Experimentally Generated Random Numbers Certified by the Impossibility of Superluminal Signaling

Peter Bierhorst, Lynden K. Shalm, Alan Mink, Stephen Jordan, Yi-Kai Liu, Scott Glancy, Bradley Christensen, Andrea Rommal, Sae Woo Nam, Emanuel Knill

National Institute of Standards and Technology, Boulder, CO

peter.bierhorst@nist.gov

September 16, 2016

First Loophole-Free Bell Experiments

Multiple experimental groups have recently reported loophole-free Bell experiments:

- Hensen et al., Nature **526** 682, October 2015
- Shalm et al., Phys. Rev. Lett. **115** 250402, December 2015
- Giustina et al., Phys. Rev. Lett. **115** 250401, December 2015
- Weinfurter et al., QCrypt conference presentation, September 2016

First Loophole-Free Bell Experiments

Local realism is falsified.

First Loophole-Free Bell Experiments

Local realism is falsified.

Now what?

First Loophole-Free Bell Experiments

Local realism is falsified.

Now what?

Quantum Information Theory!

Randomness in Bell Experiments

Nonlocality + Prohibition of FTL signaling $\rightarrow$ Randomness

Experimental Scheme

Alice measures a, Bob measures b

Experimental Scheme

Alice measures a', Bob measures b

Experimental Scheme

Alice measures a, Bob measures b'

Experimental Scheme

Alice measures a', Bob measures b'.

Experimental Distributions

	$++$	$+0$	$0+$	00
ab	.4268	.0732	.0732	.4268
ab'	.4268	.0732	.0732	.4268
$a'b$	.4268	.0732	.0732	.4268
$a'b'$	.0732	.4268	.4268	.0732

$$P(+0|ab') = .0732$$

Experimental Distributions

A Local Realist Distribution

	$++$	$+0$	$0+$	00
ab	$1/2$	0	0	$1/2$
ab'	$1/2$	0	0	$1/2$
$a'b$	$1/2$	0	0	$1/2$
$a'b'$	$1/2$	0	0	$1/2$

Experimental Distributions

A Local Realist Distribution

	++	+0	0+	00
ab	1/2	0	0	1/2
ab'	1/2	0	0	1/2
$a'b$	1/2	0	0	1/2
$a'b'$	1/2	0	0	1/2

$.5\times$

	++	+0	0+	00
ab	1	0	0	0
ab'	1	0	0	0
$a'b$	1	0	0	0
$a'b'$	1	0	0	0

$+.5\times$

	++	+0	0+	00
ab	0	0	0	1
ab'	0	0	0	1
$a'b$	0	0	0	1
$a'b'$	0	0	0	1

Experimental Distributions

The PR box, a nonlocal distribution:

	$++$	$+0$	$0+$	00
ab	$1/2$	0	0	$1/2$
ab'	$1/2$	0	0	$1/2$
$a'b$	$1/2$	0	0	$1/2$
$a'b'$	0	$1/2$	$1/2$	0

Experimental Distributions

A possible decomposition?

	++	+0	0+	00
ab	1	0	0	0
ab'	1	0	0	0
$a'b$	1	0	0	0
$a'b'$	0	1	0	0

and

	++	+0	0+	00
ab	0	0	0	1
ab'	0	0	0	1
$a'b$	0	0	0	1
$a'b'$	0	0	1	0

Experimental Distributions

A possible decomposition?

	$++$	$+0$	$0+$	00
ab	1	0	0	0
ab'	1	0	0	0
$a'b$	1	0	0	0
$a'b'$	0	1	0	0

and

	$++$	$+0$	$0+$	00
ab	0	0	0	1
ab'	0	0	0	1
$a'b$	0	0	0	1
$a'b'$	0	0	1	0

When Bob chooses b', Alice can signal Bob.

Experimental Distributions

If one cannot send signals between Alice and Bob, then the randomness in the PR box cannot be eliminated.

	$++$	$+0$	$0+$	00
ab	$1/2$	0	0	$1/2$
ab'	$1/2$	0	0	$1/2$
$a'b$	$1/2$	0	0	$1/2$
$a'b'$	0	$1/2$	$1/2$	0

Data from a photonic loophole-free experiment

Raw Counts from a data run:

	$++$	$+0$	$0+$	00
ab	6547	3415	3276	33036105
ab'	7080	2931	24396	33007876
$a'b$	6853	22536	3062	33005133
$a'b'$	117	28740	31300	32971848

Data from a photonic loophole-free experiment

Raw Counts from a data run:

	$++$	$+0$	$0+$	00
ab	6547	3415	3276	33036105
ab'	7080	2931	24396	33007876
$a'b$	6853	22536	3062	33005133
$a'b'$	117	28740	31300	32971848

Induced empirical distribution (No-signaling adjusted):

	$++$	$+0$	$0+$	00
ab	0.00019868	0.00010348	0.00009916	0.99959860
ab'	0.00021368	0.00008848	0.00073796	0.99895980
$a'b$	0.00020532	0.00067616	0.00009252	0.99902592
$a'b'$	0.00000356	0.00087792	0.00094812	0.99817032

Data from a photonic loophole-free experiment

Induced empirical distribution (No-signaling adjusted):

	$++$	$+0$	$0+$	00
ab	0.00019868	0.00010348	0.00009916	0.99959860
ab'	0.00021368	0.00008848	0.00073796	0.99895980
$a'b$	0.00020532	0.00067616	0.00009252	0.99902592
$a'b'$	0.00000356	0.00087792	0.00094812	0.99817032

Can be induced by:

$.999972\times$ Local Realist Distribution

$+$

$.000028\times$ PR box

Data from a photonic loophole-free experiment

.000028$\times$ PR Box

Over the course of 132,161,215 trials, this means $\sim$3,700 PR boxes.

Extracting the Randomness

To certify the min-entropy and extract the randomness, we need a protocol that is:

- Effective in a very low-violation regime (CHSH $\simeq 2.0000564$)
- Robust to possible memory effects
- Handles finite statistics effects (no asymptotic bounds)

Extracting the Randomness

Existing methods are not effective in our regime

- Pironio et al., Pironio/Massar, Fehr/Gelles/Schaffner
- Vidick/Vazirani
- Chung/Shi/Wu, Miller/Shi
- Coudron/Yuen
- Bancal/Sheridan/Scarani, Nieto-Silleras/Pironio/Silman
- Thinh et al.

Extracting the Randomness

The following papers develop statistical analysis techniques that are effective for falsifying local realism in low-violation photonic experiments, and suggest a way forward for certifying min-entropy.

- "A robust mathematical model for a loophole-free ClauserHorne experiment," P. Bierhorst, J. Phys. A 2015
- "Requirements for a loophole-free photonic Bell test using imperfect setting generators," J. Kofler, M. Giustina, J.-A. Larsson, M. W. Mitchell, Phys. Rev. A 2016
- "Asymptotically optimal data analysis for rejecting local realism," Y. Zhang, S. Glancy, E. Knill, Phys. Rev. A 2011

Extracting the Randomness

The following papers develop statistical analysis techniques that are effective for falsifying local realism in low-violation photonic experiments, and suggest a way forward for certifying min-entropy.

- "A robust mathematical model for a loophole-free ClauserHorne experiment," P. Bierhorst, J. Phys. A 2015
- "Requirements for a loophole-free photonic Bell test using imperfect setting generators," J. Kofler, M. Giustina, J.-A. Larsson, M. W. Mitchell, Phys. Rev. A 2016
- "Asymptotically optimal data analysis for rejecting local realism," Y. Zhang, S. Glancy, E. Knill, Phys. Rev. A 2011

The Protocol

1. Choose a Bell function T from experimental outcomes to $\mathbb{R}^+$, satisfying $T > 0$, $E_{LR}(T) \leq 1$, $E_{PR}(T) = 1 + m$, $m > 0$
2. In an experiment of n trials, compute $\prod_{i=1}^{n} T_i = V$.
3. For values of $V >> 1$, our result puts a lower bound on the amount of min-entropy σ_s present in the data
4. Extract randomness to ϵ-uniform bits using Trevisan extractor

The Protocol

1. Choose a Bell function T from experimental outcomes to $\mathbb{R}^+$, satisfying $T > 0$, $E_{LR}(T) \leq 1$, $E_{PR}(T) = 1 + m$, $m > 0$
2. In an experiment of n trials, compute $\prod_{i=1}^{n} T_i = V$.
3. For values of $V >> 1$, our result puts a lower bound on the amount of min-entropy σ_s present in the data
4. Extract randomness to ϵ-uniform bits using Trevisan extractor

	++	+0	0+	00
ab	1.0244	0.9643	0.9638	1
ab'	1.0315	0.9393	0.9958	1
$a'b$	1.0318	0.9955	0.9399	1
$a'b'$	0.9123	1.0044	1.0041	1

m = 0.012

Generate T with method of Zhang, Glancy, Knill, Phys. Rev. A 2011

The Protocol

1. Choose a Bell function T from experimental outcomes to $\mathbb{R}^+$, satisfying $T > 0$, $E_{LR}(T) \leq 1$, $E_{PR}(T) = 1 + m$, $m > 0$
2. In an experiment of n trials, compute $\prod_{i=1}^{n} T_i = V$.
3. For values of $V >> 1$, our result puts a lower bound on the amount of min-entropy σ_s present in the data
4. Extract randomness to ϵ-uniform bits using Trevisan extractor

$$n = 132,161,215$$

$$V = 2.76 \times 10^9$$

The Protocol

1. Choose a Bell function T from experimental outcomes to $\mathbb{R}^+$, satisfying $T > 0$, $E_{LR}(T) \leq 1$, $E_{PR}(T) = 1 + m$, $m > 0$
2. In an experiment of n trials, compute $\prod_{i=1}^{n} T_i = V$.
3. For values of $V >> 1$, our result puts a lower bound on the amount of min-entropy σ_s present in the data
4. Extract randomness to ϵ-uniform bits using Trevisan extractor

$$\text{Key result:} \quad \sigma_s \geq -n \log_2 \left[\frac{2m + 1 - \sqrt[n]{V \epsilon_s}}{2m} \right]$$

When the protocol is passed, σ_s is the average min entropy of the output string, conditioned on the setting string.

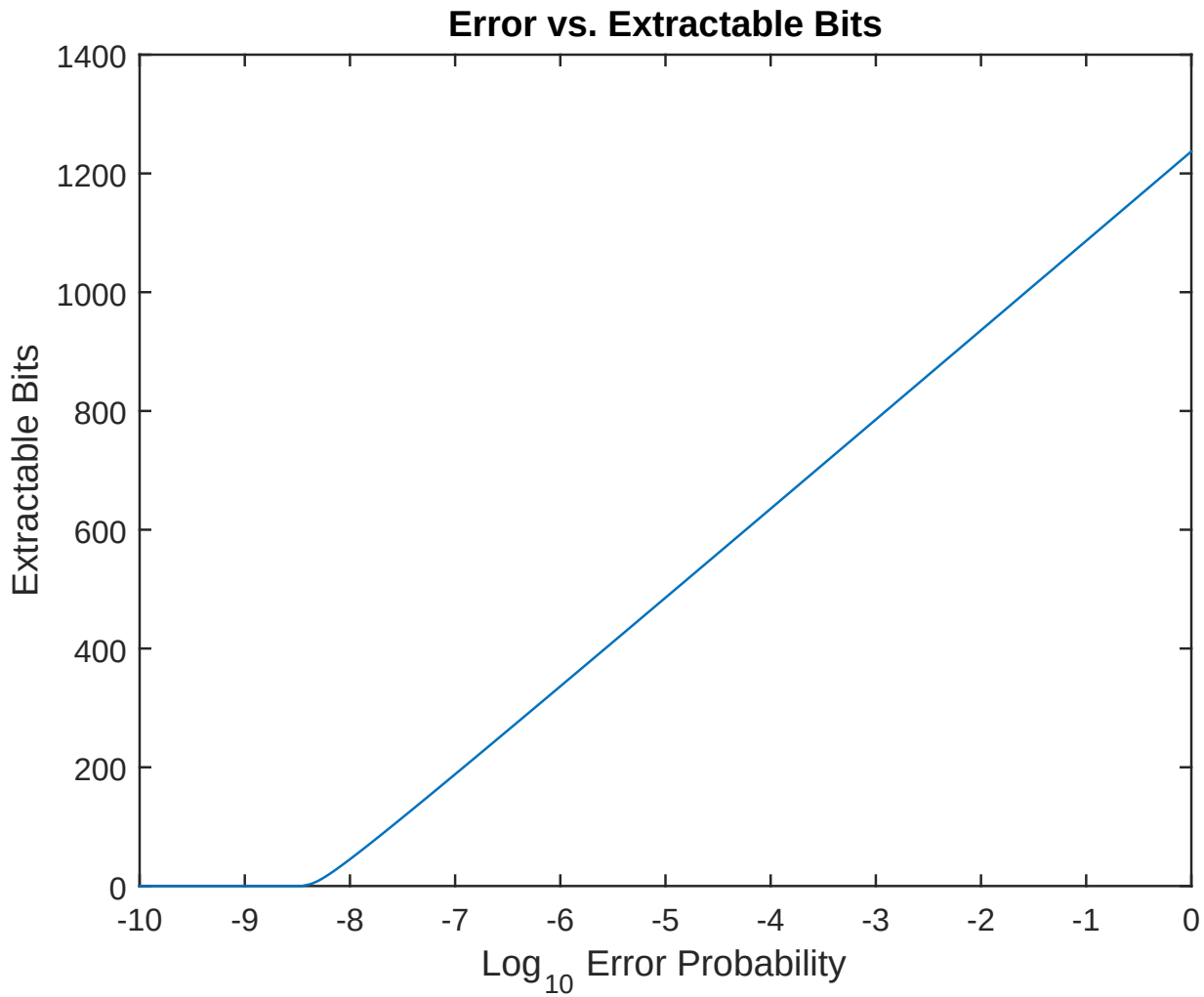
The Protocol

1. Choose a Bell function T from experimental outcomes to $\mathbb{R}^+$, satisfying $T > 0$, $E_{LR}(T) \leq 1$, $E_{PR}(T) = 1 + m$, $m > 0$
2. In an experiment of n trials, compute $\prod_{i=1}^{n} T_i = V$.
3. For values of $V >> 1$, our result puts a lower bound on the amount of min-entropy σ_s present in the data
4. Extract randomness to ϵ-uniform bits using Trevisan extractor

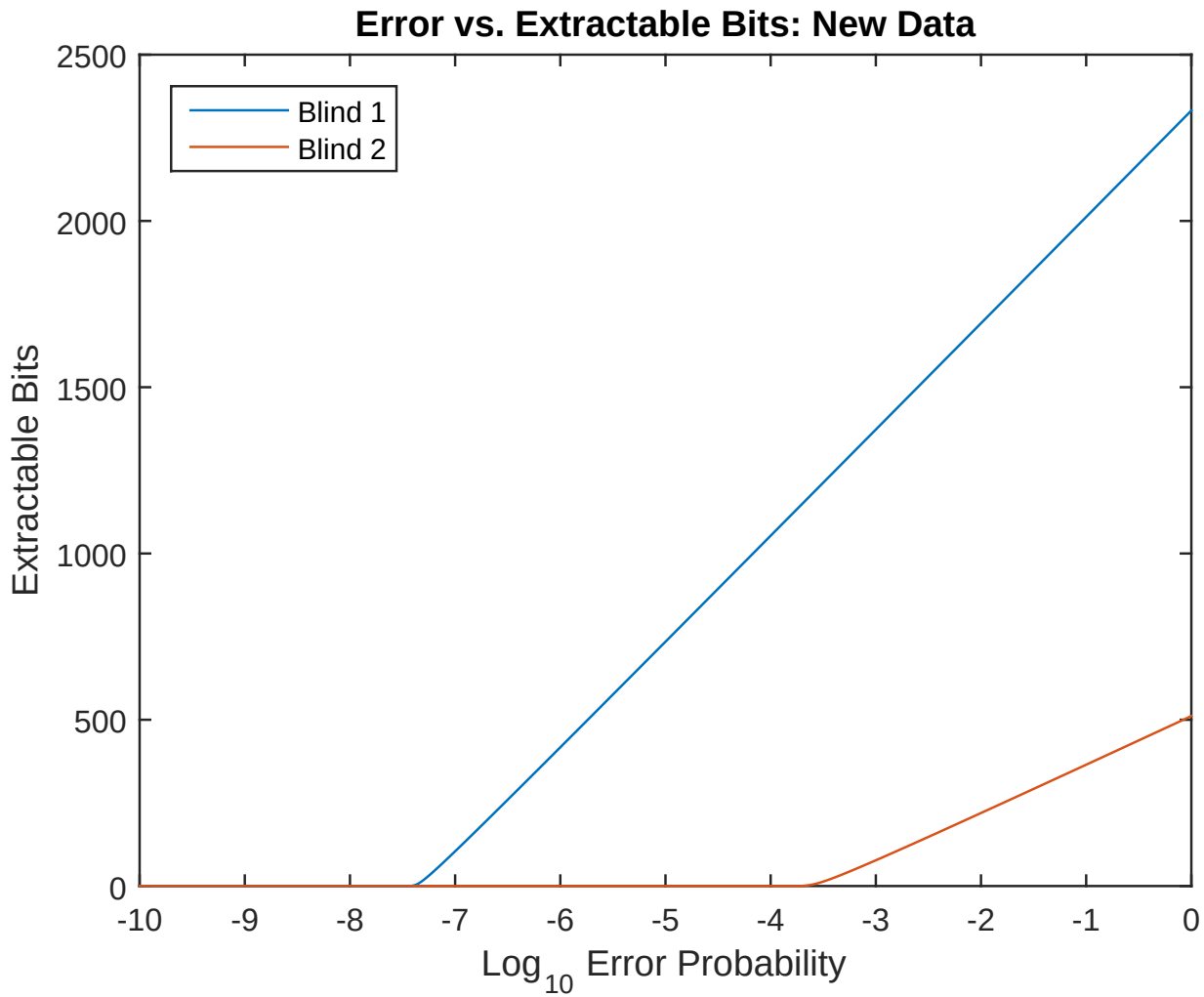
We use updated software we wrote based on the Mauerer, Portmann, Scholz (arXiv:1212:.0520) implementation of Trevisan's extractor. We can extract up to t ϵ-uniform bits where t obeys the following formula:

$$t + 4 \log_2 t \leq \sigma_s - 6 + 4 \log_2 \epsilon_{\text{ext}}$$

Results


Error vs. Extractable Bits
Extractable Bits
1400
1200
1000
800
600
400
200
0
-10
-9
-8
-7
-6
-5
-4
-3
-2
-1
0
Log 10 Error Probability

Results


Error vs. Extractable Bits: New Data
Blind 1
Blind 2
Extractable Bits
2500
2000
1500
1000
500
0
-10
-9
-8
-7
-6
-5
-4
-3
-2
-1
0
Log10 Error Probability

Conclusion

256 Extracted Bits:

1011000000101000101000011010100111001010110000111001010011101111
1001101101100010011110100101010100101001100101101110011000101001
0000100001011000100100101111110011001000000111111110001110111100
0111101101110110001100100001110101001100100101010000111101010100

Thank you!

Peter Bierhorst
National Institute of Standards and Technology, Boulder, CO