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
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…
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
  – 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)
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

- 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)

---

Time-based RNG

Theory

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

![Theoretical waiting-time distribution with 45ns dead-time](image)

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

\[ R = 11 \text{ MHz}; \ \Delta t = 5 \text{ ns} \]

- \( S_{\text{approx}} = 7.08 \) bits / detection
- \( S_{\text{actual}} = 7.02 \) bits / detection
- Min-entropy (after hashing) = 0.997 bits/bit
- Passed all FIPS tests, \( \chi^2 \)-squared, auto-correlation analysis


Final randomness rate: 40 MHz
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

\[ S_{\text{min}} = \log_2(\max\{P_i\}) \]

- The \textit{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.
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 $\sim 0.90$ bits/bit
- Discard counts outside the dotted line: $S_{\text{min}} \to 0.9984$ bits/bit.
- Post-hashed data: Passed all NIST RN test suite.
- Final entropy generation rate: $S_{\text{min}} = 112$ Mbit/s

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

**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. 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
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?
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: \( \Delta t \) \hspace{1cm} \Delta t \sim 130 \text{ ps} \\

Code “length”: \( \sim N\Delta t \)

\# bits/photon \sim \log_2 N \hspace{1cm} N \sim 1,024 \rightarrow 10 \text{ bit/pair}
Central Concept: Encode in time...

\[ |\psi\rangle \propto (|t_0 t_0\rangle + |t_1 t_1\rangle + |t_2 t_2\rangle + \ldots + |t_N t_N\rangle) \]

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

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
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]

Laser Noise QRNG

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 (amplified spontaneous emissions) 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 and thus can be realized by conventional photodetectors at a high-speed and with a rate < 6 Gb/s.

“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.
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) ⇒ 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”
Pironio, et al. observed a Bell violation of $S_{CHSH} = 2.414$ with 3016 events per month. Corresponding to $\sim 45$ bits per month.
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:  \( \rightarrow \) 2.6 MHz coincidence rate with 4 detectors
\( \rightarrow \) 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

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

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% \( \rightarrow \) 67%, assuming no background or analyzer crosstalk, and perfect quantum state.
Allowable noise vs efficiency, with measured crosstalk, for measured $\epsilon_{\text{HH}+\text{VV}}$ states

$\epsilon = 0.24$

$\epsilon = 1.0$

→ 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

\[ \eta_{\text{spatial}} \equiv \frac{C(\text{SMF,SMF})}{C(\text{SMF,MMF})} \]

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

Spectral Heralding Efficiency

355 nm → 710 nm + 710 nm
Heralding efficiency: 50% → 95%
Results

Predicted:

\[ \eta = \eta_{\text{spatial}} \times \eta_{\text{spectral}} \times \eta_{\text{optics}} \times \eta_{\text{detector}} \]

\[ = 0.9 \times 0.95 \times 0.9 \times 0.65 \]

\[ = 0.50 \]

Measured (C/S):

\[ \eta = 0.507(5) \] [with one crystal]

Record two-way heralding

BUT \( \eta_{\text{spatial}} \) drops to \(~0.6\) [for two crystals]

\[ \Rightarrow \eta = 0.32 \]

\[ \Rightarrow \text{need polarization-dependent focusing/collection} \]

Preliminary data from yesterday \( \Rightarrow \) now up to \( \eta_{2\text{xtal}} = 45\% \)

0.94 (AR-coated fibers)

0.95 (TES)

0.53

0.80

Exceeds required 75%!
High-Efficiency Single-Photon Detectors

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

- 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

E. Waks et al., PRL 92, 113602 (2004)

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