ILLINOIS

Quantum Random Number Generators

A bunch of BS (beamsplitters…)

P. Kwiat

Kwiat's Quantum Clan (2012)

Graduate Students:

- Rebecca Holmes
- Aditya Sharma
- Kevin McCusker (NWU)
- Trent Graham
- Brad Christensen
- Kevin Zielnicki
- Mike Wayne

Undergraduates:

- Daniel Kumor
- David Schmid
- Jia Jun ("JJ") Wong
- Ben Chng
- Cory Alford
- Brian Huang

Visit Prof: Hee Su Park

Post-Doc: Jian Wang

Outline

1. Motivation
2. Location, location
3. It's all a matter of timing
   - how I know when I have a good idea…
   - post-processed randomness
   - pre-processed randomness
   - a very high-rate version, not
   - a very high-rate version
   - application to QKD
4. Gerd's CV
5. DIQRNG
   - "Heinz Ketchup"
   - "when it absolutely has to be there overnight"
6. DIQKD via VLPC?

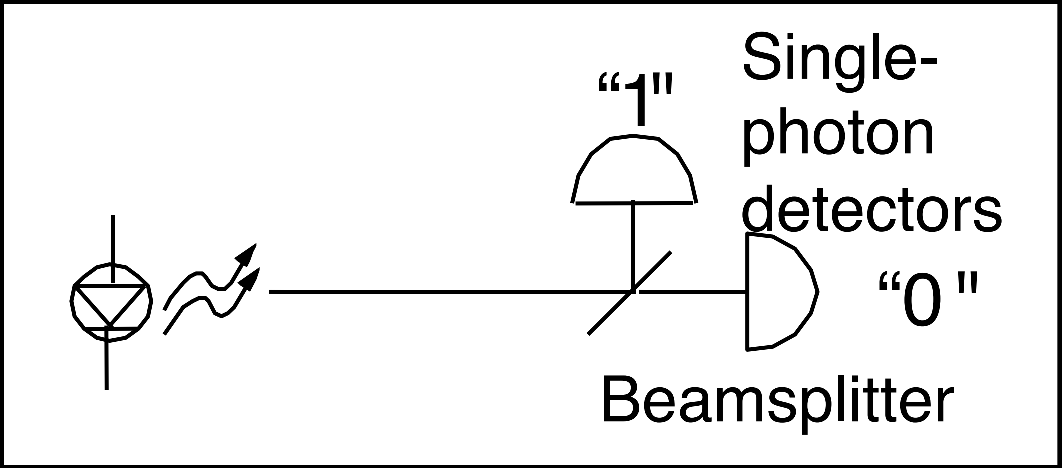
Motivation

- Base security statement of QKD on pseudo-random number generator? NO
- Use physical, non-quantum RNG? better not (bad coin, or bad flipper…)
- Need randomness in several places for QKD:
  - Transmitter basis choice
  - Transmitter bit choice
  - Receiver basis choice
- This can sometimes be achieved passively (i.e., BS at the receiver).
- Entanglement can also give random bit values

Best Motivation: Renato said so…

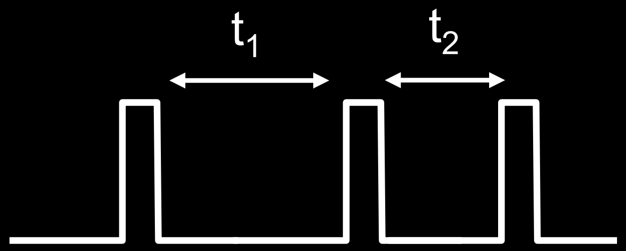
Commercial Quantum Information: Random Number Generation

God ***does*** play dice with the Universe!



- Beamsplitter Approach
  - Problems: Inefficient (< one bit per detection)
    - Detector saturation
    - Different detector efficiencies (possibly over time)
    - Multiple (expensive) detectors
  - Currently Available: ID Quantique
    - 4 MHz (one pair of detectors); 16 MHz (4 pairs of detectors)

Time-based Implementation



- Time-based Approach
  [M. Stipcevic, B. Rogina. "Quantum random number generator based on photonic emission in semiconductors", Rev. Sci. Inst. 78, 045154 (2007)]
  - Measure relative intervals between pulses
  - If $t_1 > t_2$ then record a "0" bit, else a "1" bit
  - Only one detector needed

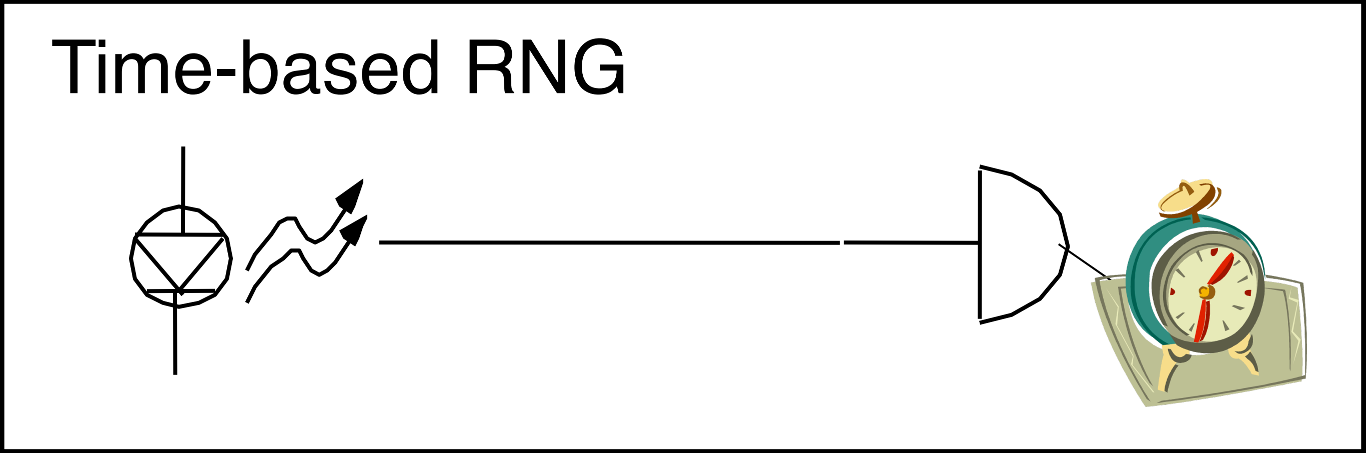
  - Problems
    - Maximum of 1/2 bit per detection
    - Slow output rate (1 MHz)

Outline

1. Motivation
2. Location, location
3. It's all a matter of timing
   - how I know when I have a good idea…
   - post-processed randomness
   - pre-processed randomness
   - a very high-rate version, not
   - a very high-rate version
   - application to QKD
4. Gerd's CV
5. DIQRNG
   - "Heinz Ketchup"
   - "when it absolutely has to be there overnight"
6. DIQKD via VLPC?

Our Approach

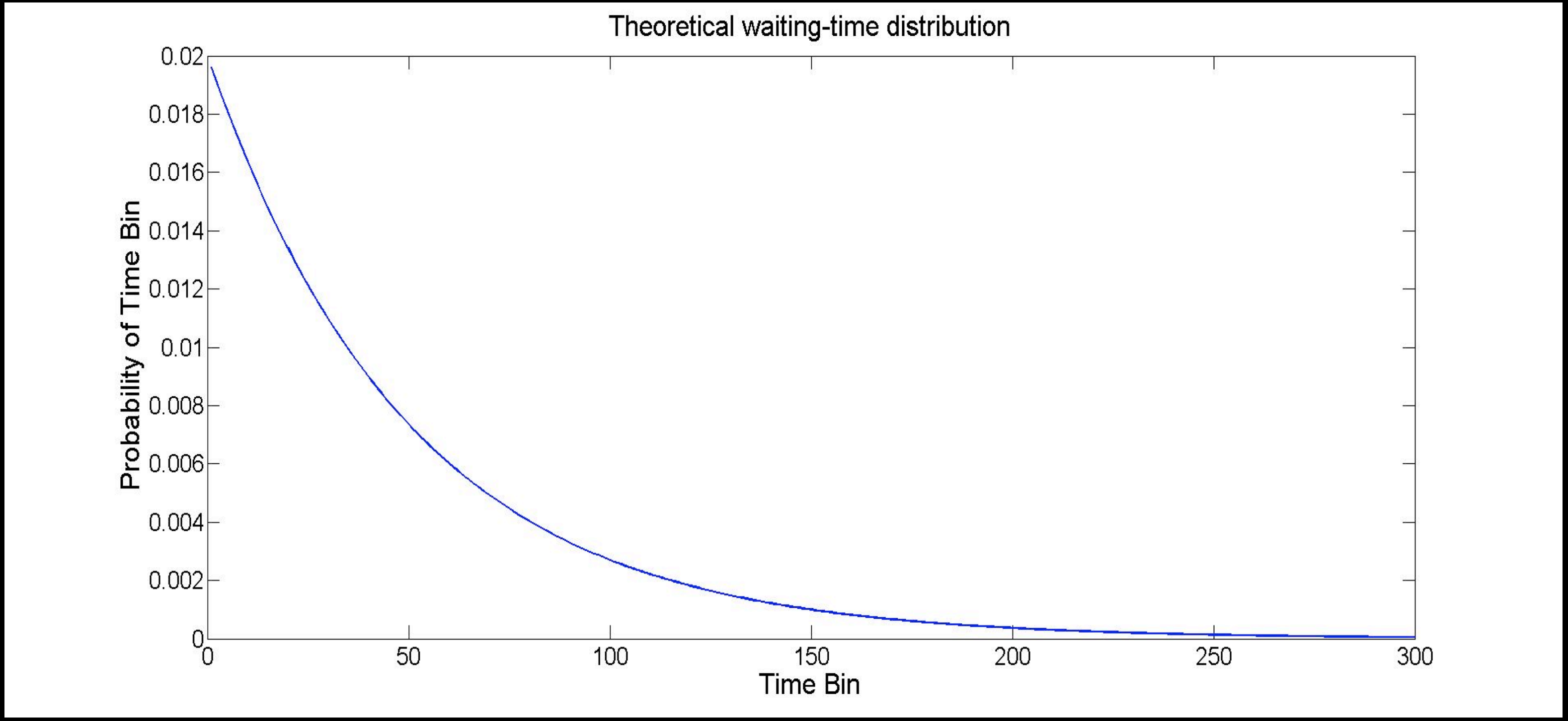
~~[P. Kwiat et al., United States Patent Application Number 20060010182 (2006)~~
N. Lutkenhaus, J. Cohen, H.K. Lo, United States Patent Number 7197523 (2002)]



- Only *one* detector required
- Split time between successive photon detections into "time-bins"; measure inter-photon arrival time
- E.g., 1024 resolvable time-bins gives up to $\log_2 1024$ = 10 bits per detection (8 after hashing)

Theory

- Behavior of incoming photons is a Poisson process, and waiting-time distribution between events behaves as a decaying exponential.
  - Assume simple model: $P(t, \Delta t) = R\, e^{-Rt}\, \Delta t$ (R = average rate)
  - Discrete version: $P(i) = R\, e^{-(R\, \Delta t\, i)}\, \Delta t$ for a given rate, time-bin resolution Δt, and time-bin i.

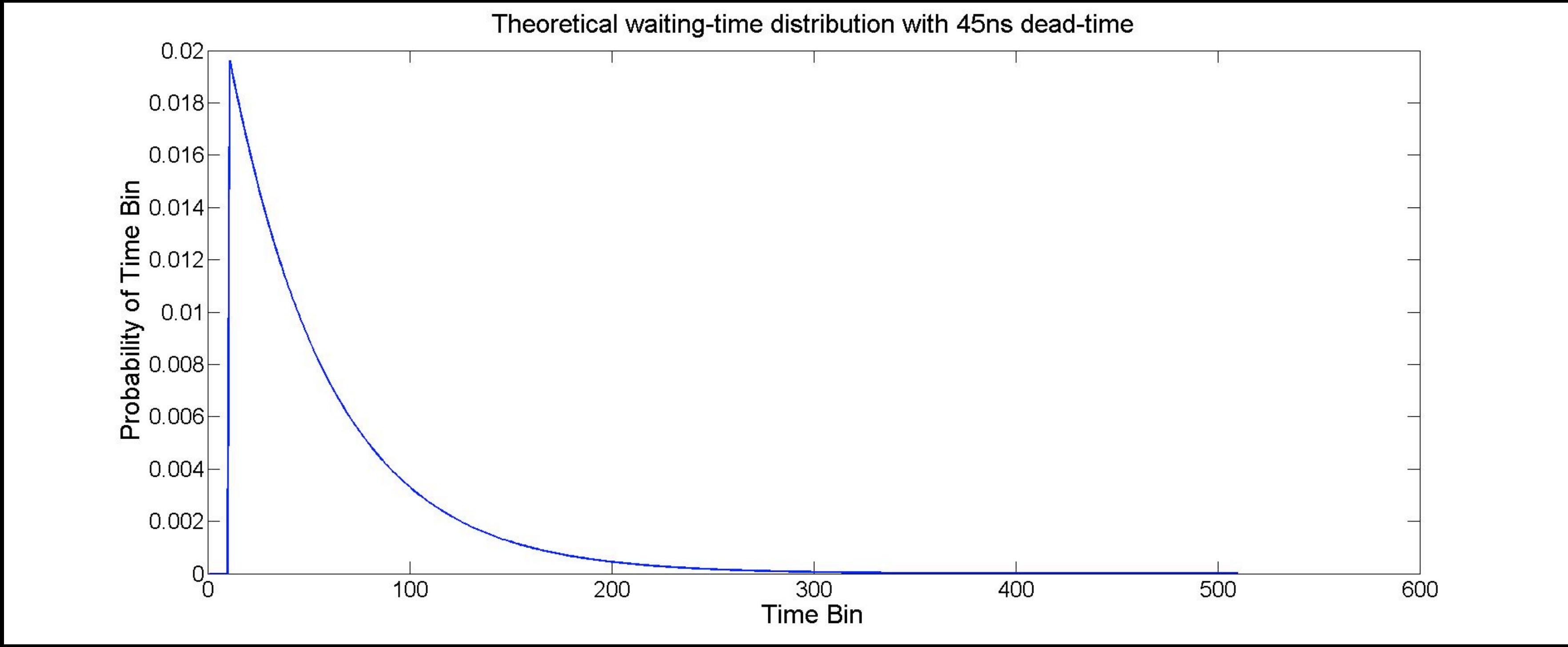


- Not all time bins are equally likely

  $\Rightarrow$ smaller values occur more often $\Rightarrow$ need to *hash (SHA256)*

Theory - Modified

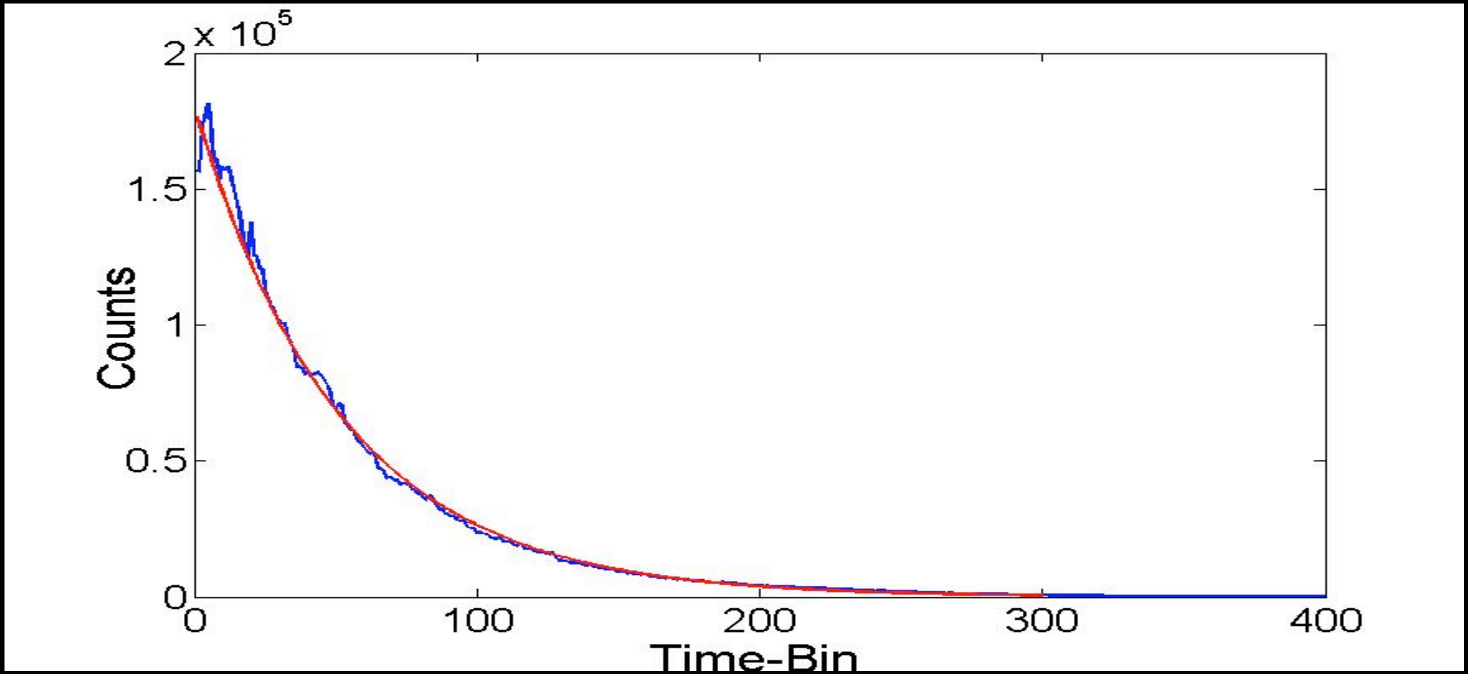
- All real detectors have a deadtime: after a detection event, the detector cannot register another photon for some recovery interval (e.g., 45 ns). *Solution: Ignore initial bins*



- Detectors can also produce “afterpulses”: echoes of a detection (~1% for our detectors). *Solution: Slightly more hashing needed.*

Entropy in our (first) system

R = 11 MHz; Δt = 5 ns



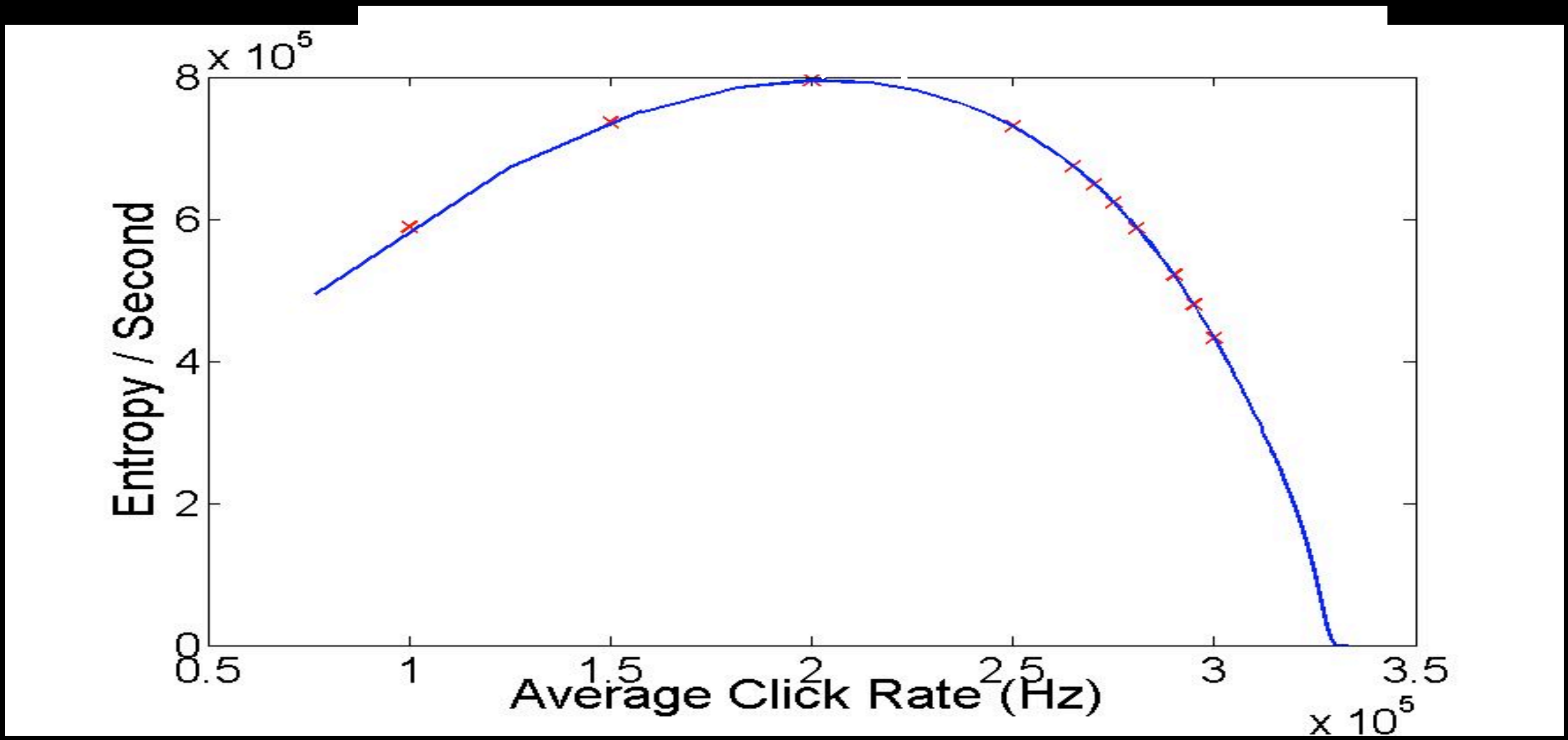
- S_{approx} = 7.08 bits / detection
- S_{actual} = 7.02 bits / detection
- Min-entropy (after hashing) = 0.997 bits/bit
- Passed all FIPS tests, χ-squared, auto-correlation analysis

Final randomness rate: 40 MHz

M. Wayne et al., J. Mod. Opt. 56, 516 (2009)

Entropy Saturation

- As count rate increases, the interval between detections will decrease and the smaller valued time-bins will have more counts, decreasing the entropy per detection.



Attenuation

- Strong random deletion 'washes out' minor correlations due to non-quantum system characteristics or bunching.
- Attenuation achieved using standard neutral density filter (**ESSENTIALLY A VERY REFLECTIVE BS**), as well as a series of crossed polarizers.
- No observable effect on output randomness, i.e., attenuation mechanism does not seem to introduce any correlations.

Hashing

- "Whiten" the raw waiting-time data to give every value approximately same chance of occurring
  - SHA hash functions
    - Performs a series of complex logical bit operations upon the input string
    - Takes a variable-length string and reduces it to a shorter fixed-length string
    - Every output bit depends on every input bit
  - Relatively fast process, compatible with high detection rates

• Approximately 10 extra bits "overhead" of input entropy required to saturate the hash output

• E.g., 266 bits into SHA-256: Attacker guesses 50.1% of bits correctly

- Other 'randomness extractors' could be used, e.g, bitwise XOR, Toeplitz-hashing extractor, Trevisan's extractor

→ "Postprocessing for QRNG: Entropy evaluation and randomness extraction", Ma…HKLo, q-ph 1207.1473v1

→ Use min-entropy, not Shannon

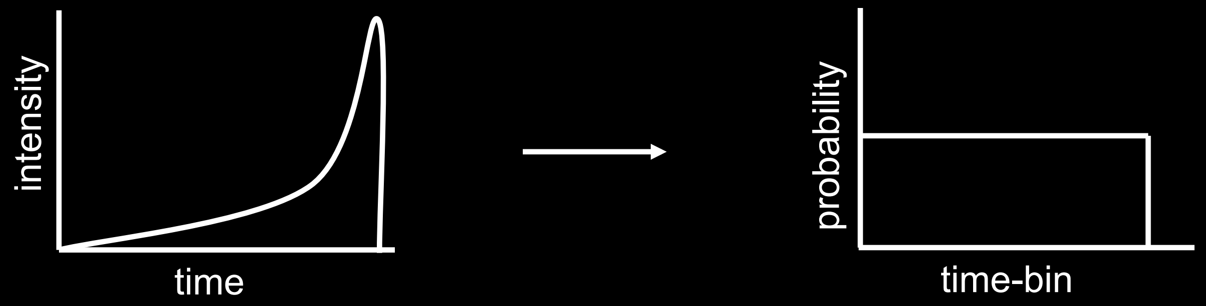
Min-Entropy

$$S_{min} = \log_2(\max\{P_i\})$$

- The *min-entropy* describes the worst-case scenario; what is the maximum amount of information that could be learned by an adversary?
- For our decaying-exponential probability distribution, the min-entropy is always determined by the first time-bin, as it occurs the most often ($P_1 = R\Delta t = 1/\lambda$).
  - Smaller time-bin resolution will cause first bin's contribution to be proportionally smaller, bringing the min-entropy closer to the Shannon Entropy

Shaped Pulses

- By driving the laser diode with a shaped pulse such that every time-bin has an equal probability of occurring, we can increase min-entropy and reduce or eliminate the need for hashing.

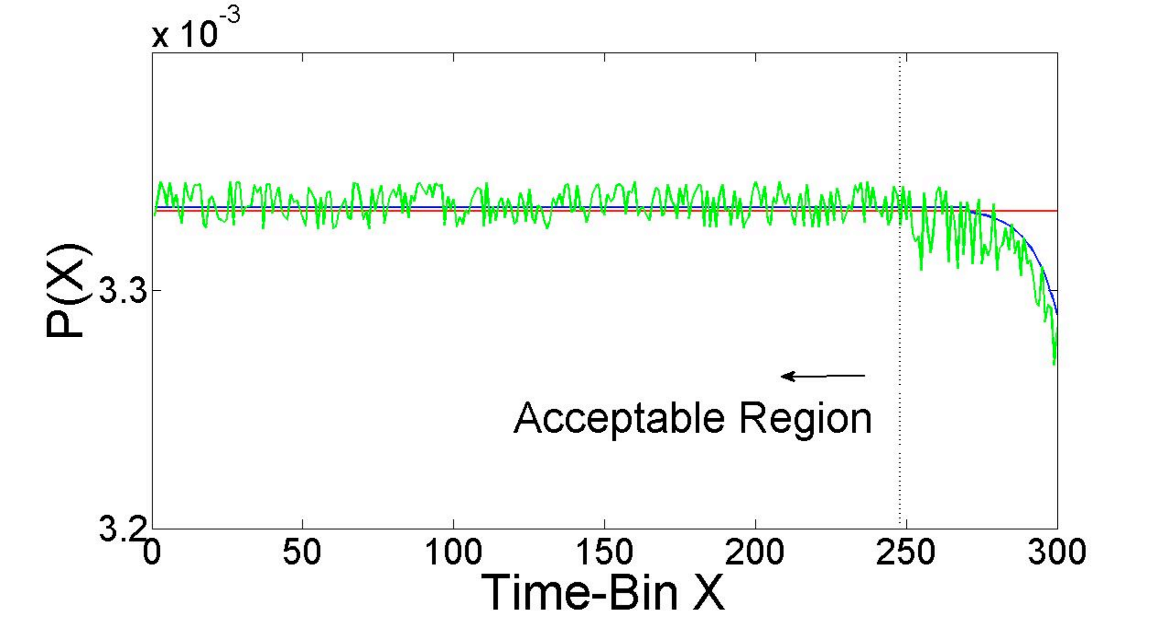


- Optimal pulse shape $\propto$ 1/(t-T)
- For a flat waiting-time distribution, the min-entropy is equal to the Shannon entropy.

ILLINOIS

Shaped Pulse Source

By shaping the current to approximate 1/(T-t), the waiting-time distribution can be tailored to fit the ideal uniform case.



- Resulting waiting-time distribution: min-entropy ~0.90 bits/bit
- Discard counts outside the dotted line: S_{min} → 0.9984 bits/bit.
- Post-hashed data: Passed all NIST RN test suite.
- Final entropy generation rate: S_{min} = 112 Mbit/s

M. Wayne & PGK, Opt. Exp. 18, 9351 (2010)

Outline

1. Motivation
2. Location, location
3. It's all a matter of timing
   - how I know when I have a good idea…
   - post-processed randomness
   - pre-processed randomness
   - a very high-rate version, not
   - a very high-rate version
   - application to QKD
4. Gerd's CV
5. DIQRNG
   - "Heinz Ketchup"
   - "when it absolutely has to be there overnight"
6. DIQKD via VLPC?

Ultra-high speed QRNG, not quite

APPLIED PHYSICS LETTERS **98**, 171105 (2011)

An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements

Michael Wahl,[1,a)] Matthias Leifgen,[2,b)] Michael Berlin,[2] Tino Röhlicke,[1] Hans-Jürgen Rahn,[1] and Oliver Benson[2]
[1]*PicoQuant GmbH, Rudower Chaussee 29, 12489 Berlin, Germany*
[2]*Nano-Optik, Institut für Physik, Humboldt-Universität zu Berlin, 12489 Berlin, Germany*

(Received 22 December 2010; accepted 25 March 2011; published online 26 April 2011)

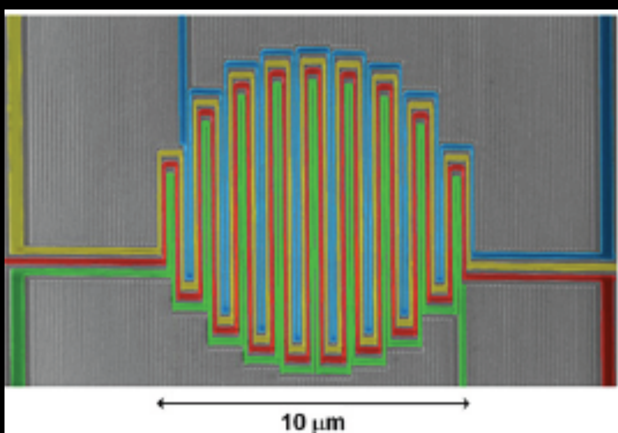
- Claim 16 bit/photon → 150 Mb/s !
- Detector: PMT (Hamammatsu H5783)
  - risetime = 0.8 ns

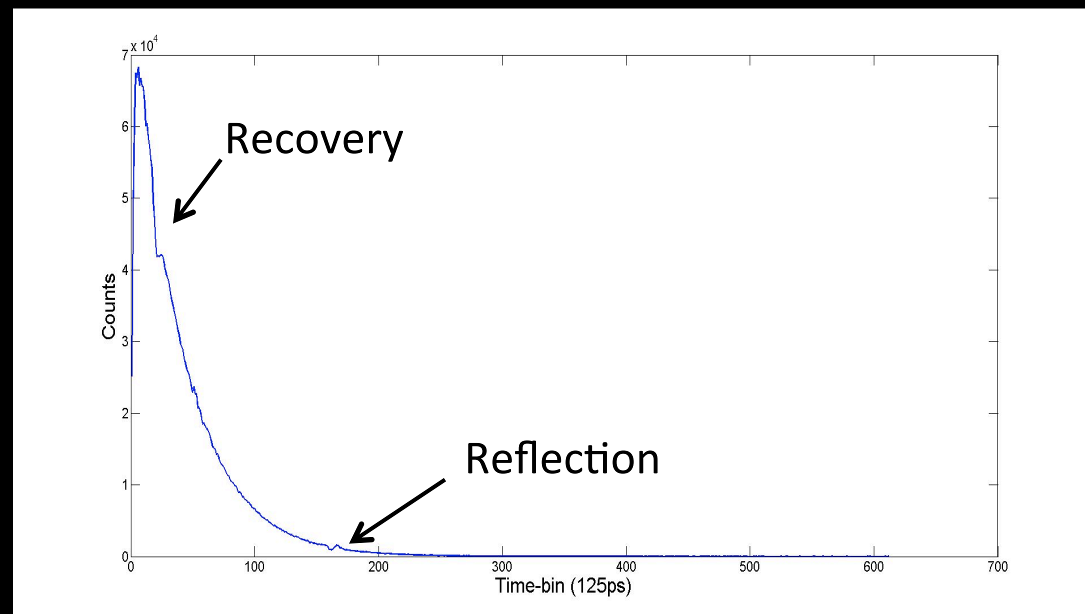
For the analysis of the photon arrival times we use time tagging electronics with a resolution of 1 ps and a throughput of 12.5 Mcps.[6] In order to achieve real-time performance we

- Detector jitter?? 30-150 ps → 10 or 9 bit/photon → ~100Mb/s

(Preliminary) Ultra-high speed QRNG

- Superconducting nanowire detectors allow fast rate of detection→ up to ~400 Mc/s, with <~100 ps jitter
- Xilinx Vertex-6 FPGA + 600MHz Clock + 1:16 DeMux
  → 104-ps bins
- Final entropy rate (after post-processing): **1.86 Gbit/s!**





Eric Dauler
Andrew Kerman
Danna Rosenberg

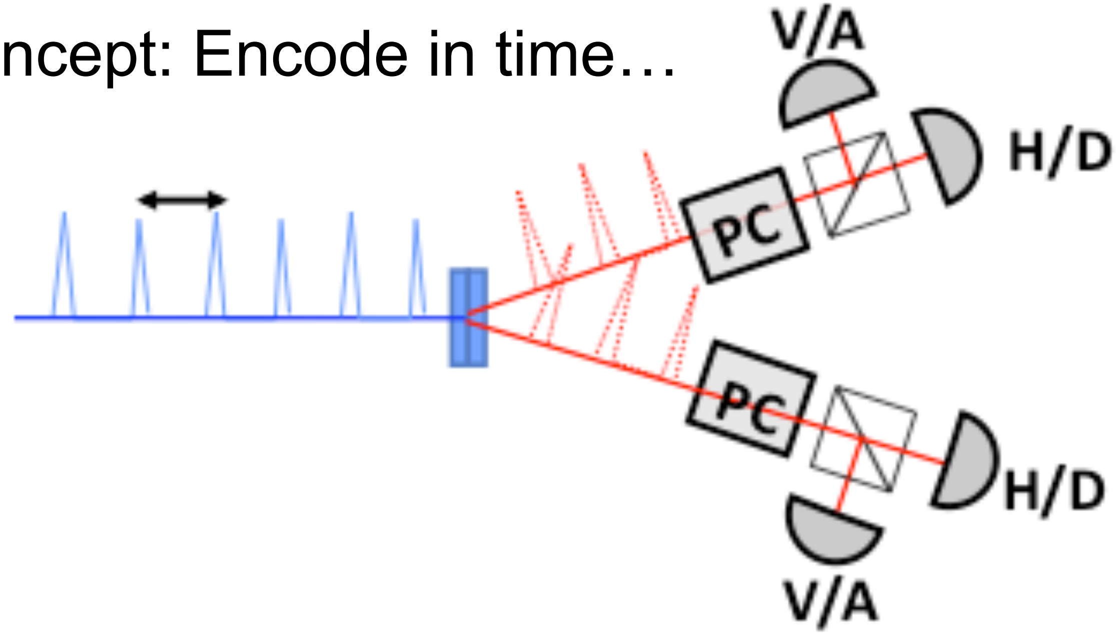
LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Outline

1. Motivation
2. Location, location
3. It's all a matter of timing
   - how I know when I have a good idea…
   - post-processed randomness
   - pre-processed randomness
   - a very high-rate version, not
   - a very high-rate version
   - application to QKD – foreshadowing…
4. Gerd's CV
5. DIQRNG
   - "Heinz Ketchup"
   - "when it absolutely has to be there overnight"
6. DIQKD via VLPC?

Hyper-entanglement Enhanced QKD

Central Concept: Encode in time…



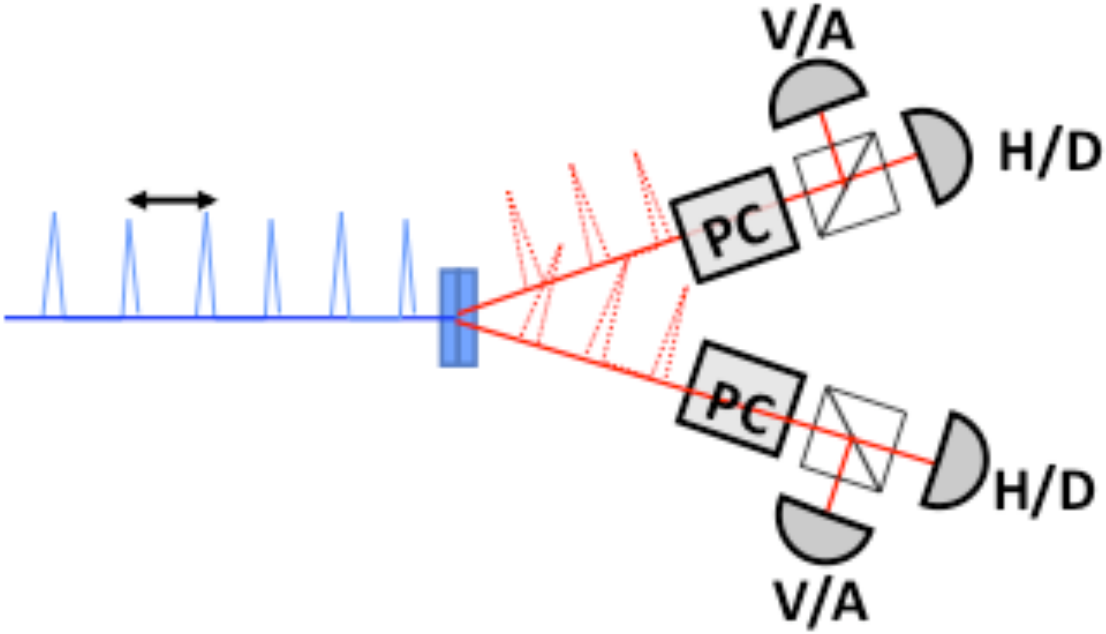
$$|\psi\rangle \propto \left(|t_0 t_0\rangle + |t_1 t_1\rangle + |t_2 t_2\rangle + \ldots + |t_N t_N\rangle\right)$$

Bin spacing: Δt $\quad\Delta t \sim 130$ ps

Code "length": $\sim N\Delta t$

bits/photon $\sim \log_2 N$ $\quad N \sim 1{,}024$ → 10 bit/pair

Central Concept: Encode in time…

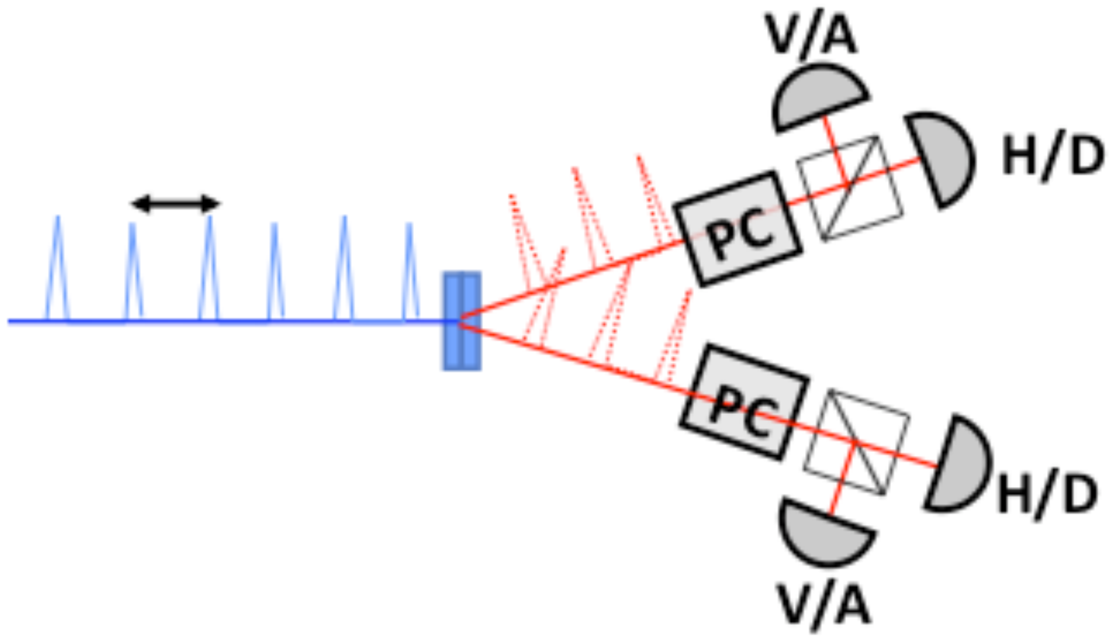


$$|\psi\rangle \propto \left(|t_0 t_0\rangle + |t_1 t_1\rangle + |t_2 t_2\rangle + \ldots + |t_N t_N\rangle\right)$$

*Alice and Bob use which time bin they detect a photon in to generate multiple bits per click.**

*Ali-Khan, Broadbent, Howell, Phys. Rev. Lett. **98**, 060503 (2007)

Central Concept: Encode in time, verify in polarization



$$|\psi\rangle \propto \left(|t_0 t_0\rangle + |t_1 t_1\rangle + |t_2 t_2\rangle + \ldots + |t_N t_N\rangle\right) \otimes \left(|HH\rangle + |VV\rangle\right)$$

- *Alice and Bob use which time bin they detect a photon in to generate multiple bits per click.* Get extra bpp from BB84 with polarization.*
- *They can constantly check for an eavesdropper using the D/A polarization basis (assuming no QND capability for Eve). "Future security"*
- *Perform standard error detection/correction and privacy amp.*
- *Eventually measure in MUB.*

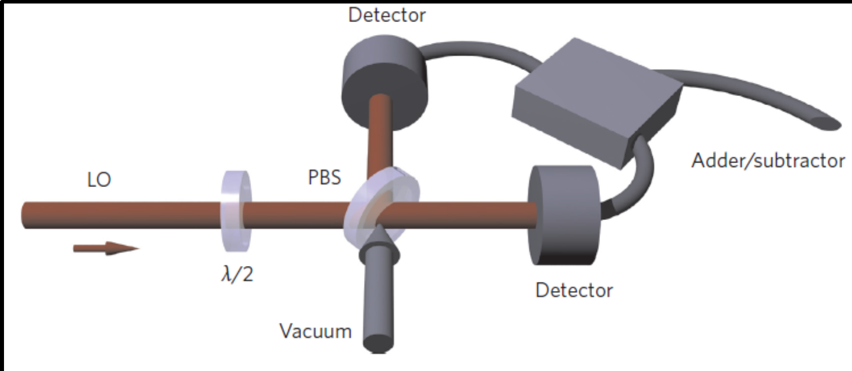
Current status: >5bit/photon, >2 Mb/s   End goal: 10 bpp, >1Gb/s

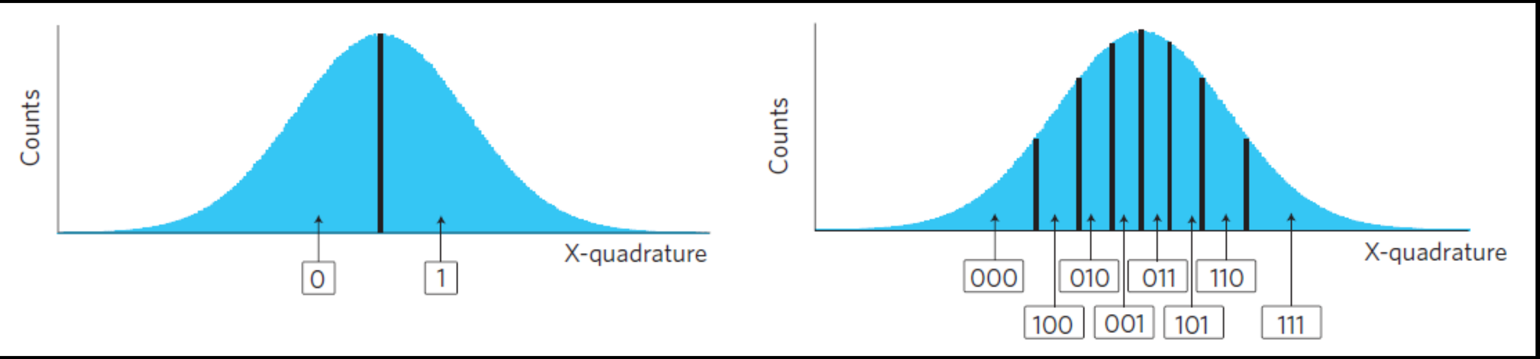
Outline

1. Motivation
2. Location, location
3. It's all a matter of timing
   - how I know when I have a good idea…
   - post-processed randomness
   - pre-processed randomness
   - a very high-rate version, not
   - a very high-rate version
   - application to QKD
4. Gerd's CV
5. DIQRNG
   - "Heinz Ketchup"
   - "when it absolutely has to be there overnight"
6. DIQKD via VLPC?

Continuous Variable QRNG

- uses quantum uncertainty in quadrature amplitudes of the vacuum state as a source of randomness
- uses homodyne detection to measure the position quadrature of the vacuum state
- multiple bits may be extracted by dividing the quadrature into equal probability sections
- numerical hashing methods are required to eliminate classical sources of randomness and experimental biases
- demonstrated rates of 6.5Mbps [1] , 2 Gbps [2]





1. C. Gabriel …G. Leuchs, Nature Photonics **4**, 711-715 (2010).
2. T. Symul, S.M. Assad, and P.K. Lam, Appl. Phys. Lett. **98**, 231103 (2011).

Laser Noise QRNG

F. Xu, …and HK Lo, Opt. Expr. 20, 12366 (2012)

Abstract: A quantum random number generator (QRNG) can generate true randomness by exploiting the fundamental indeterminism of quantum mechanics. Most approaches to QRNG employ single-photon detection technologies and are limited in speed. Here, we experimentally demonstrate an ultrafast QRNG at a rate over 6 Gbits/s based on the quantum phase fluctuations of a laser operating near threshold. Moreover, we consider

noise) of a laser, which yields a speed of 500 Mb/s [18,19]. Instead of directly measuring weak quantum effects, this scheme measures the enhanced quantum noise (amplified spontaneous emissions) and thus can be realized by *conventional photodetectors* at a high-speed and with a

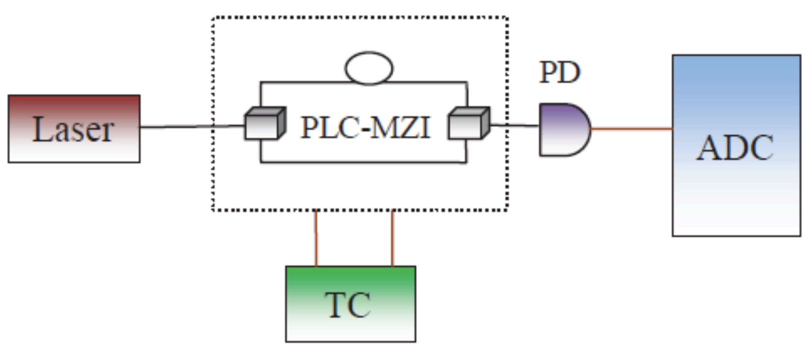


Fig. 1. Experimental setup. Laser, 1550nm cw DFB laser diode (ILX Lightwave); PLC-MZI, planar lightwave circuit Mach-Zehnder interferometer with a 500ps delay difference (manufactured by NTT); TC, temperature controller (PTC 5K from Wavelength Electronics Inc.); PD, 5GHz InGaAs photodetector (Thorlabs SIR5-FC); ADC, 8-bit analog-to-digital convertor inside an oscilloscope (Agilent DSO81204A).

"We finally remark that our implementations of randomness extractors [Toeplitz-hashing Trevisan's extractor] with Matlab on a standard PC are not fast enough for a real-time QRNG."

Don't know what the rate is, but < 6 Gb/s.

ILLINOIS

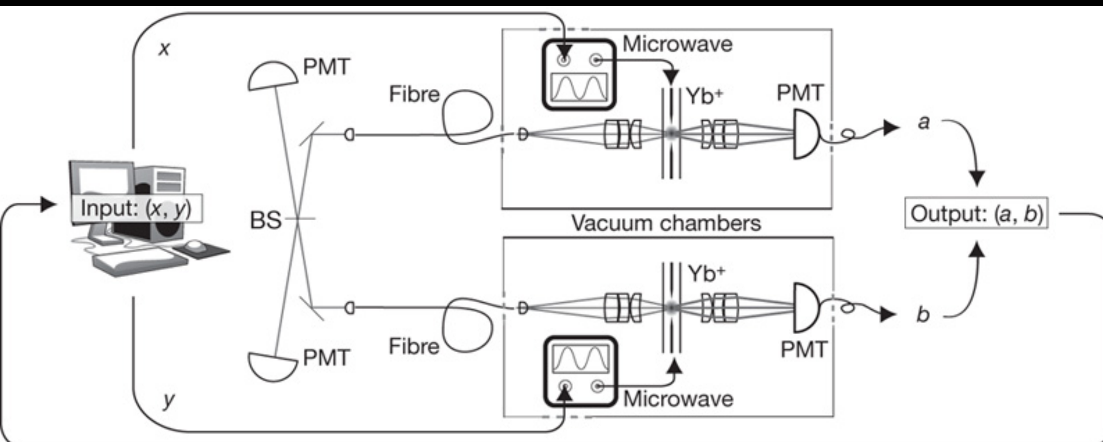
Outline

1. Motivation
2. Location, location
3. It's all a matter of timing
   - how I know when I have a good idea…
   - post-processed randomness
   - pre-processed randomness
   - a very high-rate version, not
   - a very high-rate version
   - application to QKD
4. Gerd's CV
5. DIQRNG
   - "Heinz Ketchup"
   - "when it absolutely has to be there overnight"
6. DIQKD via VLPC?

Advantages of Entanglement (for QKD)

- Automatic ***randomness*** of key
- Longer distances accessible (since Bob knows *when* to look for a photon) [But decoy states…]
- Established methods to verify security of key
- Any leakage of info to other DOF (from source)
  $\Rightarrow$ increased bit error rate (BER)
  [cf 4-diode source of Canary Island experiment…]
- System can be automatically verified (even if "sold" by Eavesdropper!). If you can make a "loophole-free" Bell inequality violation → "device-independent QKD"

Device-Independent QRNG



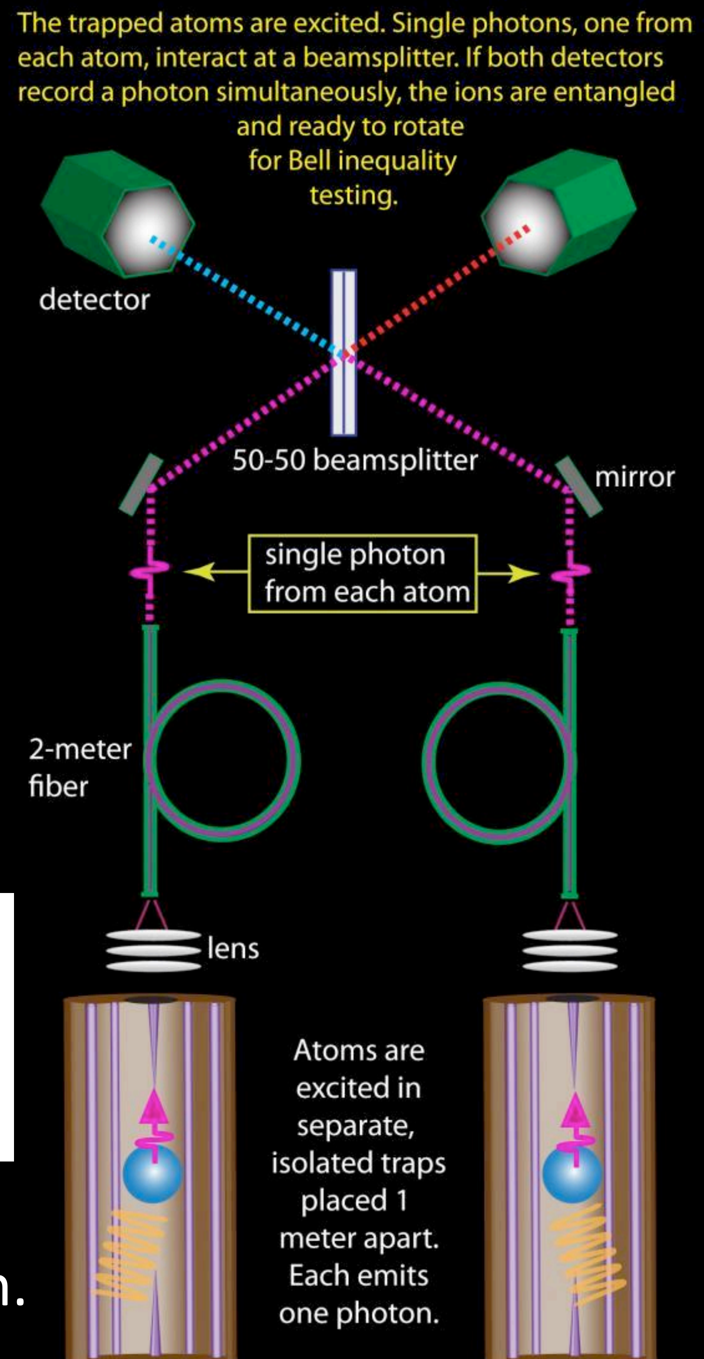
Random numbers certified by Bell's theorem

S. Pironio[1,2,7], A. Acín[3,4,7], S. Massar[1,7], A. Boyer de la Giroday[5], D. N. Matsukevich[6], P. Maunz[6], S. Olmschenk[6], D. Hayes[6], L. Luo[6], T. A. Manning[6] & C. Monroe[6]

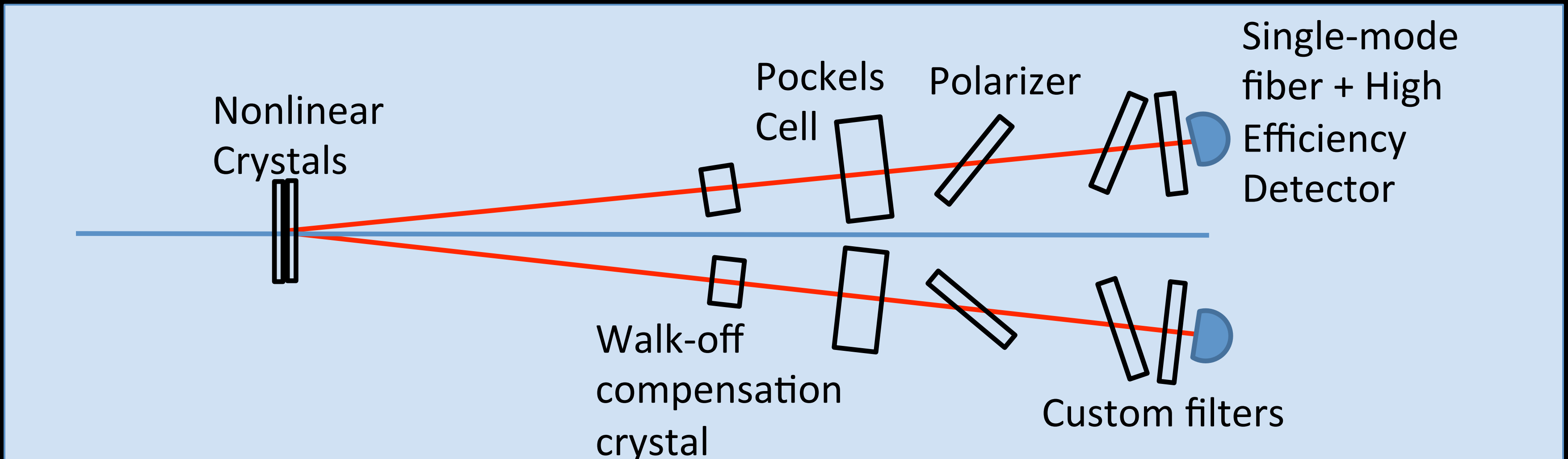
Random, but Not by Chance: A Quantum Random-Number Generator for Encryption, Security

ScienceDaily (Apr. 19, 2010) — Researchers have encrypted communications and other uses, that is cryptographically secure, inherently private and -- most importantly -- certified random by laws of physics.

Pironio, *et al* observed a Bell violation of SCHSH = 2.414 with 3016 events per month. Corresponding to ~45 bits per month.



SPDC Device-Independent QRNG…



Instead of atoms, we can/should be able to violate a Bell inequality using a downconversion source with 81% heralding efficiency (assume detector efficiency of ~92%)

Our source can run at $>10^6$ events per second

Data TODAY: → 2.6 MHz coincidence rate with 4 detectors

→ should have >5MHz coincidence rate with 8 detectors

With 95% efficiency detectors, we will have an estimated ~30 kb/s. (10^9 improvement…)

Detection Loophole in tests of Nonlocality

Clauser-Horne Inequality

Phys. Rev. D 10, 526 (1974)

$$C(A_1, B_1) + C(A_1, B_2) + C(A_2, B_2) - C(A_2, B_2)$$
$$\leq S(A_1) + S(B_1)$$

Works with non-maximally entangled state:

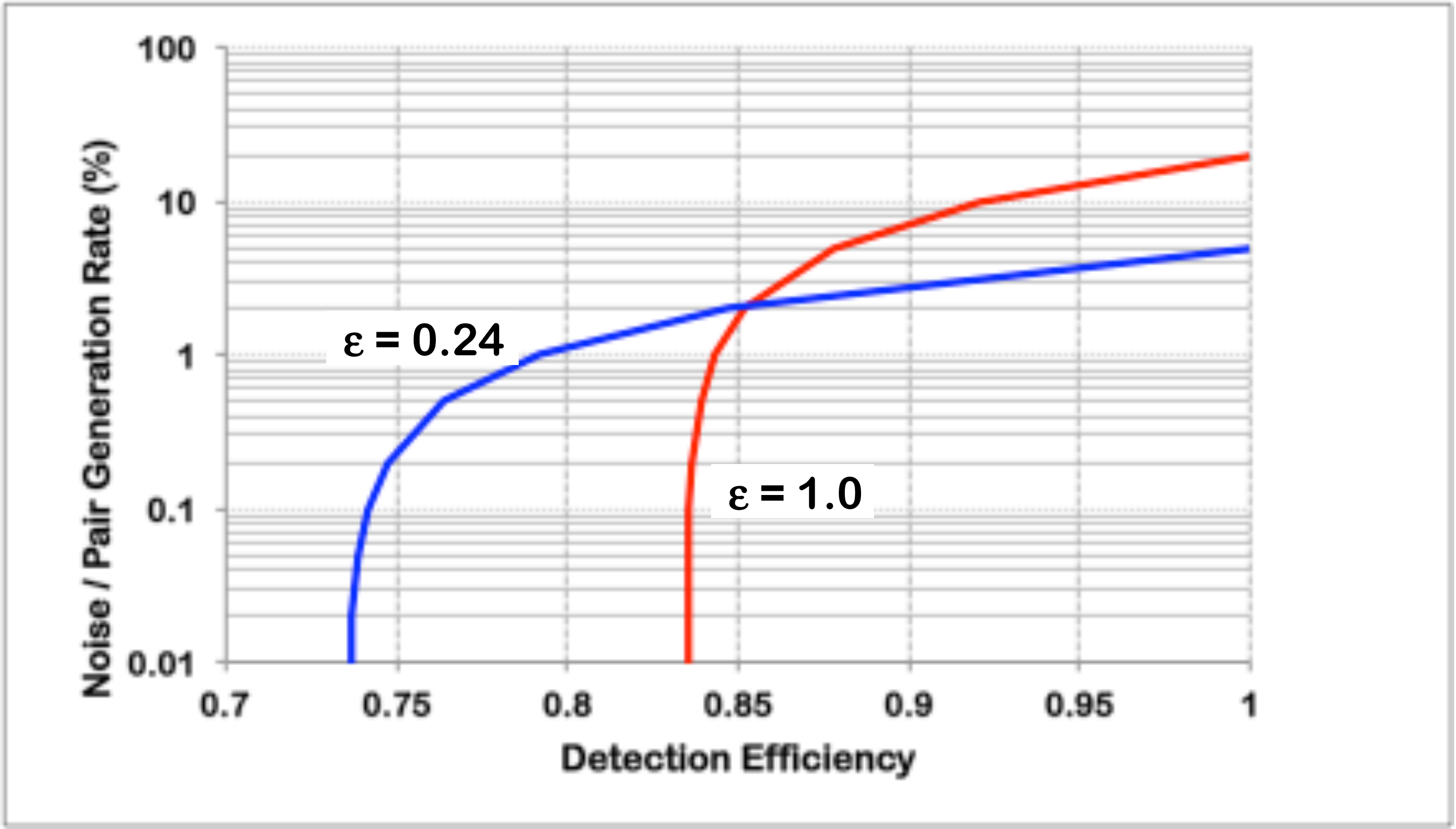
$|HH\rangle + \varepsilon |VV\rangle$ (Eberhard, PRA 47, 747 (1993))

→ choose A_1 and B_1 to minimize singles contribution

→ choose A_2 and B_2 to enable violation

→ reduce required detector efficiency, 83% → 67%, *assuming no background or analyzer crosstalk, and perfect quantum state.*

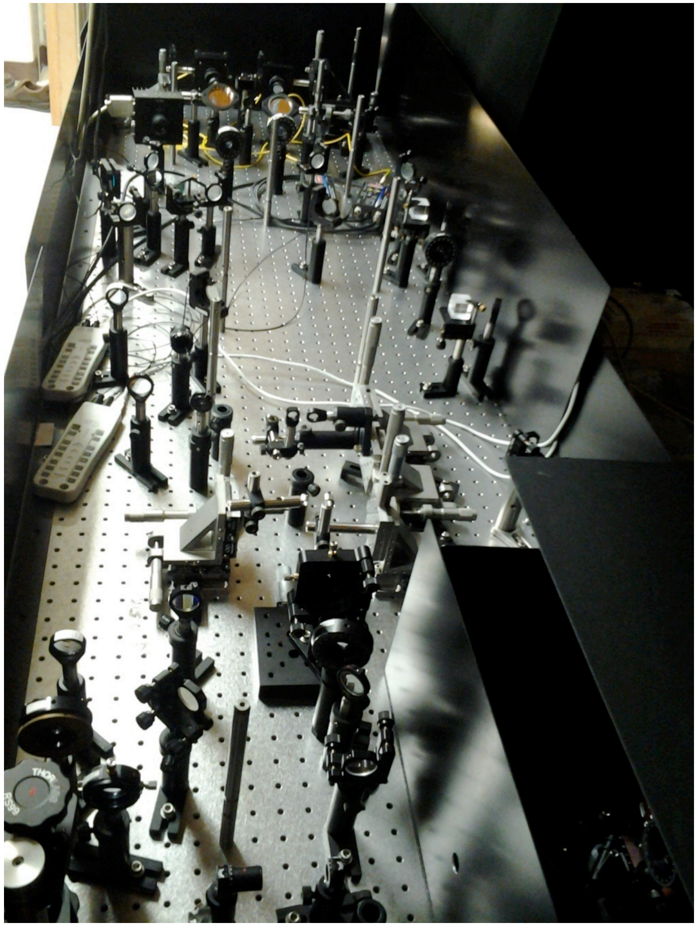
Allowable noise vs efficiency, with measured crosstalk, for measured εHH+VV states

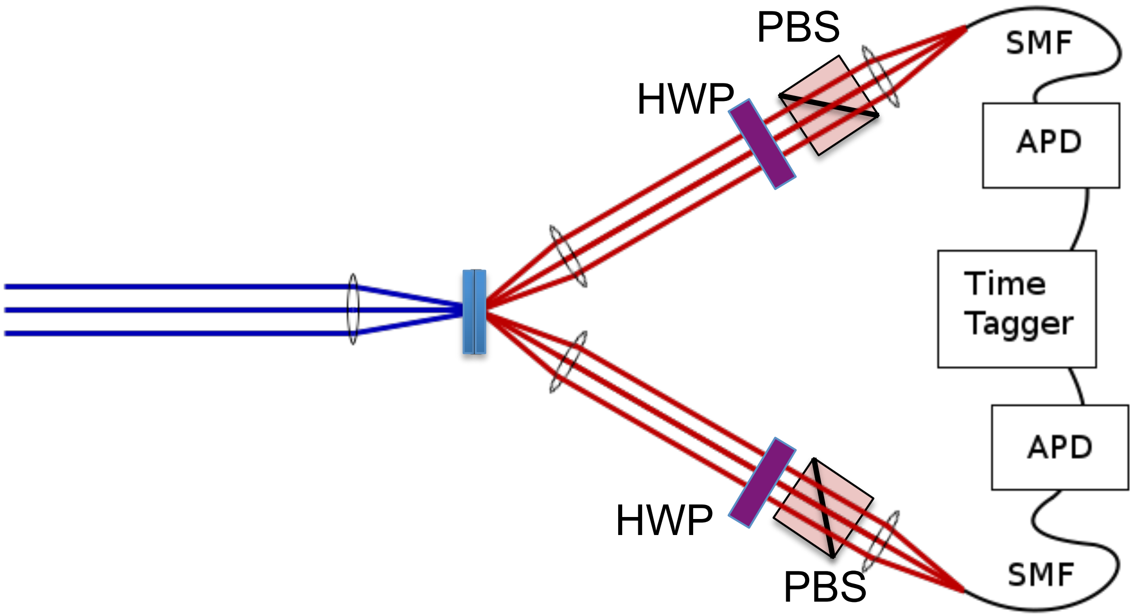


→ for our measured noise (0.1%), need $\eta > 74\%$

→ how are we doing…

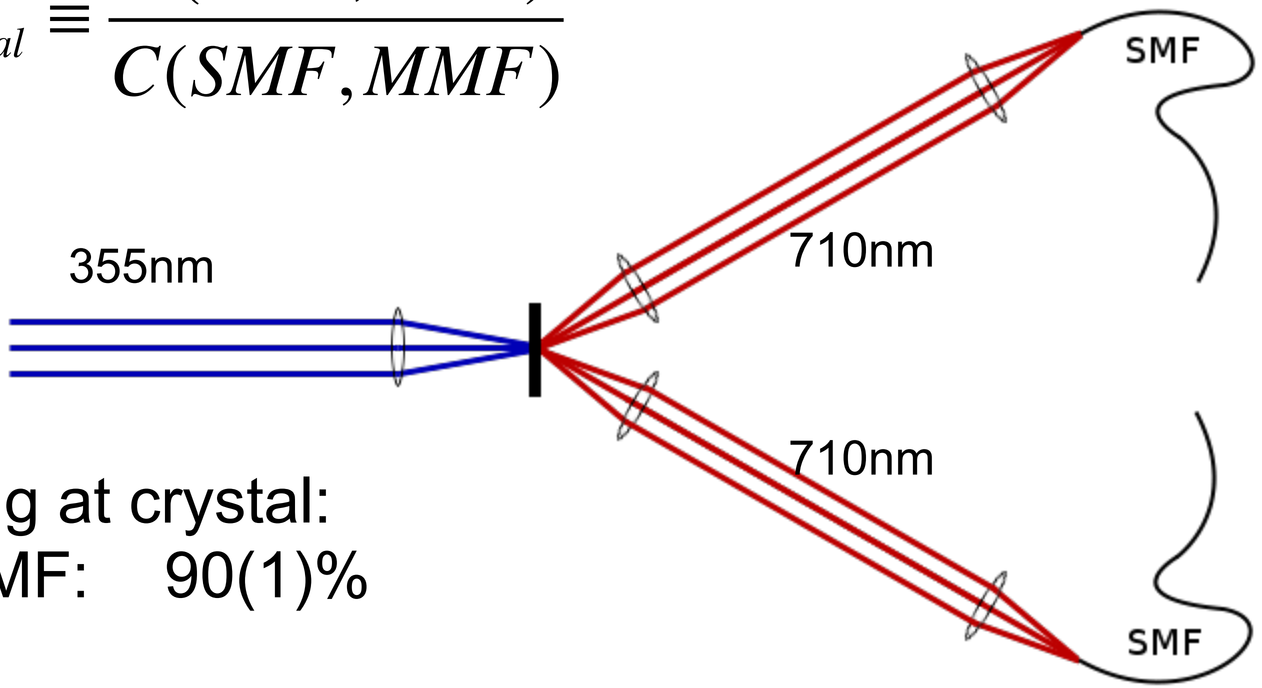
- 4 W, 120 MHz, 5 ps, 355 nm
- BiBO double-crystal setup





Spatial Heralding Efficiency

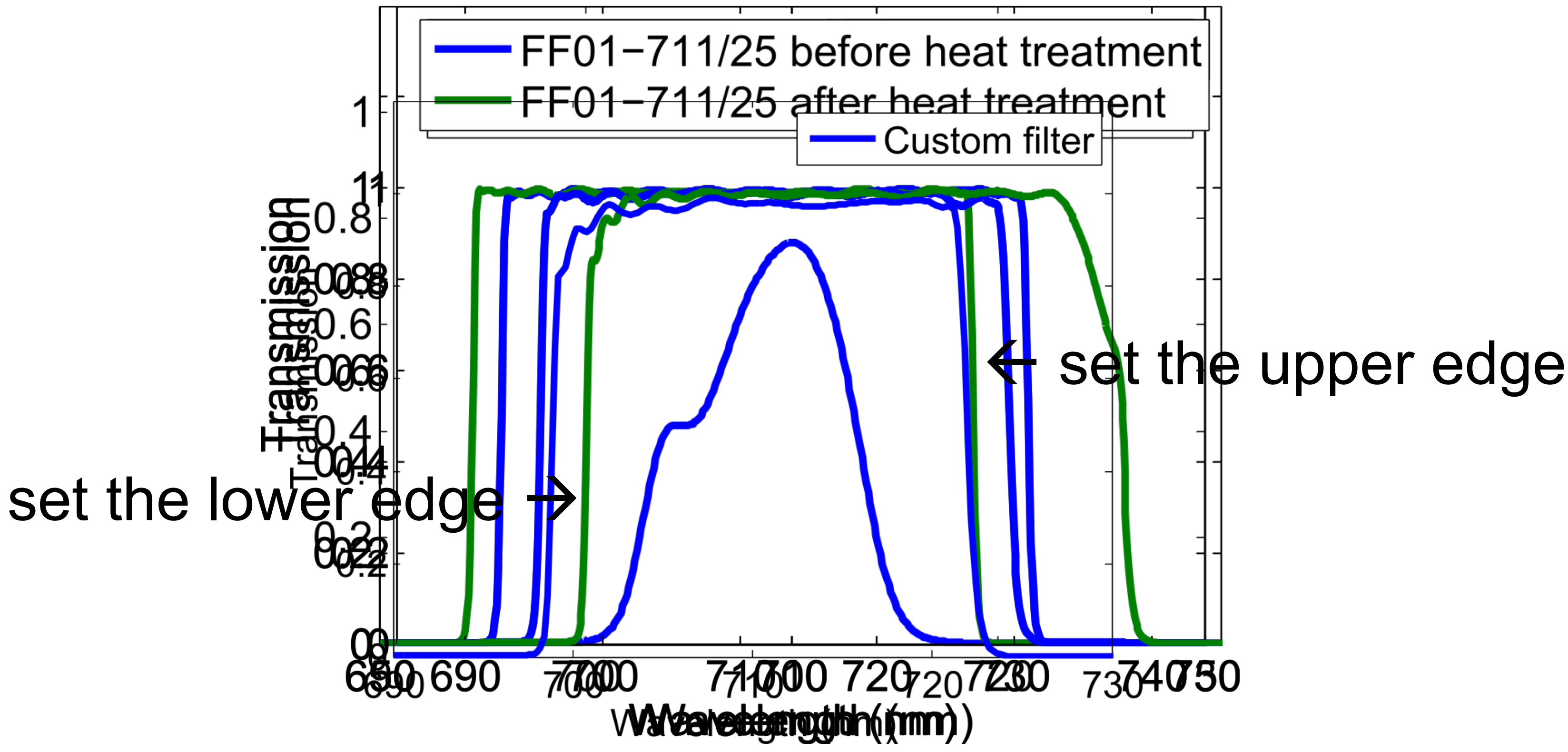
$$\eta_{spatial} \equiv \frac{C(SMF,SMF)}{C(SMF,MMF)}$$



Focusing at crystal:
SMF-SMF: 90(1)%

R. Bennink, Phys. Rev. A **81**, 053805 (2010).

Spectral Heralding Efficiency



355 nm → 710 nm + 710 nm

Heralding efficiency: 50% → 95%

Results

Predicted:

$\eta = \eta_{spatial} * \eta_{spectral} * \eta_{optics} * \eta_{detector}$

$= 0.9 * 0.95 * 0.9 * 0.65$

$= 0.50$

0.94 (AR-coated fibers)

0.95 (TES)

Measured (C/S): $\eta = 0.507(5)$ [with one crystal]

0.53

0.80

Exceeds required 75%!

Record two-way heralding

BUT $\eta_{spatial}$ drops to ~0.6 [for two crystals]

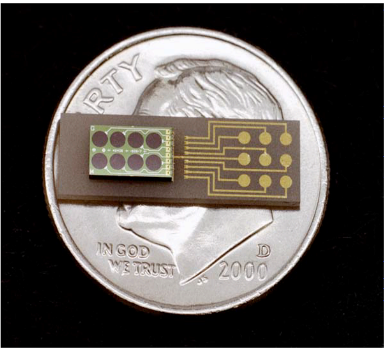
→ $\eta = 0.32$

→ need polarization-dependent focusing/collection

Preliminary data from yesterday → now up to $\eta_{2\ xtal} = 45\%$

(Other) High-Efficiency Single-Photon Detectors

- *Solid State Photomultipliers (SSPMs)*
- *Visible Light Photon Counters (VLPCs)*



VLPCs

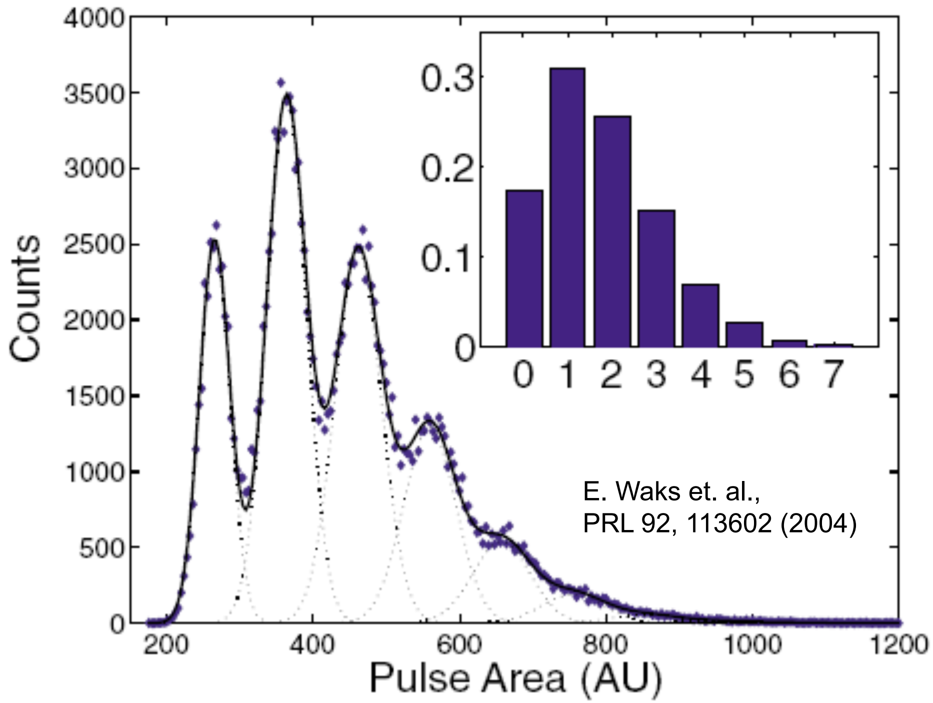
SSPMs

- *SSPMs originally developed by Rockwell for IR military applications*
- *VLPCs are their IR-desensitized successors (used by FermiLab)*
- *High measured efficiency (~88%)*
- *Very high inferred efficiency (~95%)*
- *Multi-photon detection capability*

  [Takeuchi et al. APL 74, 1063 (1999)]
- *~Fast (~300ps jitter)*
- *~6K operation*
- *"Big" – 1 mm → good for turbulent spatial modes*

Photon Number Resolving Capability

- VLPC can resolve photon number
  - Localized avalanche allows multiple parallel detection events
  - Low multiplication noise (low gain dispersion)
  - Pulse height proportional to incident photon number
  - Photon number resolution of up to ~20 photons



PNR useful for entanglement sources or heralded single-photon sources – determine there aren't two pairs.

Outline

1. Motivation
2. Location, location
3. It’s all a matter of timing
   - how I know when I have a good idea…
   - post-processed randomness
   - pre-processed randomness
   - a very high-rate version, not
   - a very high-rate version
   - application to QKD
4. Gerd’s CV
5. DIQRNG
   - “Heinz Ketchup”
   - “when it absolutely has to be there overnight”
6. DIQKD via VLPC?

Summary

1. Motivation
2. Location, location
3. It's all a matter of timing
   - how I know when I have a good idea…
   - post-processed randomness
   - pre-processed randomness
   - a very high-rate version, not
   - a very high-rate version
   - application to QKD
4. Gerd's CV
5. DIQRNG
   - "Heinz Ketchup"
   - "when it absolutely has to be there overnight"
6. DIQKD via VLPC?

Questions?

You wouldn't attack someone holding a puppy would you?