1] and Sae Woo Nam[1]

1. National Institute of Standards and Technology, 325 Broadway, Boulder, CO 80305, USA
2. Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, 200 University Ave West, Waterloo, Ontario, Canada, N2L 3G1
3. Department of Physics, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA
4. National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899,USA
5. Département de Physique et d'Astronomie, Université de Moncton, Moncton, New Brunswick E1A 3E9, Canada
6. Joint Quantum Institute, National Institute of Standards and Technology and University of Maryland, 100 Bureau Drive, Gaithersburg, Maryland 20899, USA
7. Jet Propulsion Laboratory, California Institute of Technology, 4800 Oak Grove Drive, Pasadena, CA 91109
8. ICFO - Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain
9. ICREA - Institució Catalana de Recerca i Estudis Avancats, 08015 Barcelona, Spain
10. Quantum Information Science Program, Canadian Institute for Advanced Research, Toronto, ON, Canada

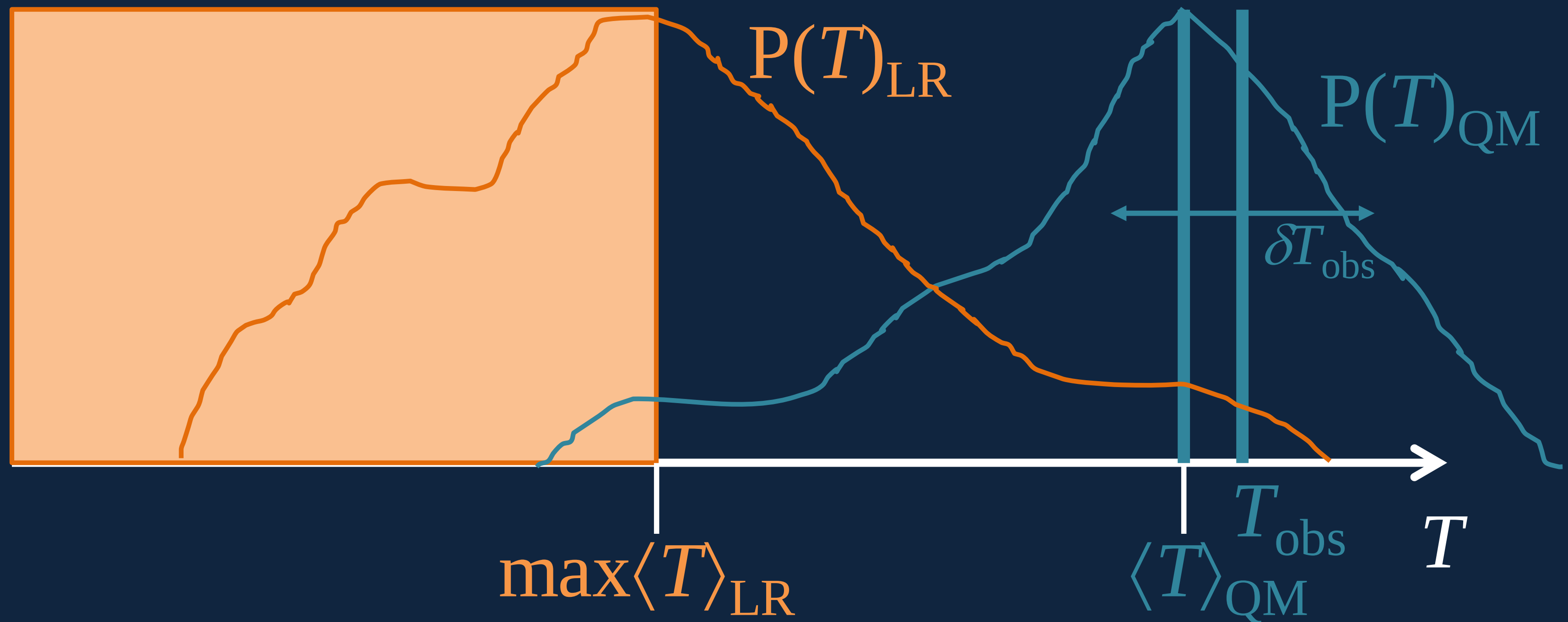
P-value Cartoon



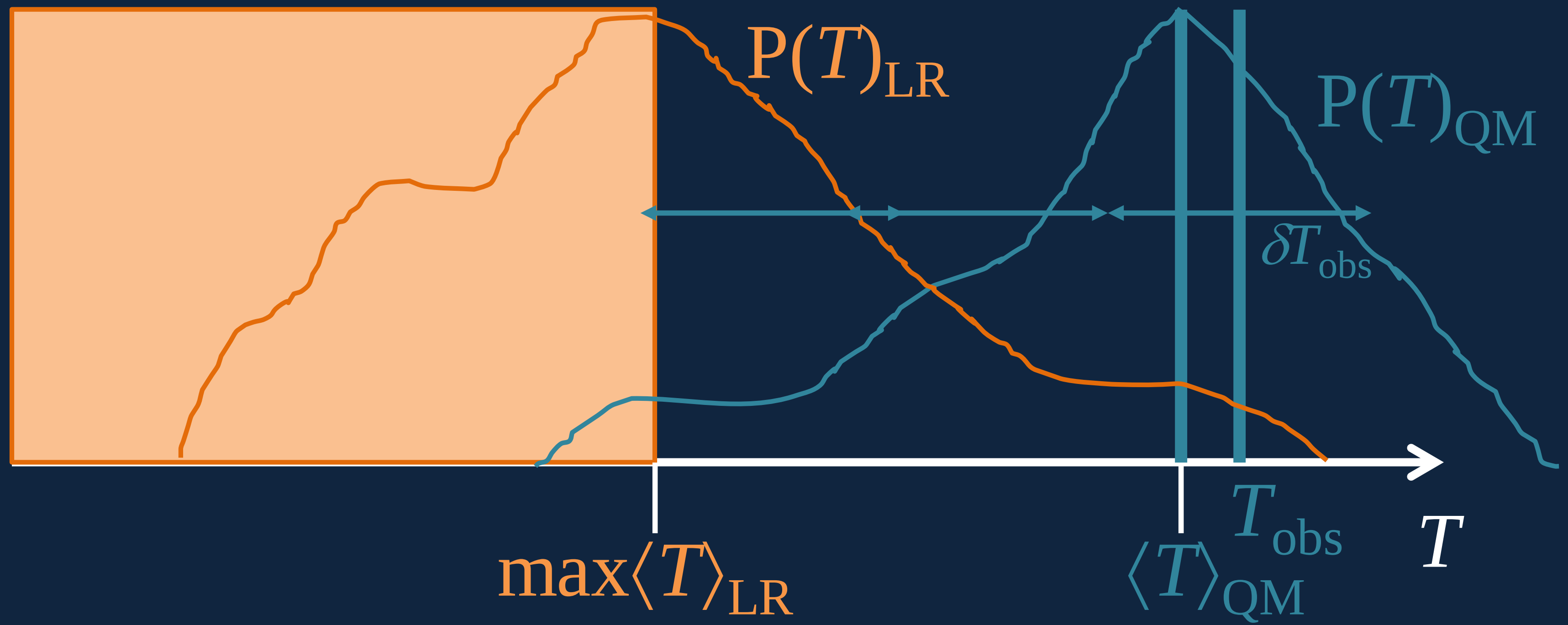
P-value Cartoon



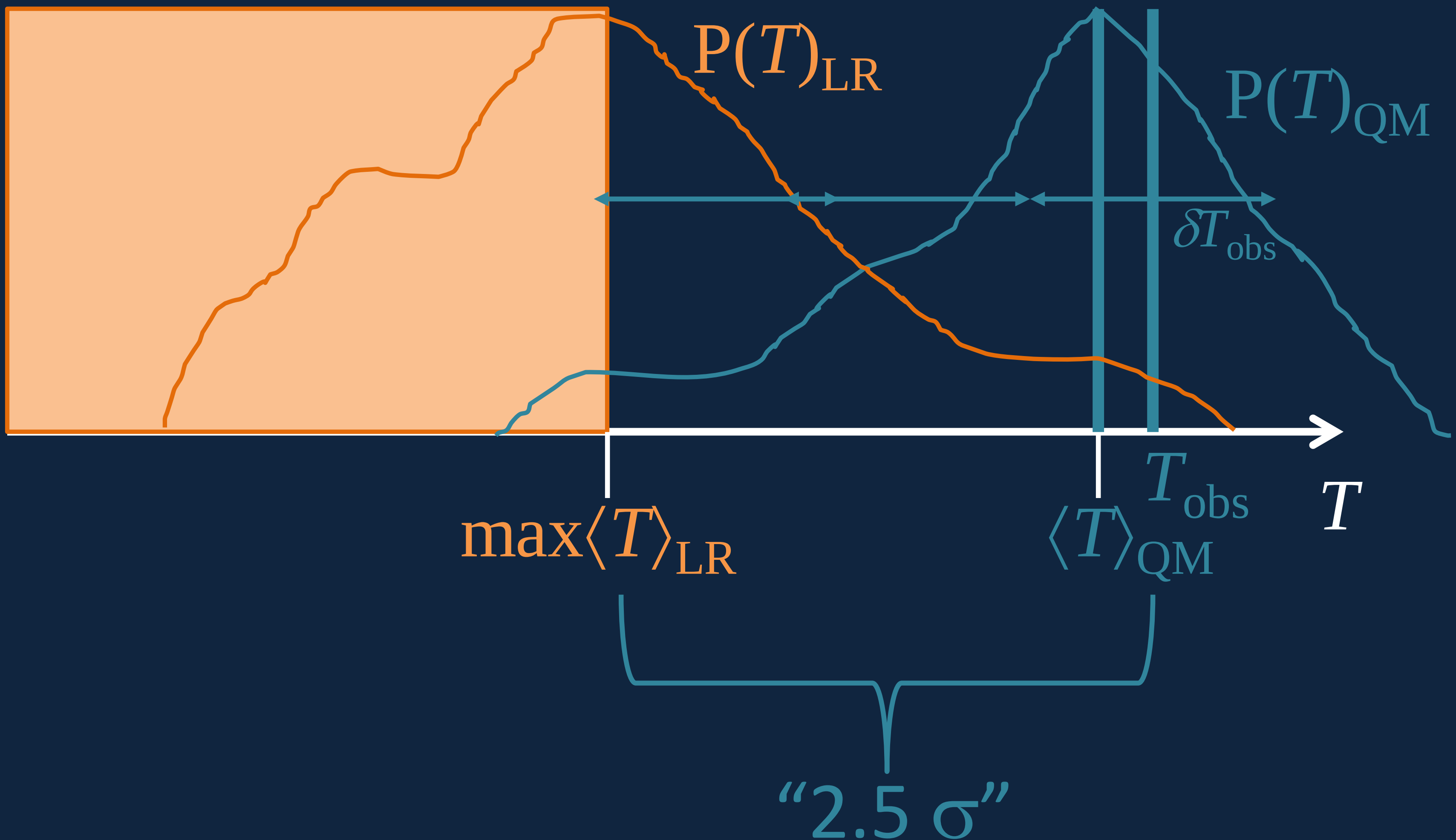
P-value Cartoon



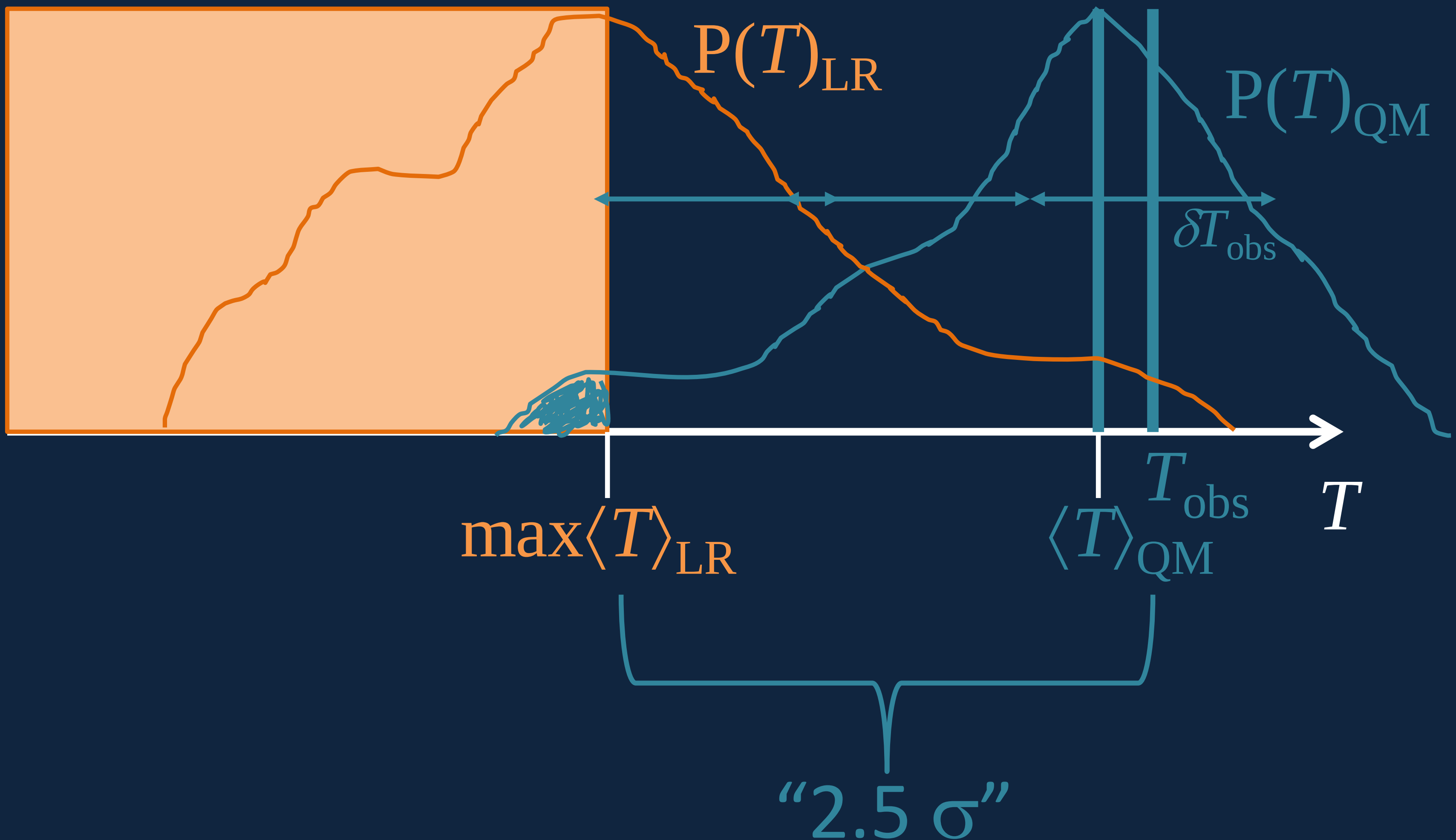
P-value Cartoon



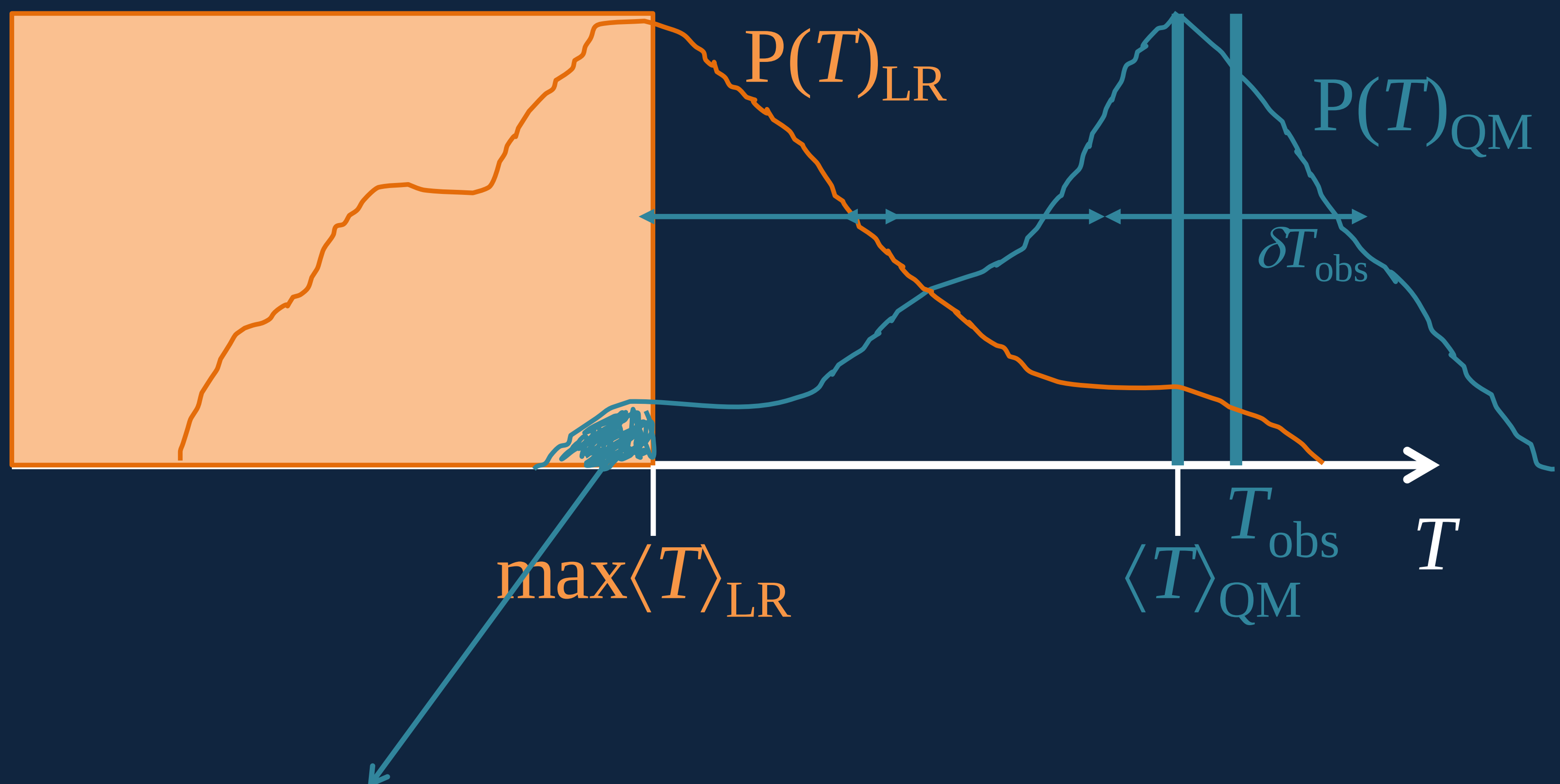
P-value Cartoon



P-value Cartoon

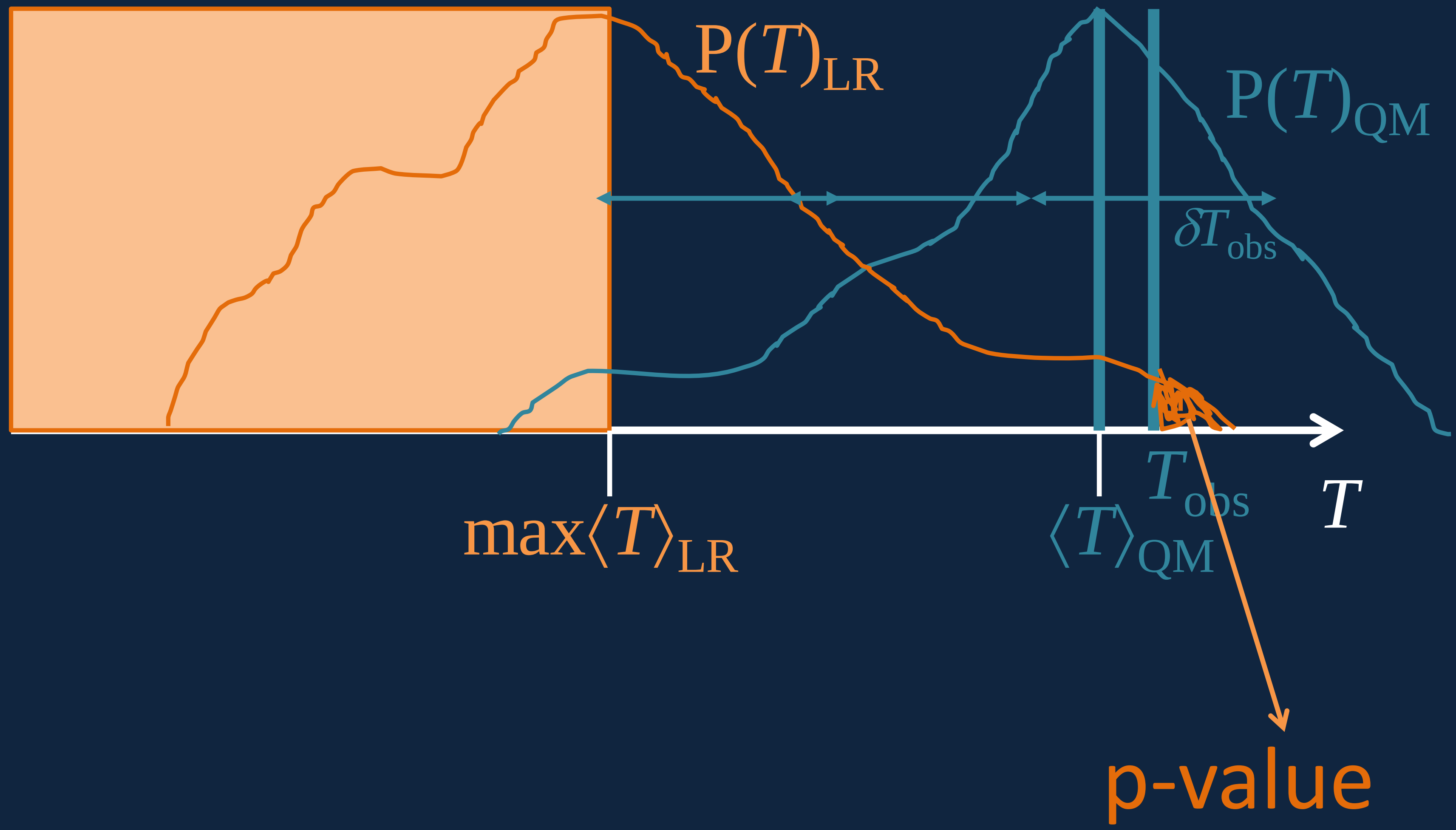


P-value Cartoon



not what
we wanted

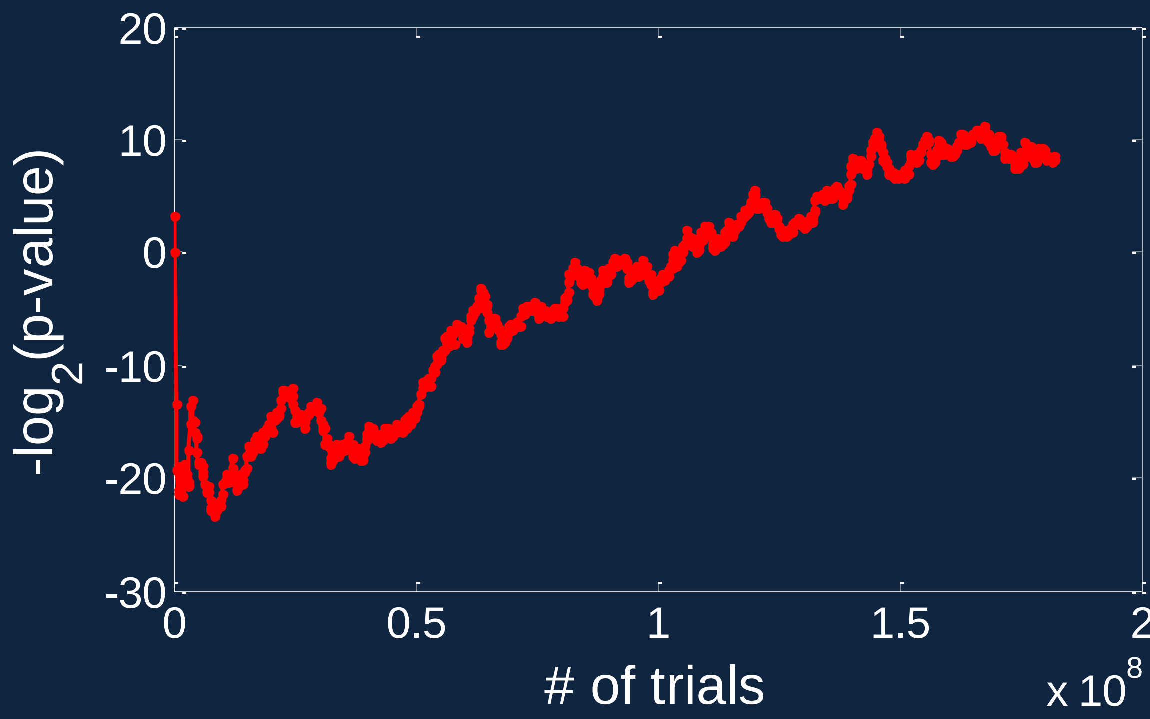
P-value Cartoon



Prediction Based Ratio (PBR)

- Achieves asymptotically optimal p-value reduction per trial.
- Uses previous trials to design best inequality for next trial.
- Before trial i construct $R_i(o_i)$ such that $R_i(o_i) \geq 0$ and $\langle R_i(o_i) \rangle_{\mathrm{LR}} \leq 1$.
  - Various constructions are possible.
  - We used [arXiv:1108.2468]
- Test statistic $T = \prod_{i=1}^{N} R_i(o_i)$.
- By the Markov Inequality $(\text{p-value})_{\mathrm{PBR}} \leq 1/T$.

Prediction Based Ratio



- “Classical XOR 3 data set” analyzing 5 pulses per trial.
- Big, bad learning transient.
- Final p-value = 0.0033

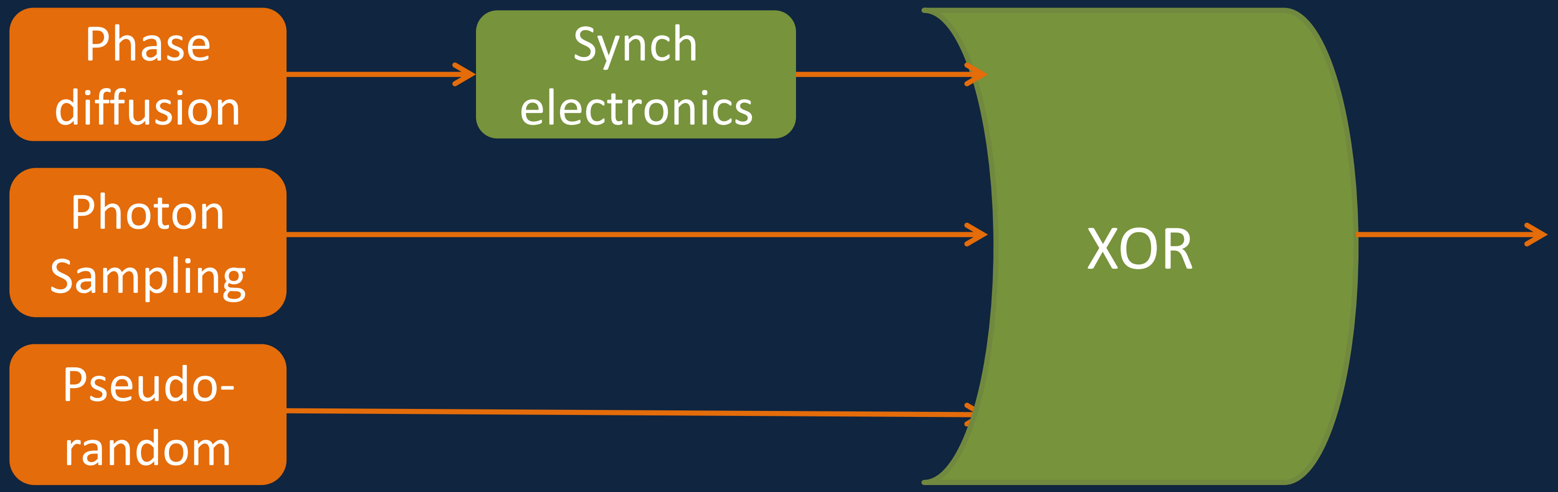
RNG Bias Correction

- What if RNGs have bias: P(a) $\neq P$(a') $\neq$ ½ or P(b) $\neq P$(b') $\neq$ ½?
- How should we adjust p-values?
- Define excess predictability bound
  - $\varepsilon = 2 \max[P(\text{a}), P(\text{a}'), P(\text{b}), P(\text{b}')] - 1$
- Under the optimal LR theory, $\varepsilon \neq 0$ allows
  - P(HEADS) $\leq \frac{1}{2} + \frac{\varepsilon}{1+\varepsilon^2}$.
  - If $\varepsilon \leq 3\times10^{-3}$, p-value $\leq 2.3\times10^{-7}$,

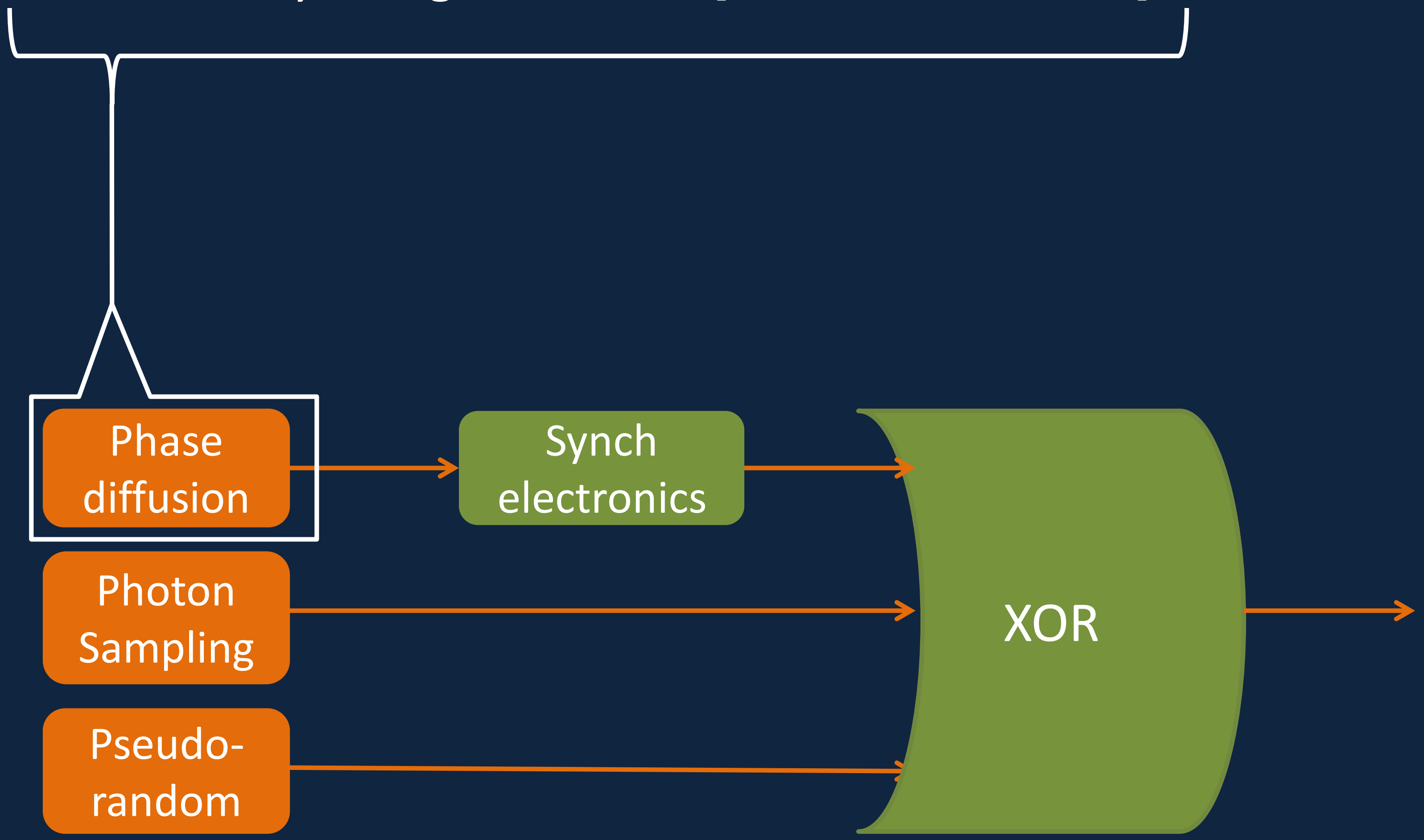
- Recall:
  - $++ab \rightarrow$ HEADS, {+0ab’, 0+a’b, ++a’b’} $\rightarrow$ TAILS
  - $\varepsilon \geq 2 \max[P(\text{a}), P(\text{a'}), P(\text{b}), P(\text{b'})] - 1$
- Under the optimal LR theory, $\varepsilon \neq 0$ allows
  - P(HEADS) $\leq \frac{1}{2} + \frac{\varepsilon}{1+\varepsilon^2}$.
- P-value = probability to get at least observed # of HEADS using biased coin.

- How to choose excess predictability ε?
- No "loophole-free" or "device-independent" options.
  - No statistical tests can measure ε.
  - An instance of the "super-determinism loophole".

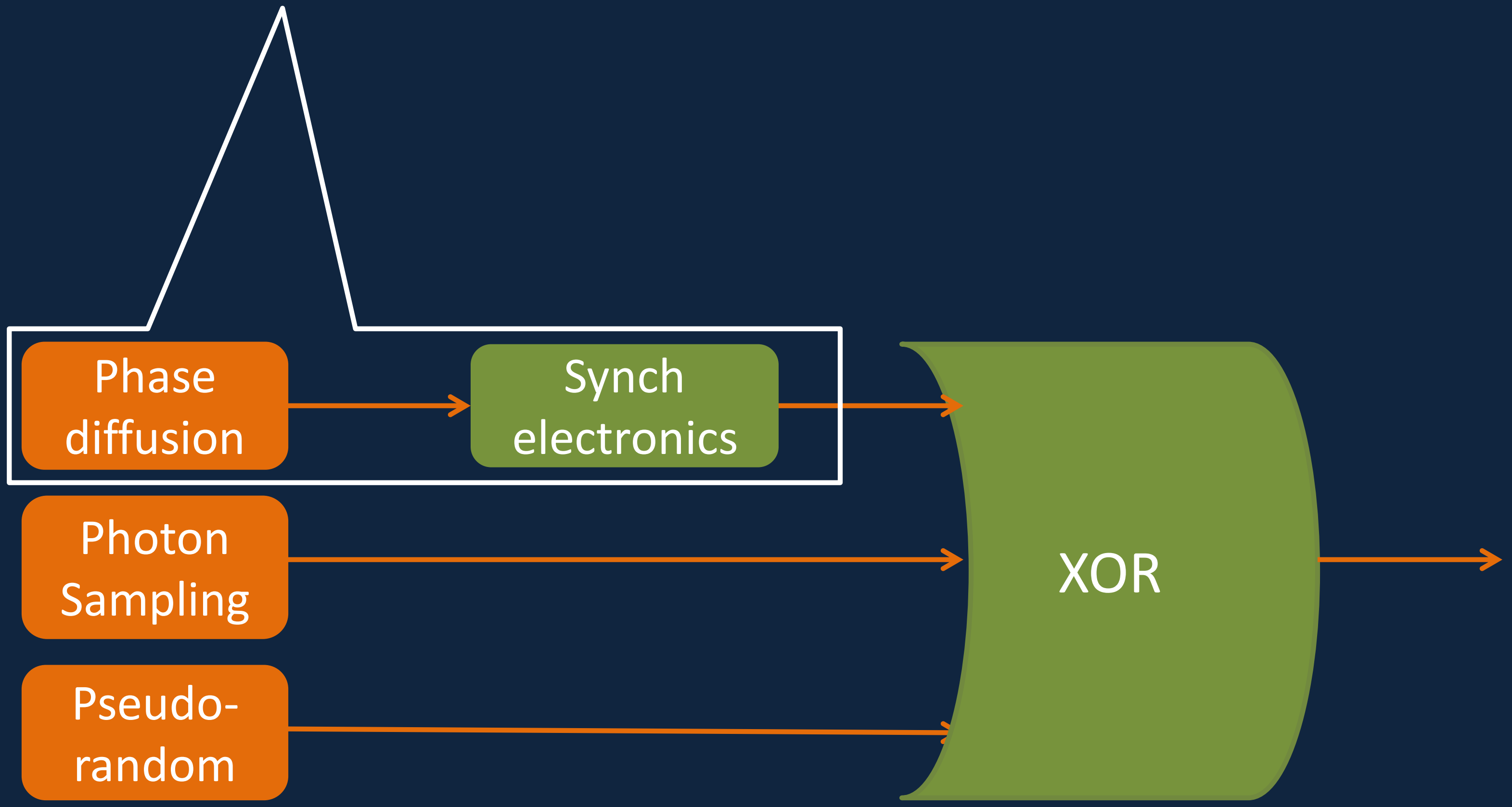
- Physics modeling and characterization

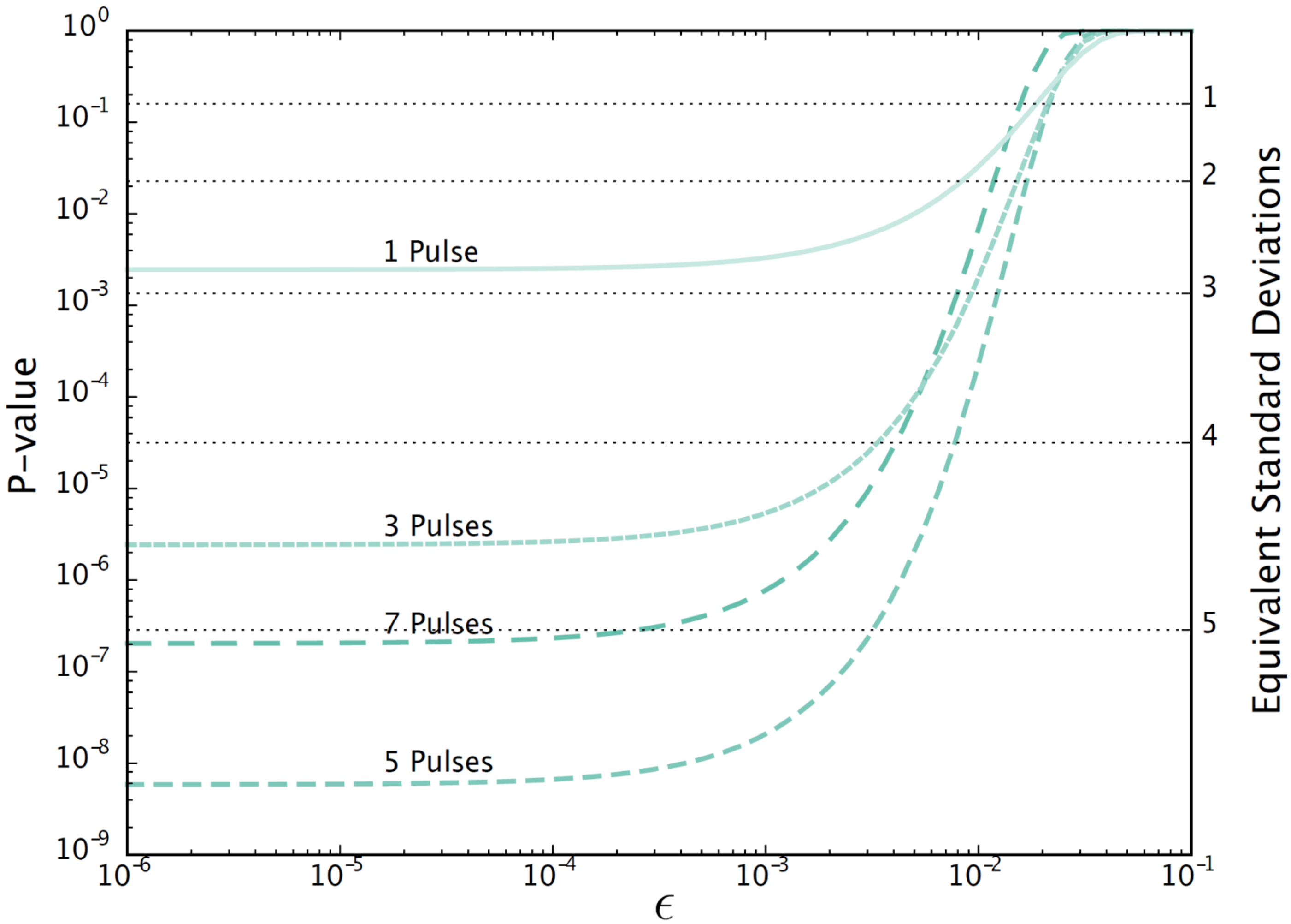


- Physics modeling and characterization
  - Described by Morgan Mitchel [arXiv:1506.02712].

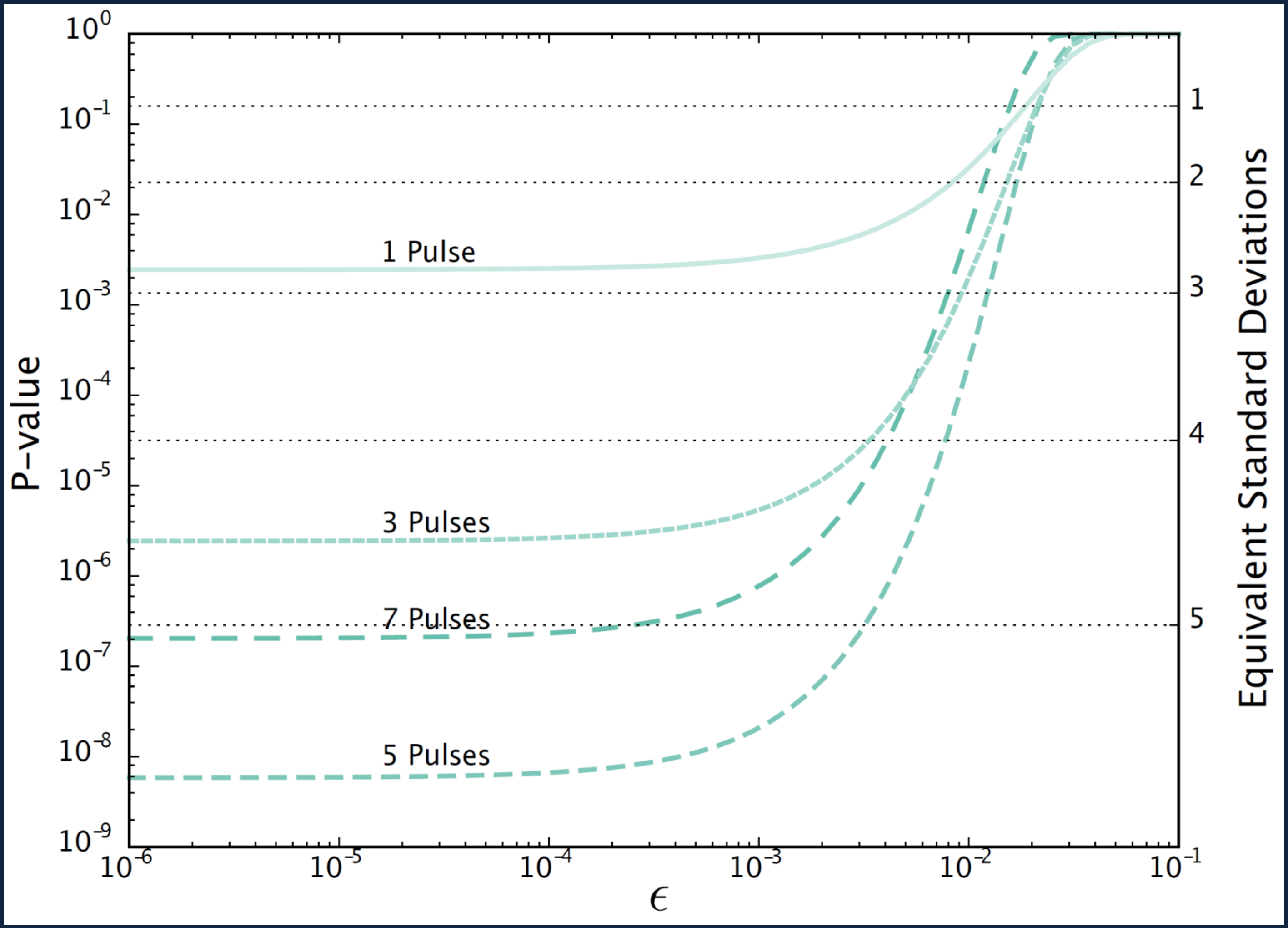


- Physics modeling and characterization
  - Described by Morgan Mitchel [arXiv:1506.02712].
  - Bias after synch is greater than Morgan’s model predicts. ☹

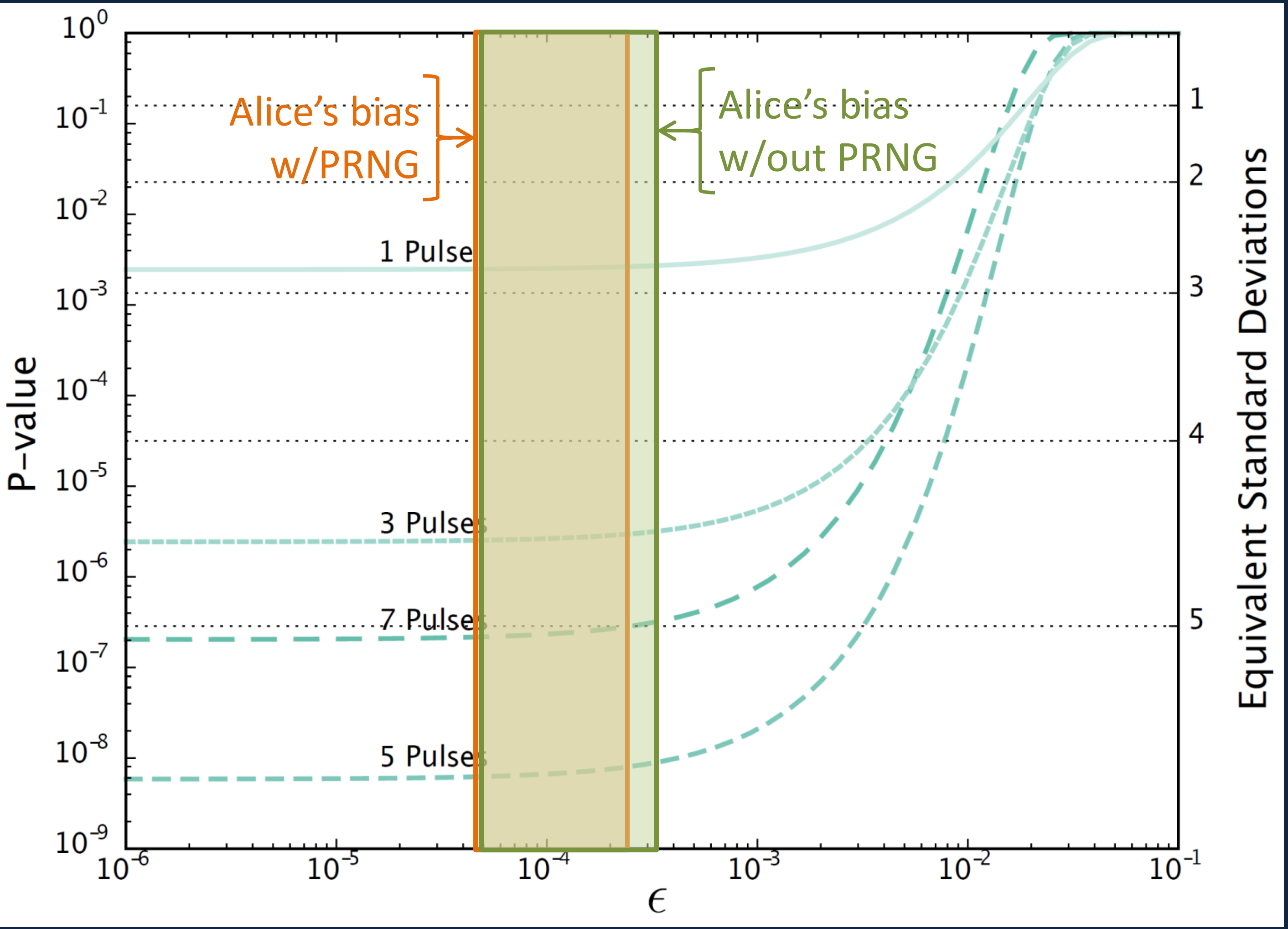




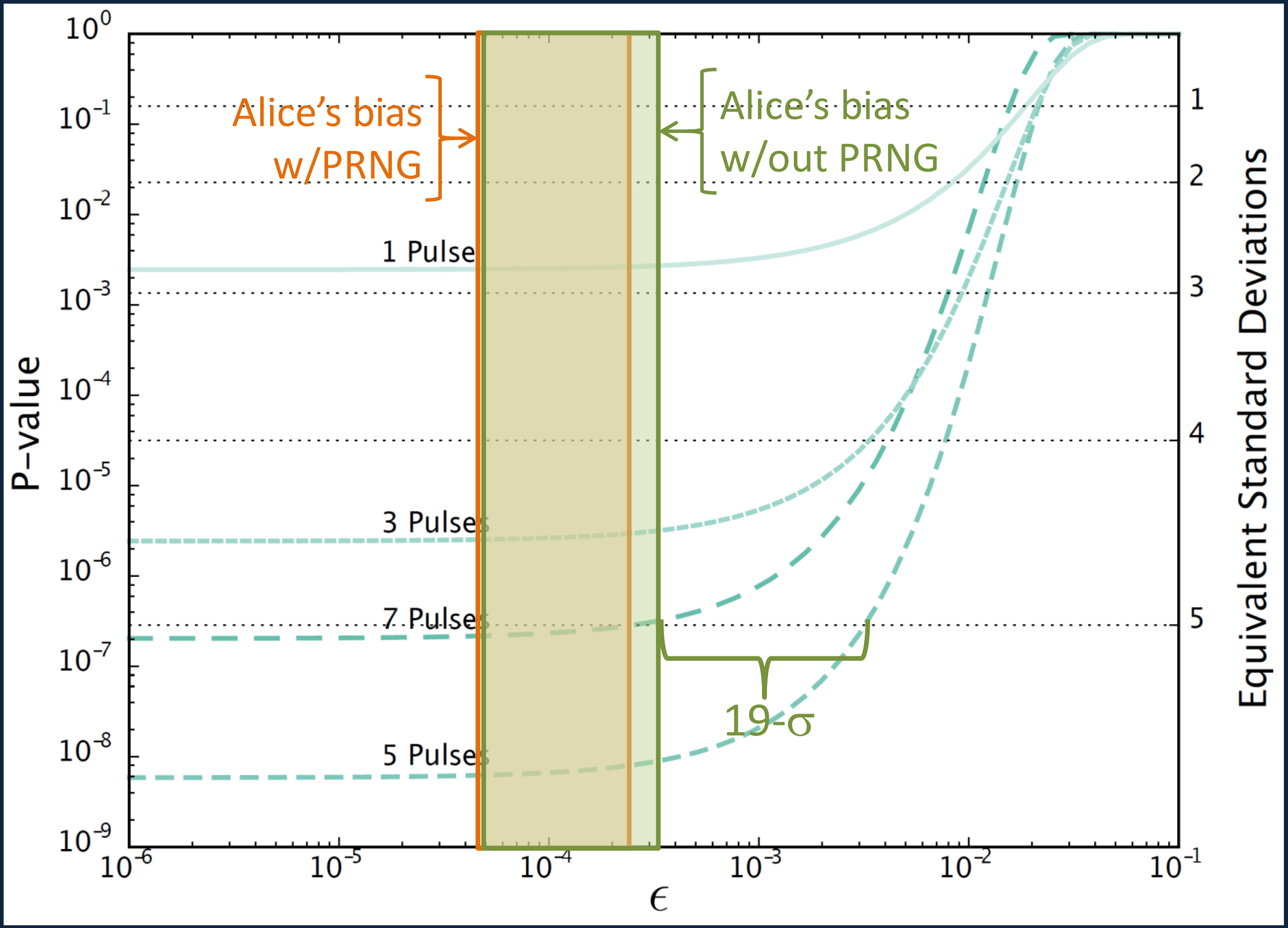
P−value
Equivalent Standard Deviations
1 Pulse
3 Pulses
7 Pulses
5 Pulses
ϵ
10^0
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
10^{-8}
10^{-9}
10^{-6}
10^{-5}
10^{-4}
10^{-3}
10^{-2}
10^{-1}
1
2
3
4
5



- Bias measurements allow us to lower-bound ε.



- Bias measurements allow us to lower-bound ε.
- Shaded regions show 1-σ uncertainty.
- Alice's bias is larger than Bob's



- Bias measurements allow us to lower-bound ε.
- Shaded regions show 1-σ uncertainty.
- Alice's bias is larger than Bob's

Choosing ε

- Measured bias gives a lower bound: $\varepsilon \geq 2\times10^{-4}$.
- We need an upper bound!
- ¯_(ツ)_/¯ … × 15 should be enough.
- $\varepsilon \leq 15\times2\times10^{-4} = 3\times10^{-3}$.
- With this ε, p-value becomes $\cancel{5.85\times10^{-9}}$ 2.3×10^{-7}.

- Measured bias gives a lower bound: $\varepsilon \geq 2\times10^{-4}$.
- We need an upper bound!
- ¯_(ツ)_/¯ … × 15 should be enough.
- $\varepsilon \leq 15\times2\times10^{-4} = 3\times10^{-3}$.
- With this ε, p-value becomes ~~5.85×10^{-9}~~ 2.3×10^{-7}.
- (We ignored 2 randomness sources' contribution in ε.)