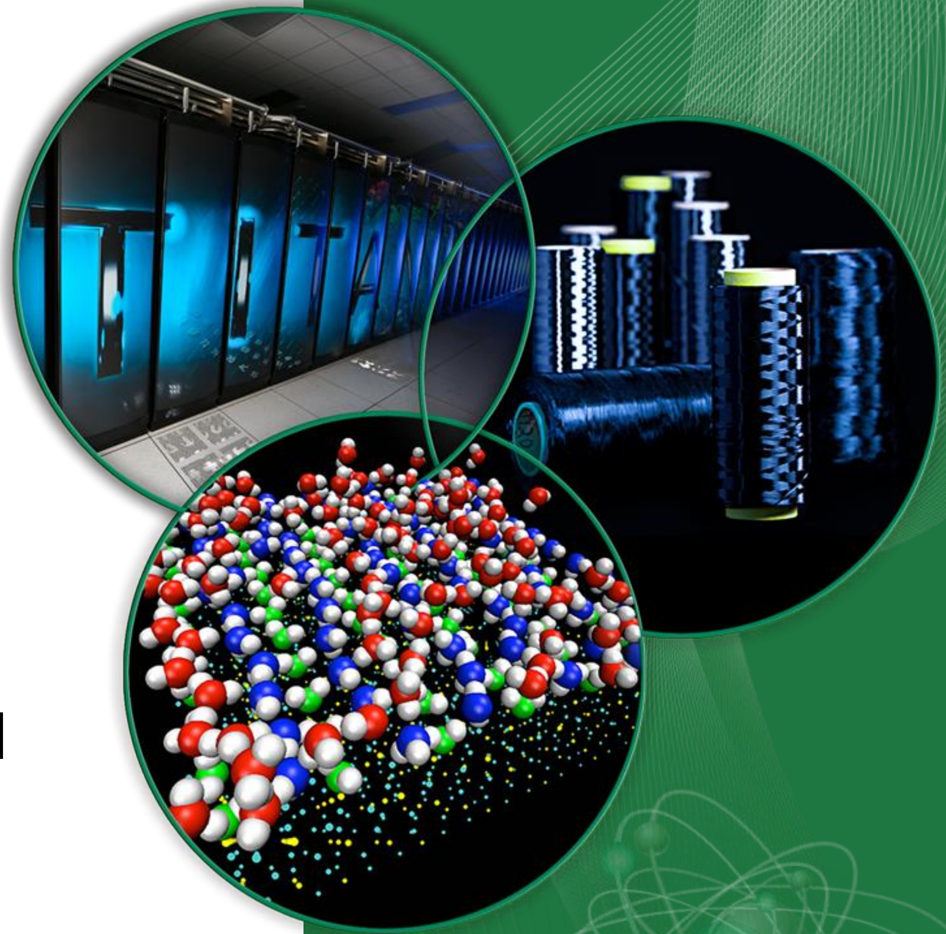
Integrated self-correcting true random number generators



Principal Investigator: Raphael Pooser

Lead Division: CSED

Co-Investigator: Ben Lawrie

Motivation

- Random number generators are critical to vast number of important applications: HPC, national security, health data security, the grid security, and consumer authentication products.
- Current pseudorandom number generators (PRNG) have shortcomings:
  - Inaccuracies arise from intrinsic periodicity (bias)
  - Multifactor authentication: ***2011 RSA hack***
    - **2015 OPM clearance hack preventable with stronger randomness in authentication protocols**
  - Encryption: PRNG cited as one of the most vulnerable parts of the cryptography chain
    - The Dual_EC_DRBG random number generator used by RSA ***included a back door that rendered SSL as clear text***.

State of the art

TRNGs are based on quantum superposition of photons on a beam splitter. The beam splitter samples the photon position distribution like a 50/50 coin toss, but suffer from shortcomings.

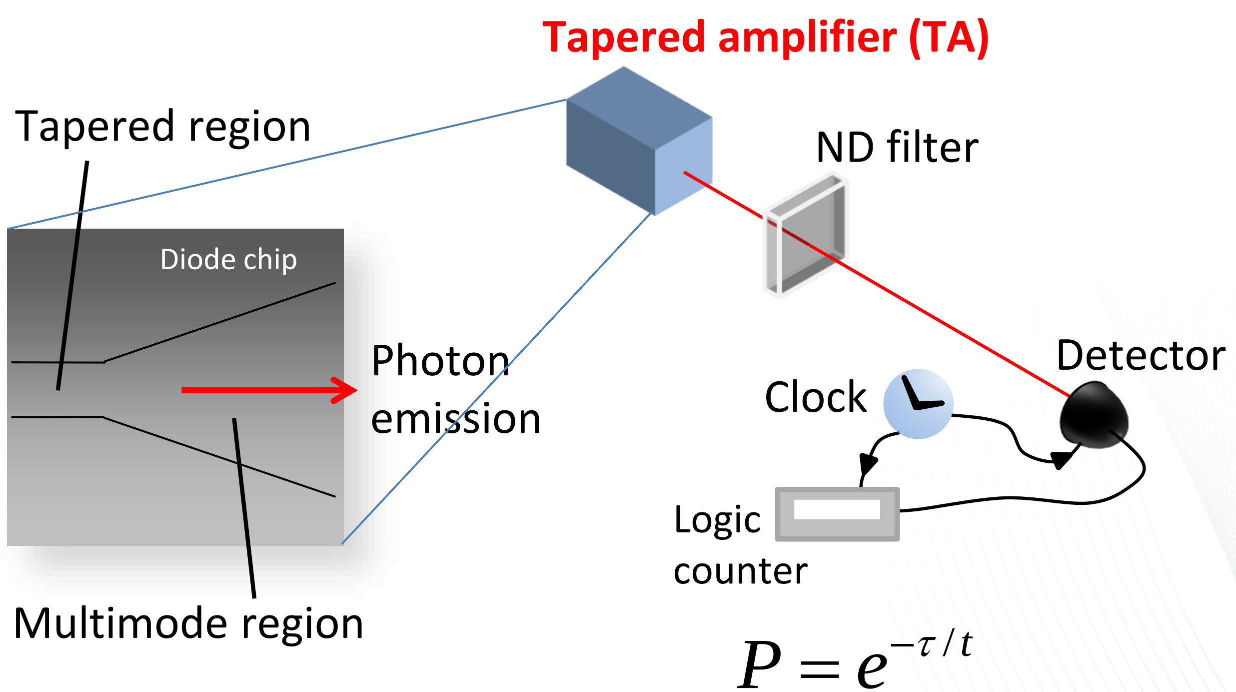
- Expensive (>$1.5-20k)
- Low bandwidth (4Mbps)
- Periodicity (bias) still possible in depending on implementation
  - Mathematical extractors must be used to extract randomness

ORNL QRNGs

Use quantum random number generators

- Such as arrival time distribution of photons

Random numbers are derived from quantum physics, not deterministic events or calculations

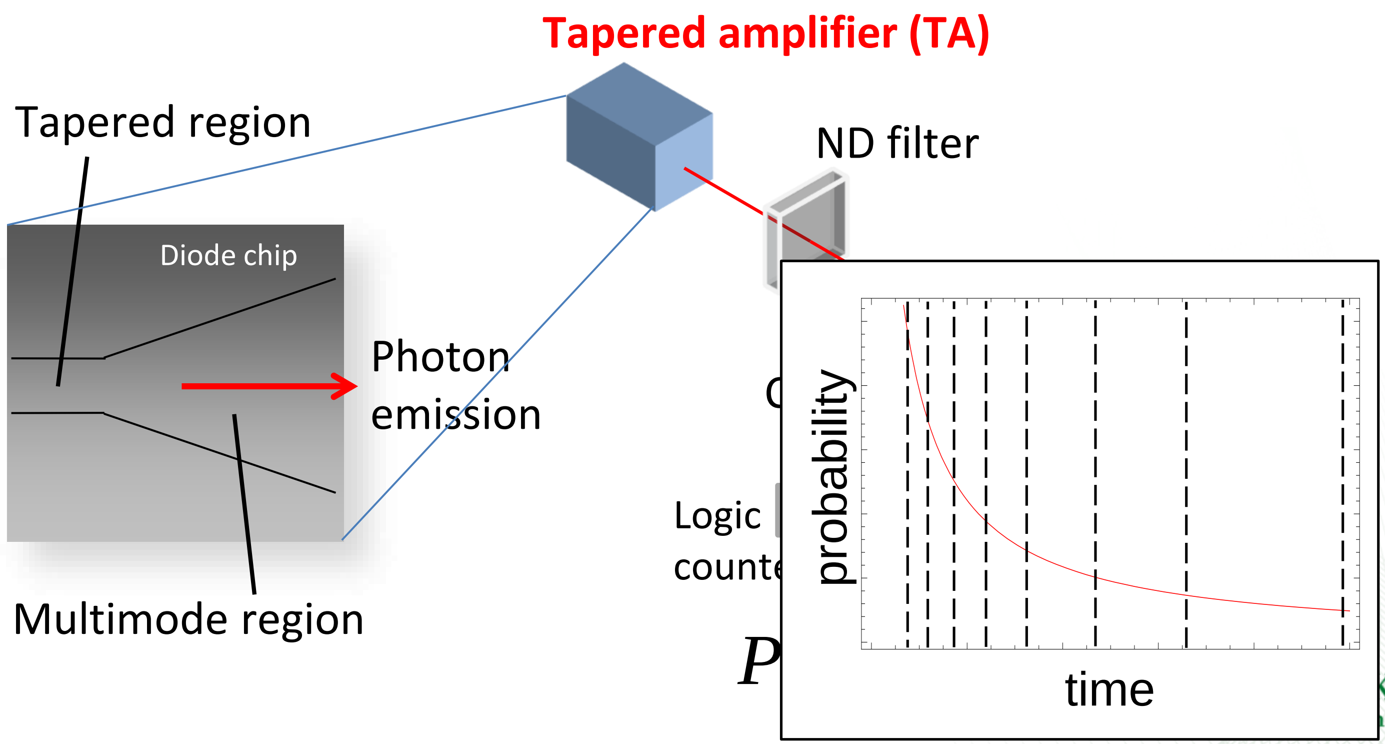


ORNL QRNGs

Use quantum random number generators

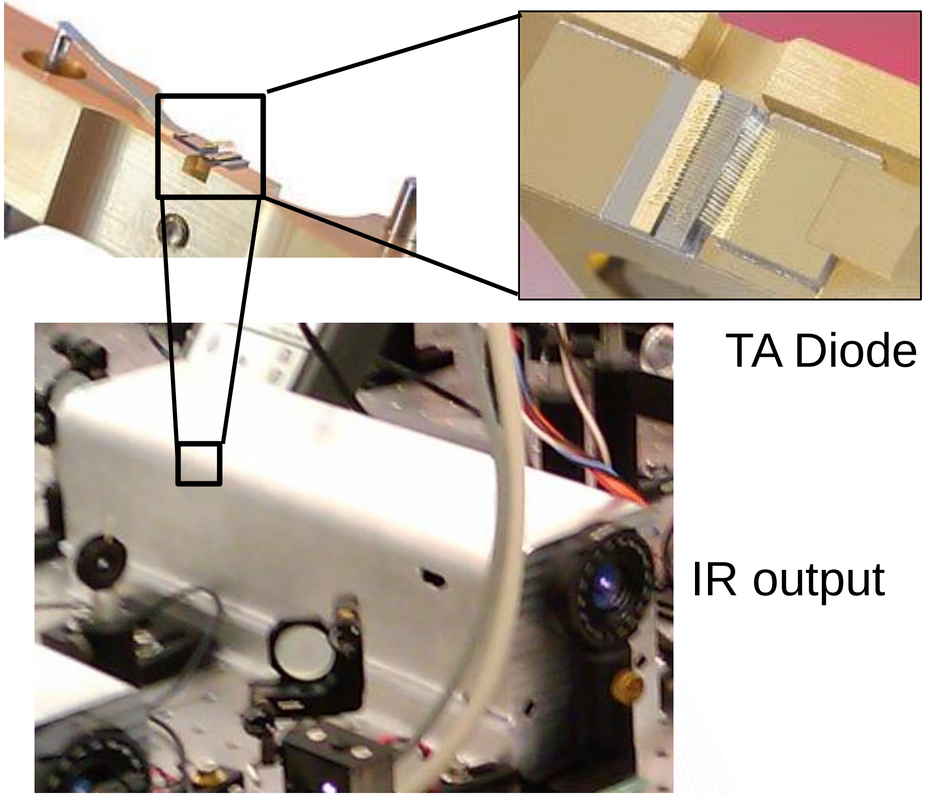
- Such as arrival time distribution of photons

Random numbers are derived from quantum physics, not deterministic events or calculations



ORNL QRNGs

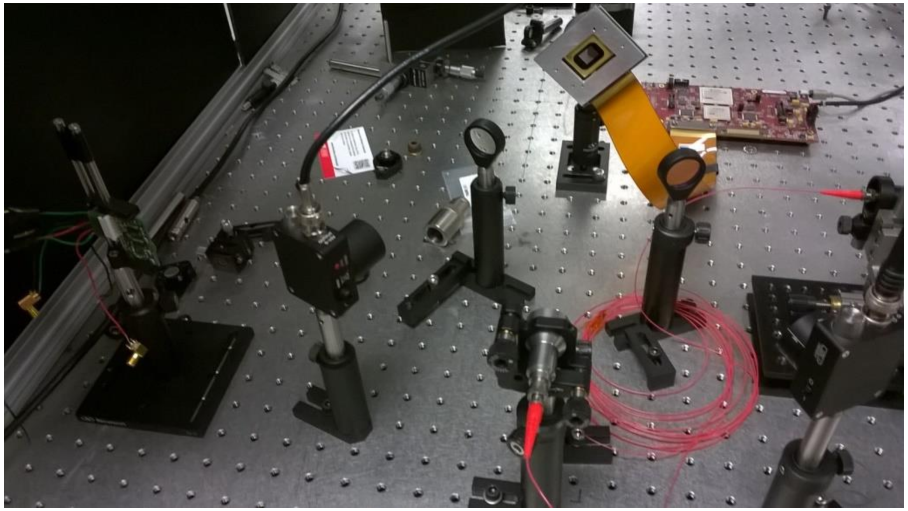
- Low noise high current source supplies current to TA
- Modulation input allows current pulse shaping
- Cooling to 18 C by heat sinking diode mount to Peltier, temperature lock loop
- Diode is off the shelf component
- Diode mount, heat sink, connectors, optics custom built

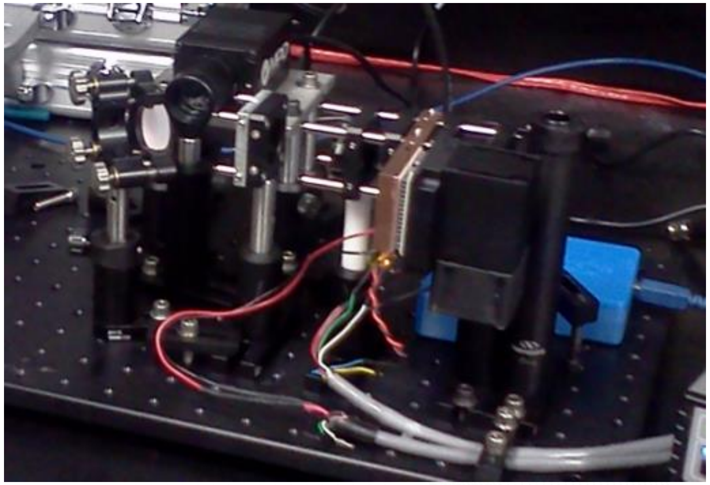


Example custom built TA

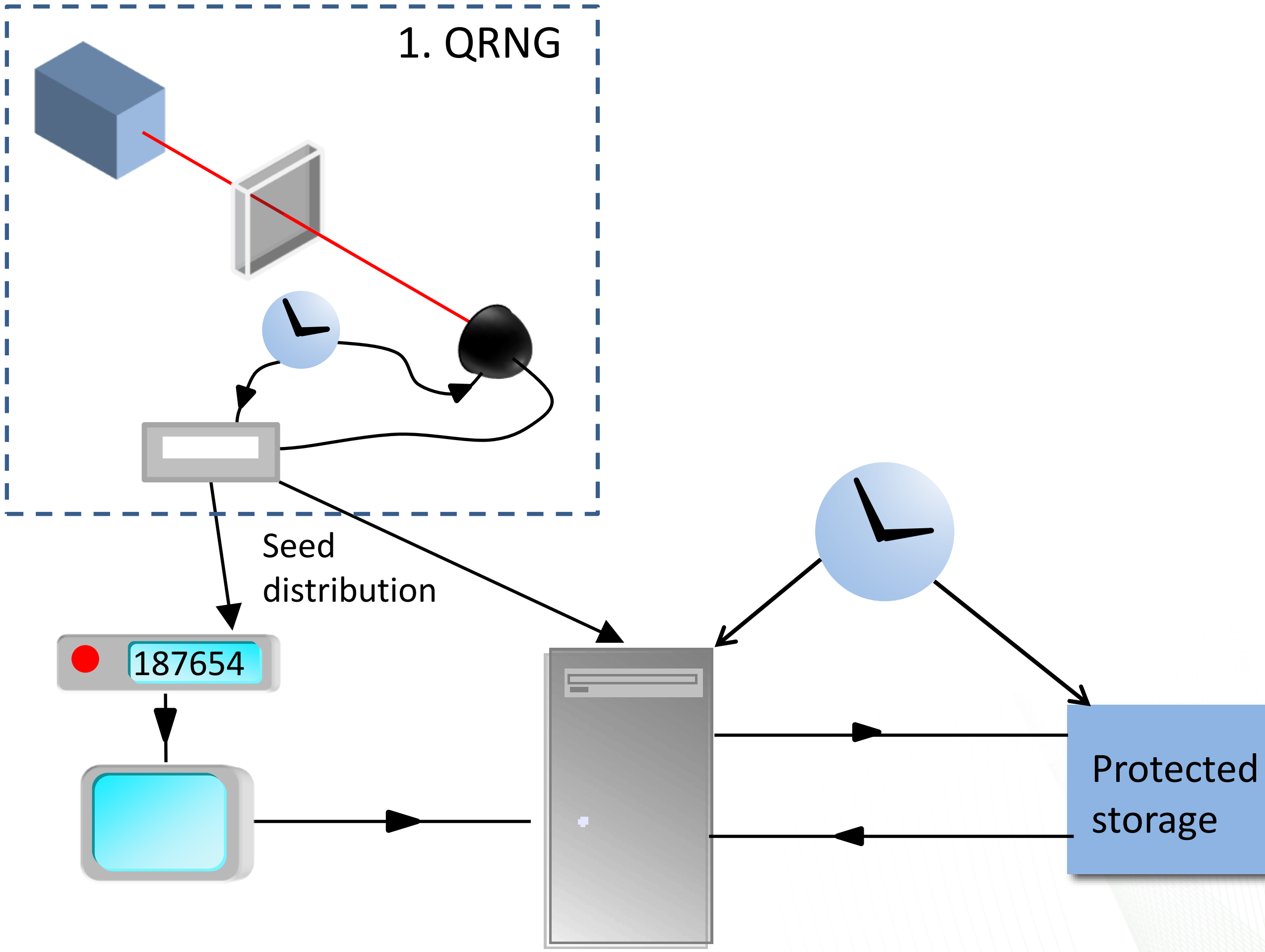
ORNL QRNGs

- Measure shot noise of vacuum field

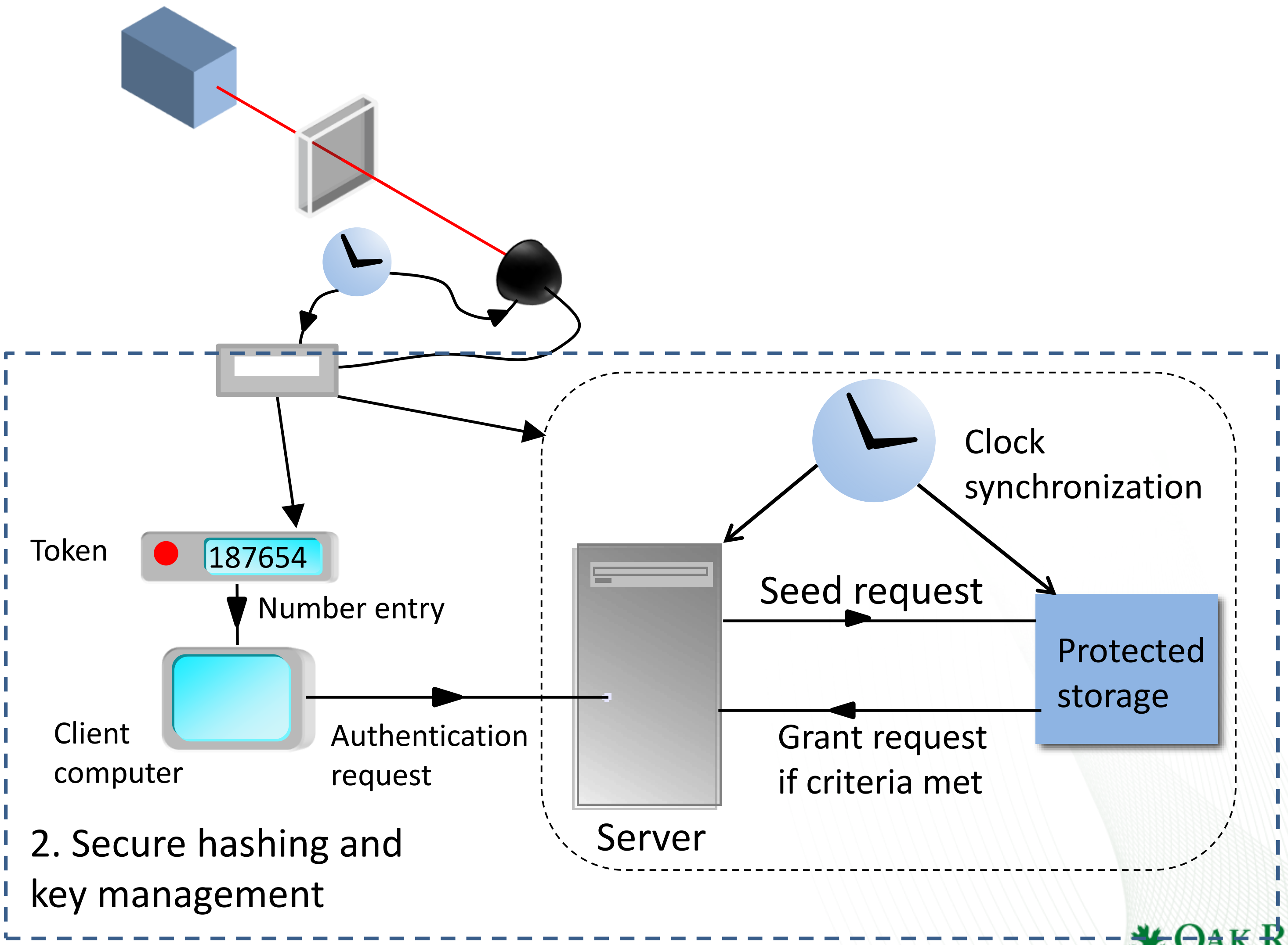




Two factor authentication application

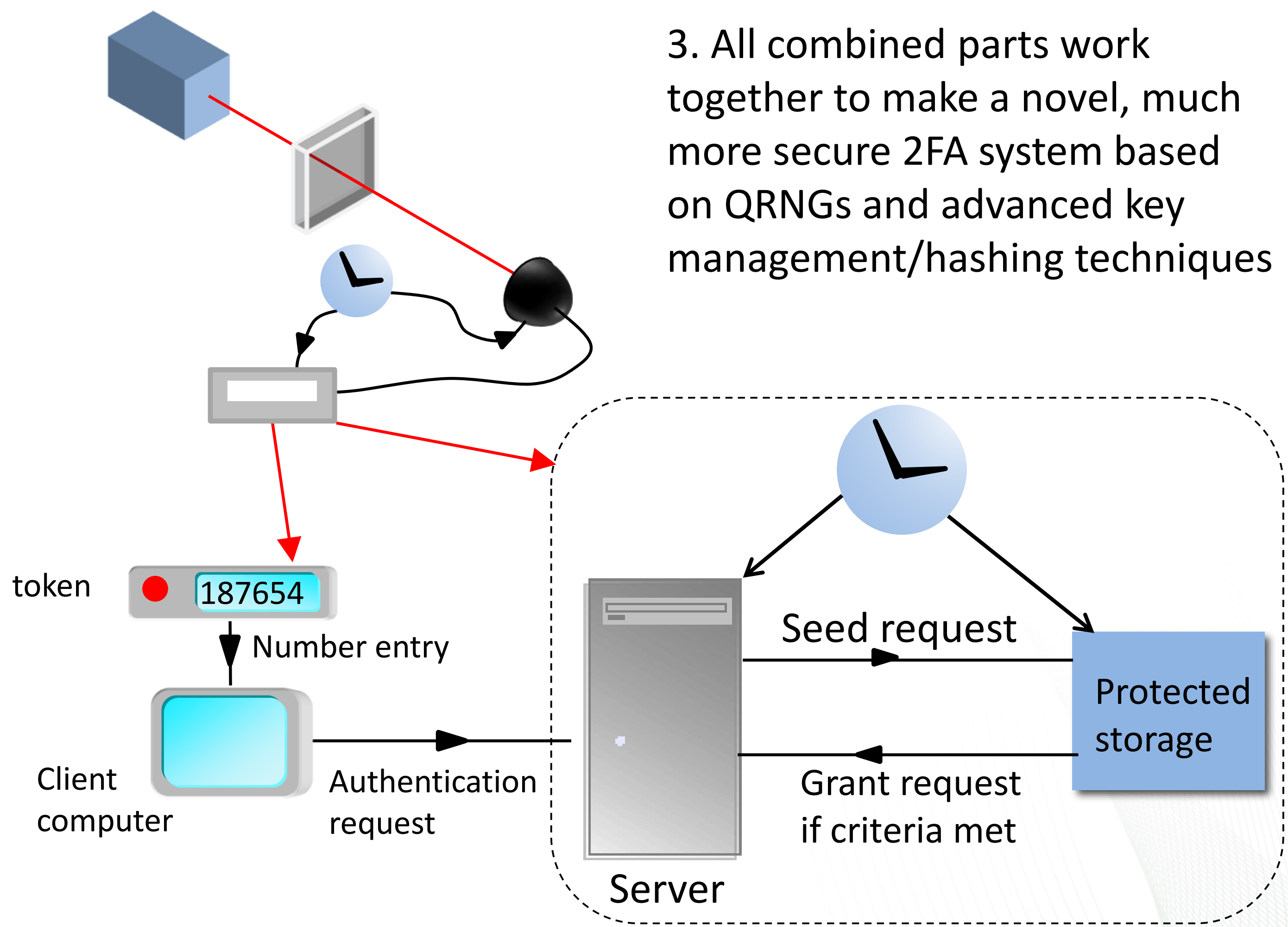


Two factor authentication application



Two factor authentication application

3. All combined parts work together to make a novel, much more secure 2FA system based on QRNGs and advanced key management/hashing techniques



Two factor authentication application

Improved hashing and key management:

- Random seeds expire over time
- Force move to a new seed via button press

seed

time

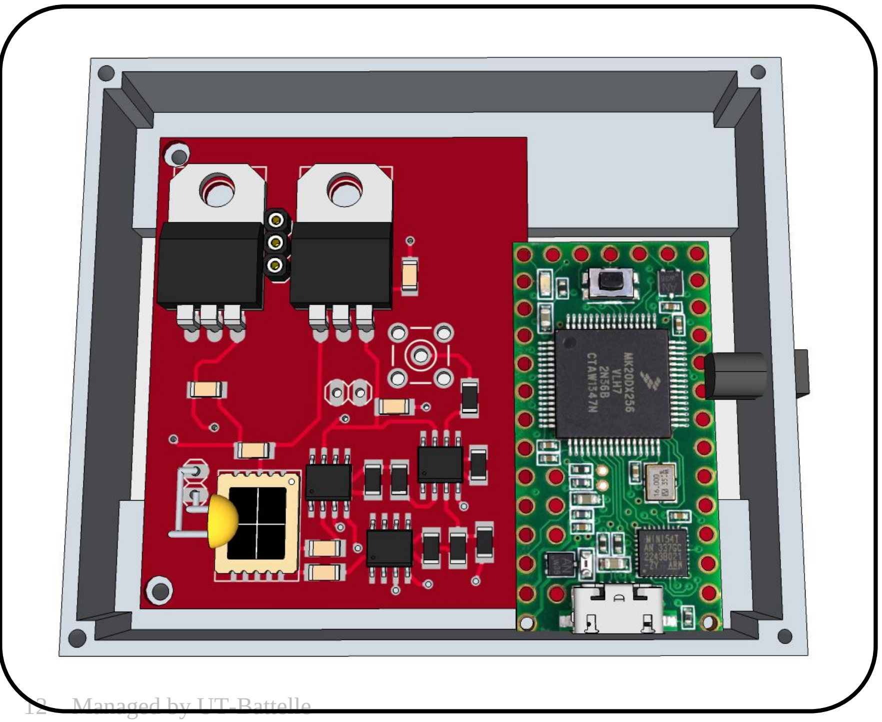
	S_1	S_2	S_3 …
T_1	$H_1(S_1)$	$H_1(S_2)$	$H_1(S_3)$
T_2	$H_2(H_1(S_1))$	$H_2(H_1(S_2))$	$H_2(H_1(S_3))$
T_3	$H_3(H_2(H_1(S_1)))$	$H_3(H_2(H_1(S_2)))$	$H_3(H_2(H_1(S_3)))$
…	…	…	…

- Store seeds securely in protected memory

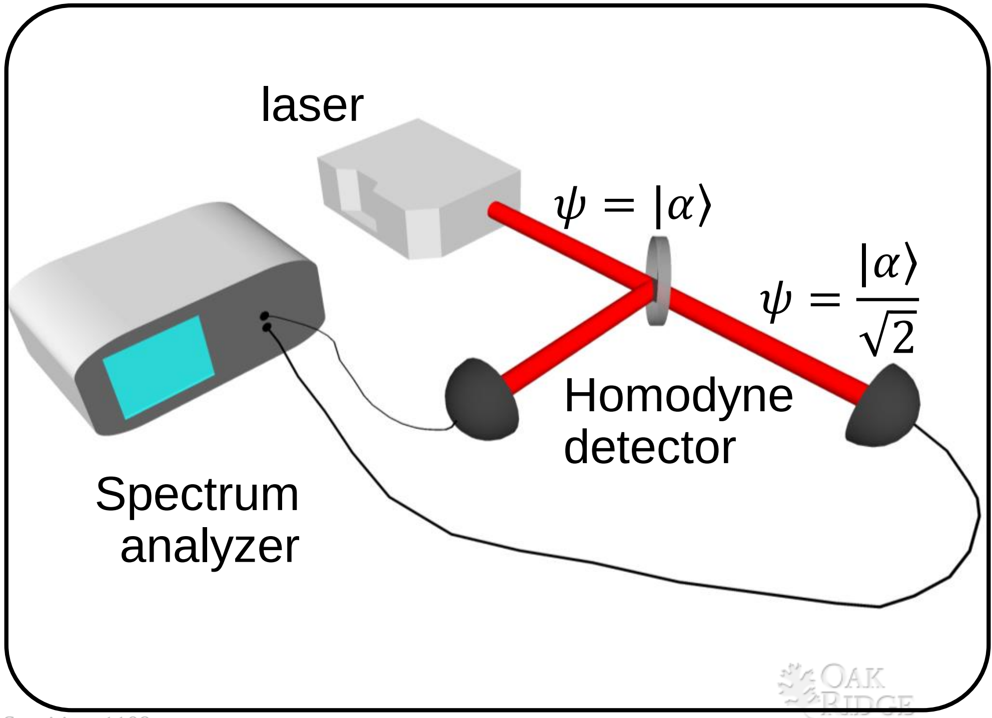
Technology Description

Why is the output random?

- The noise of the quantum vacuum field is random. Even in the absence of light (n=0), the electromagnetic field fluctuates; $H = h\upsilon(n + \frac{1}{2})$
- We amplify these fluctuations with via interference with a local oscillator on a beam splitter
- The split diode accomplishes this task as an integrated beam splitter



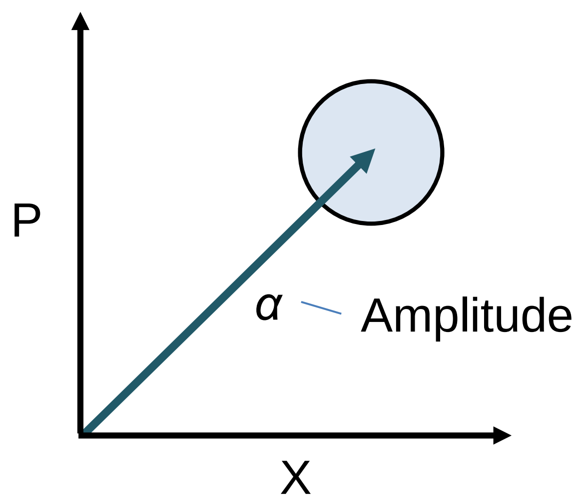
=



Technology Description

Why is the output random? (cont.)

Coherent state phase space

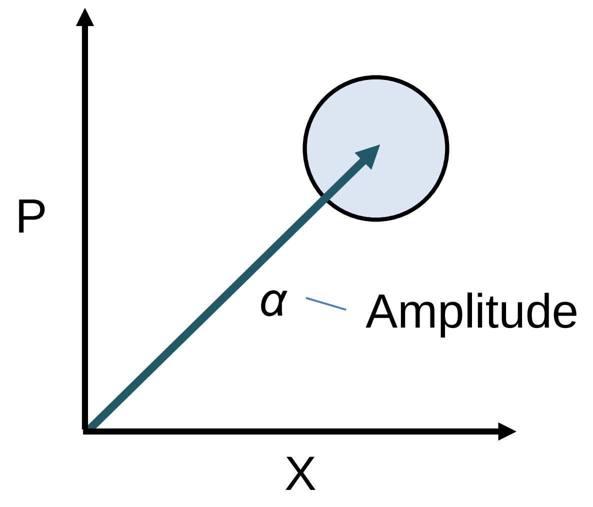


Technology Description

Why is the output random? (cont.)

Heisenberg's uncertainty principle: $\Delta X \, \Delta P \geq \hbar/2$

Coherent state phase space

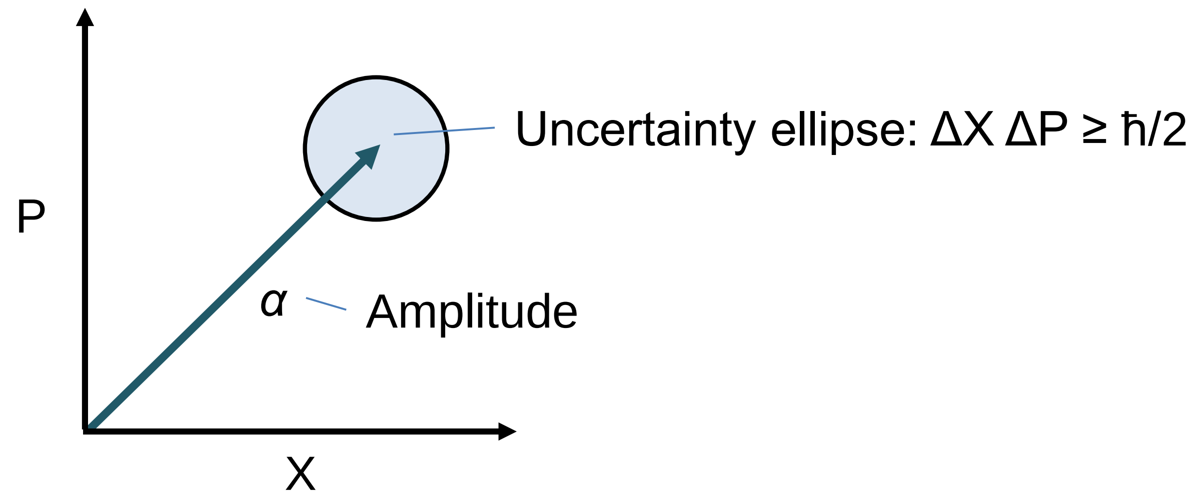


Technology Description

Why is the output random? (cont.)

Heisenberg's uncertainty principle: ΔX ΔP ≥ ħ/2

Coherent state phase space

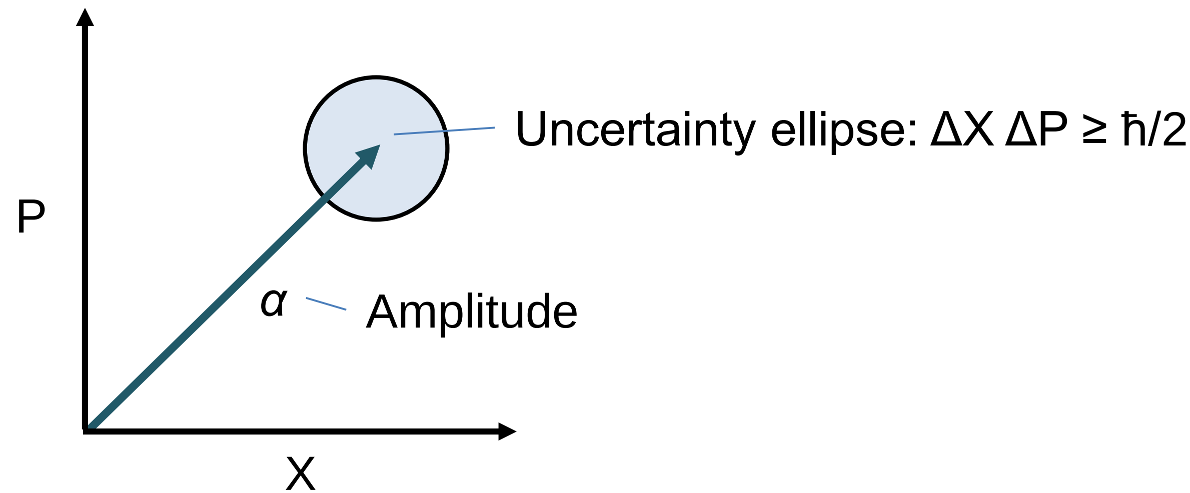


Technology Description

Why is the output random? (cont.)

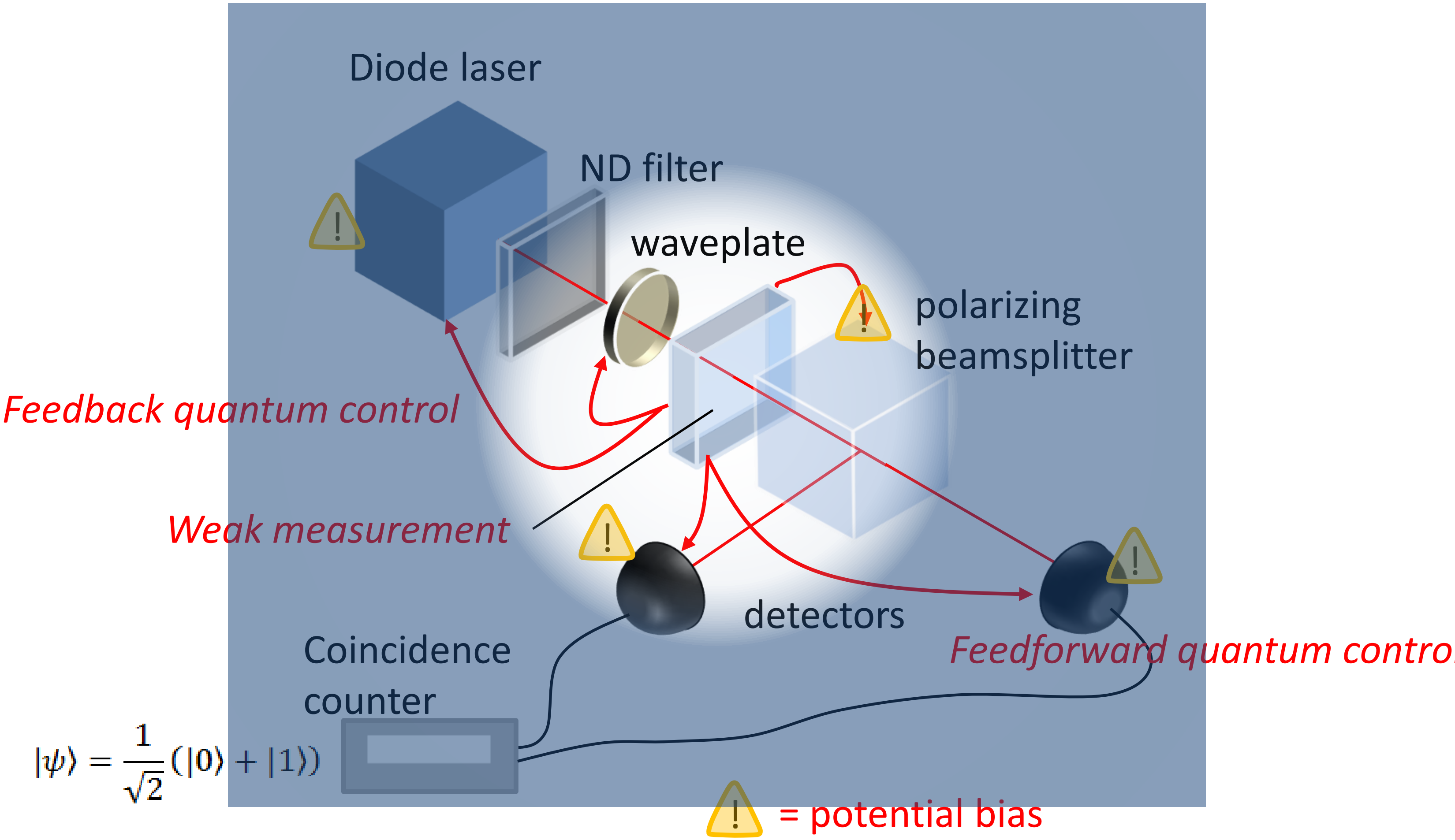
Heisenberg's uncertainty principle: $\Delta X \, \Delta P \geq \hbar/2$

Coherent state phase space



A measurement of X or P (or *α*) cannot be absolutely precise. The result is random within the limits of the HUP! To generate random numbers, access this source of quantum noise

Technology Description: bias detection

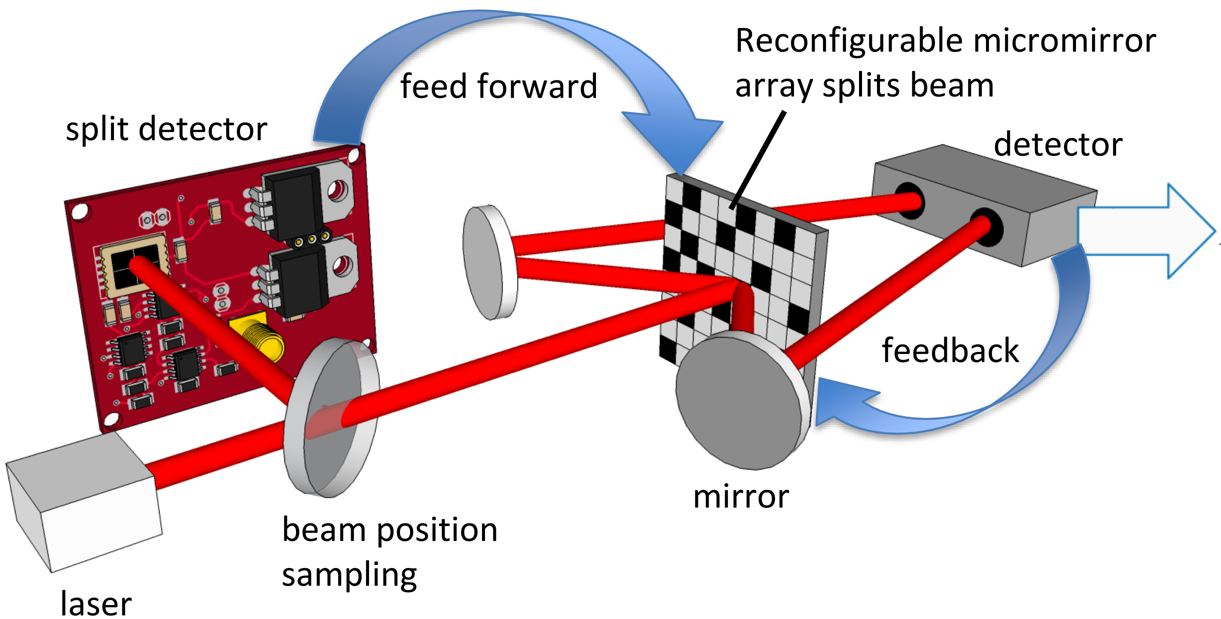


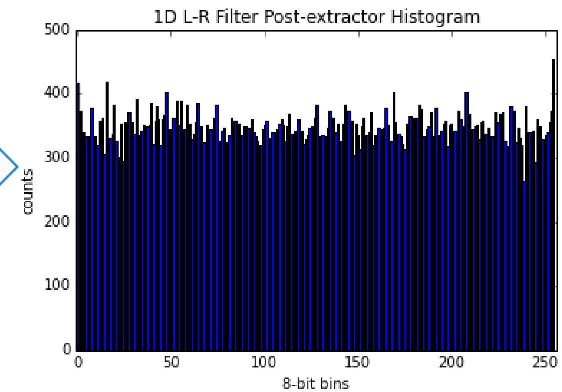
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

QRNG with weak measurement and feedback / feedforward

Canonical QRNG implementation

Technology Description: Previous bias removal implementation

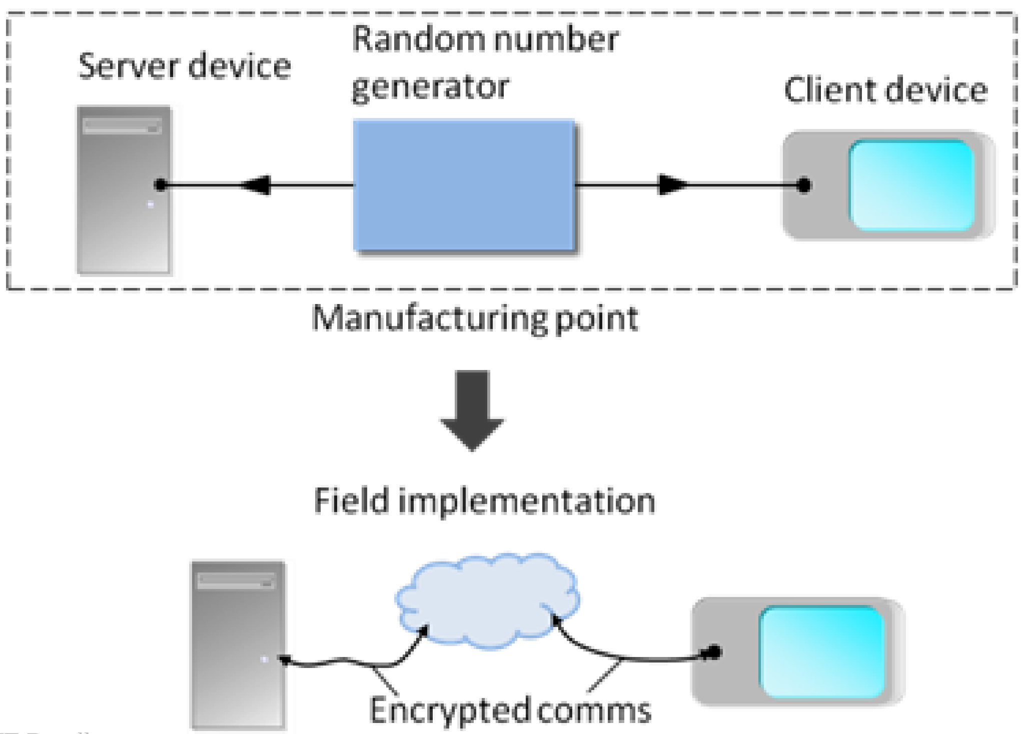




Binned difference data leads to random numbers with automatic bias removal

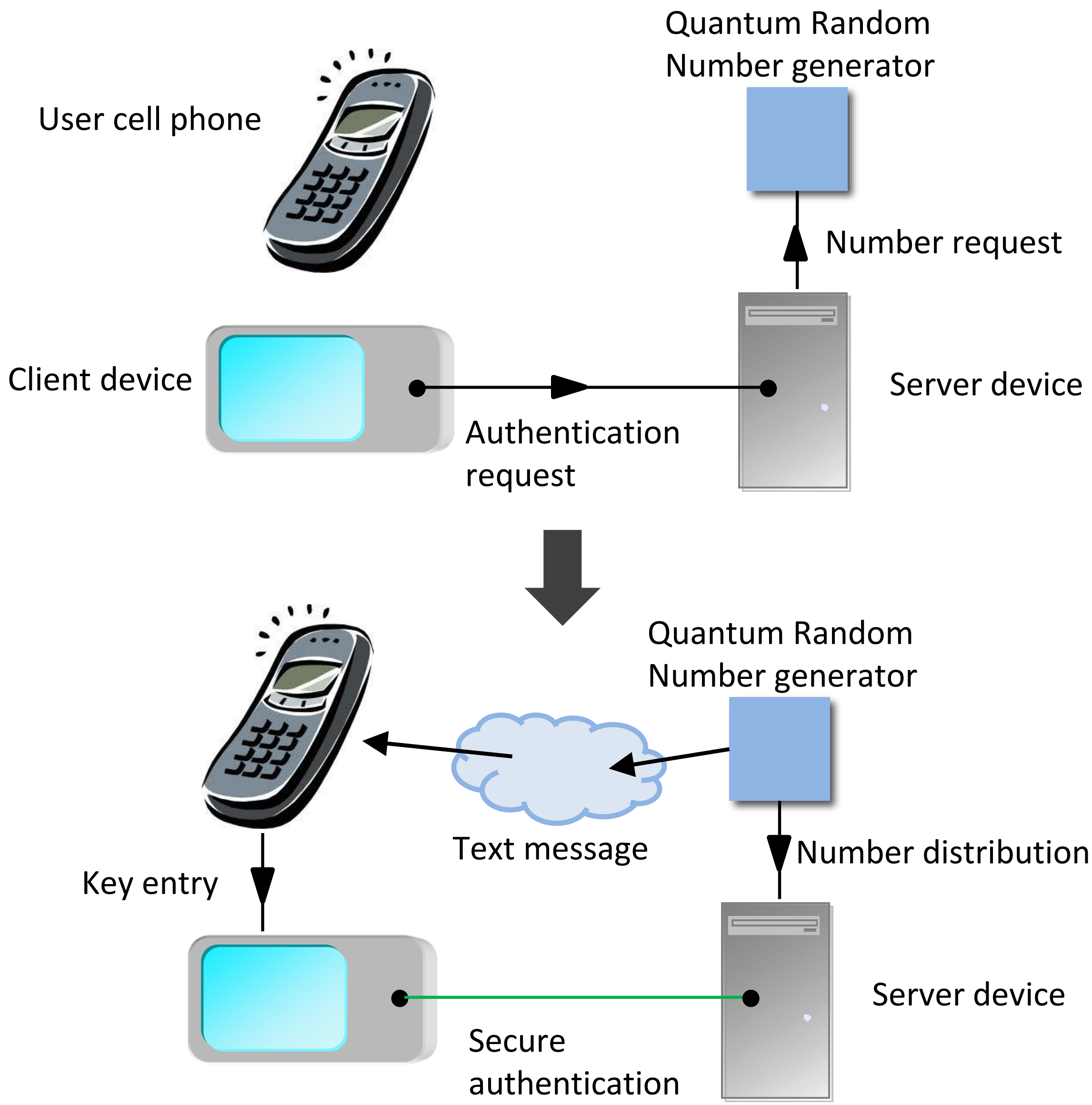
Technology Description

- How would we distribute keys?
- Random number generation and sharing at the point of manufacture. Both devices are separated and share encryption or authentication keys in the field. The table shows example random number lists, in contrast to the pseudorandom seed/hash methods.



time	Server	Client
T_1	R_1	R_1
T_2	R_2	R_2
T_3	R_3	R_3

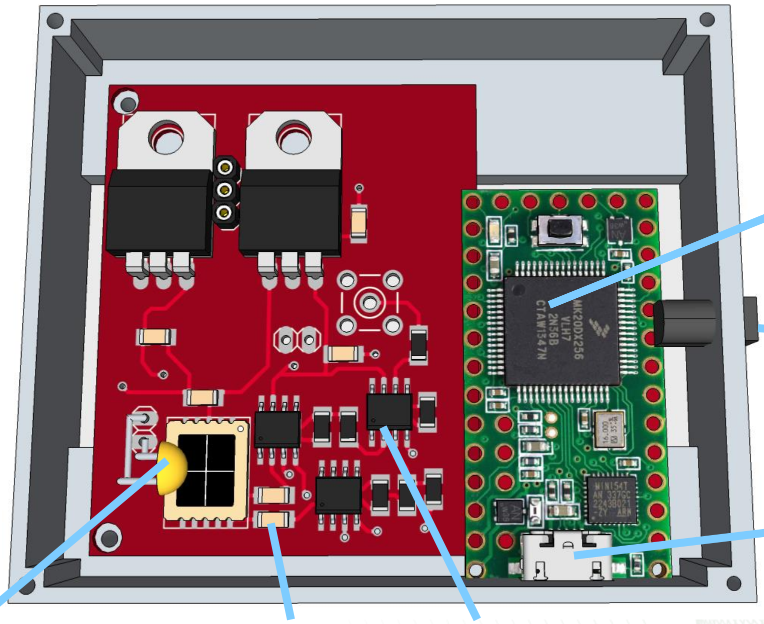
Technology Description



Technology Description

Our TRNG leverages advances in photodetection and quantum state stabilization to achieve at least 3 orders of magnitude higher bitrates, lower bias, and 15x lower cost than previously possible

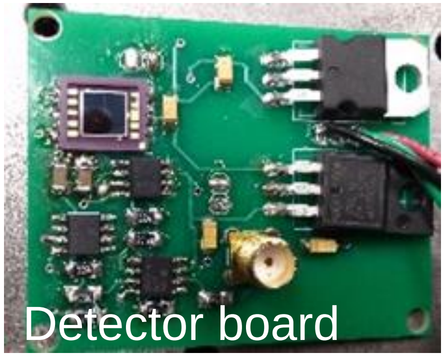
- Beam splitter interaction integrated into diode
- Controller analyzes beam position on diode and adjusts balance to remove bias in situ
- Off the shelf components allow for more economical, highly integrated, and faster detector

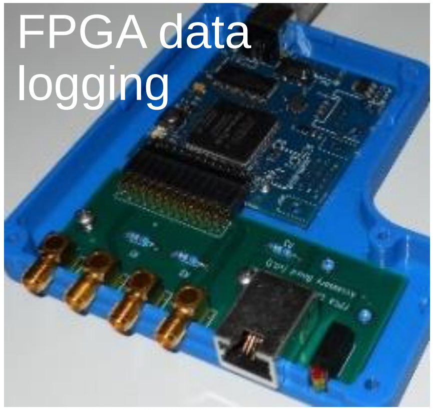


OAK RIDGE National Laboratory

Research and Development Goals

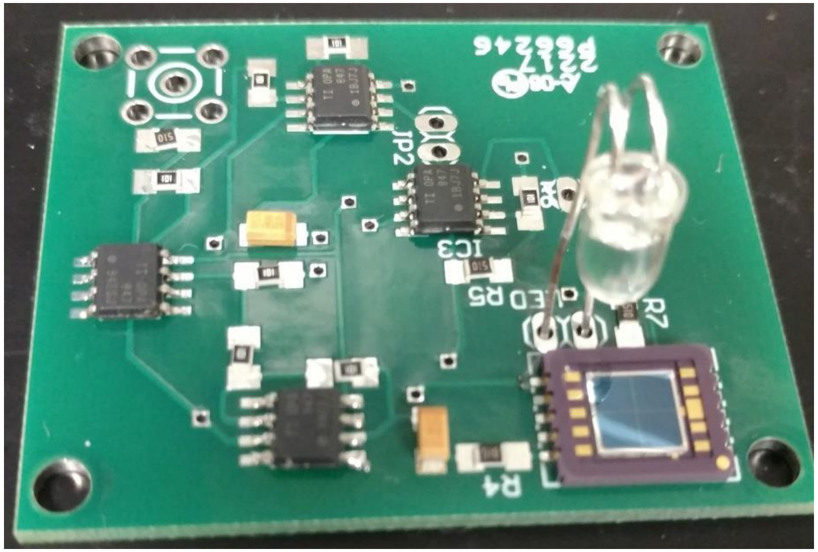
- Reduce TRNG footprint while increasing detection bandwidth
- Integrate LED onto detector board while minimizing excess noise, implementing a homodyne detector;
- Integrate bias correction algorithm
- Verify output of microcontroller with NIST and DIEHARD randomness tests
- Key challenges: detector and LED must be shot noise limited across a large bandwidth; bias detection algorithm must work at high bandwidth to obtain representative sample; attenuators must have sufficient range



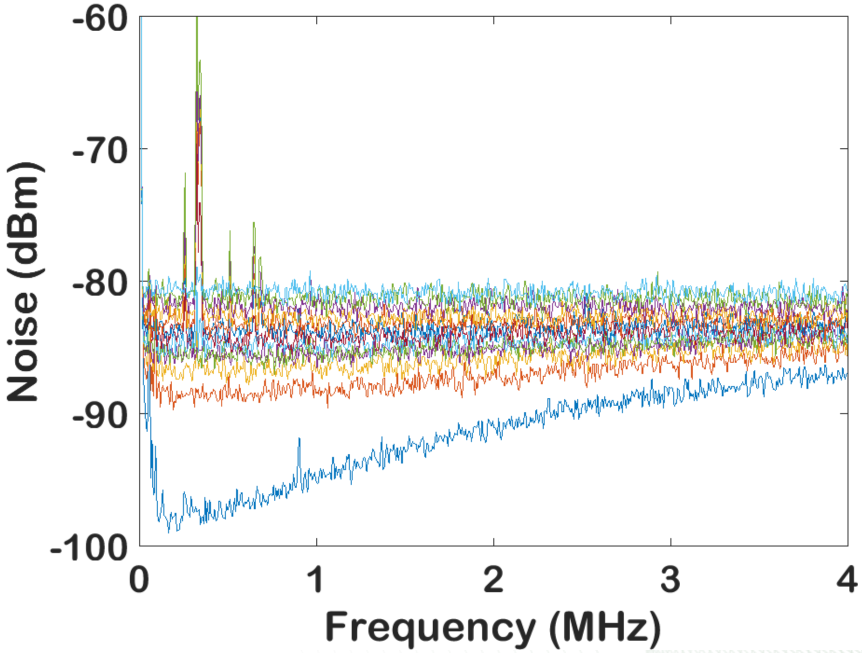


Quantum vacuum noise measurements

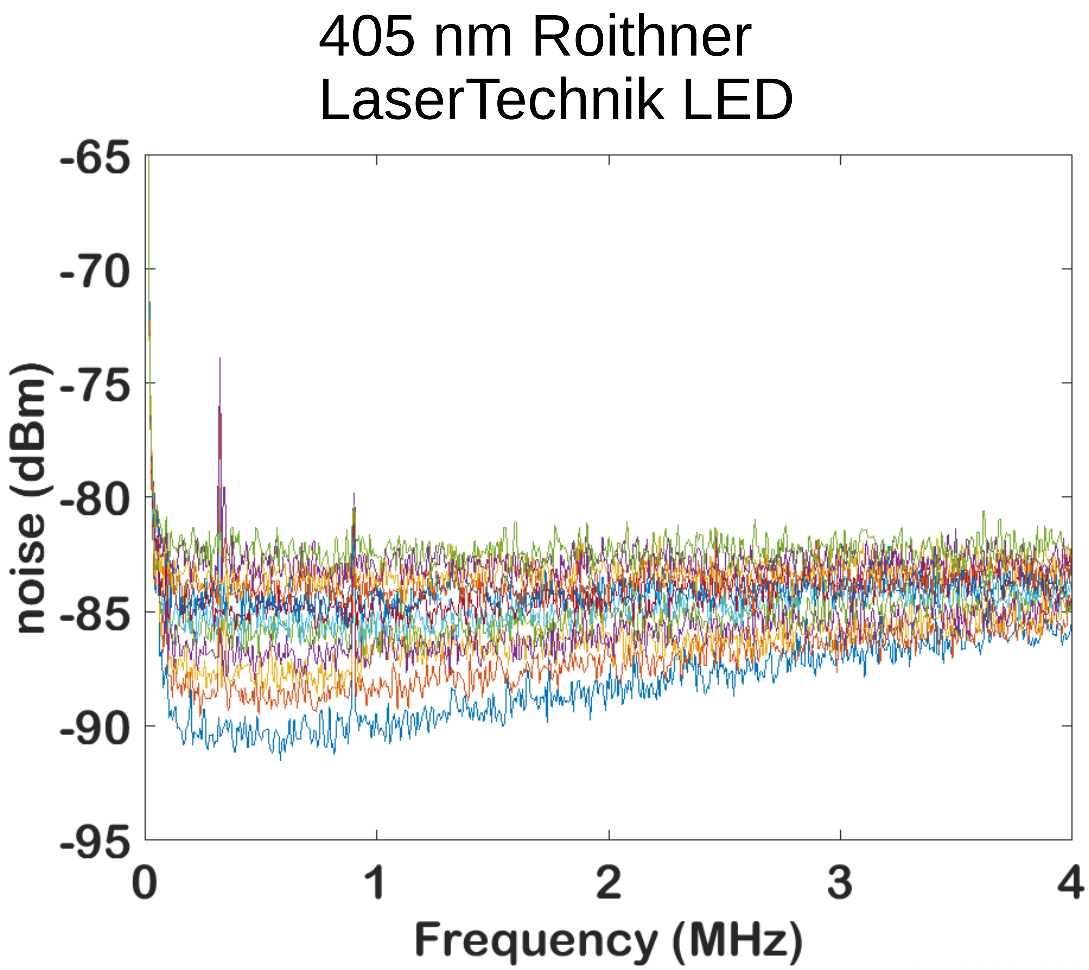
Broadband photon shot noise observed for a variety of LEDs across visible spectrum. Reduced gain in the final circuit will increase the bandwidth by at least two orders of magnitude.



660 nm Hamamatsu LED

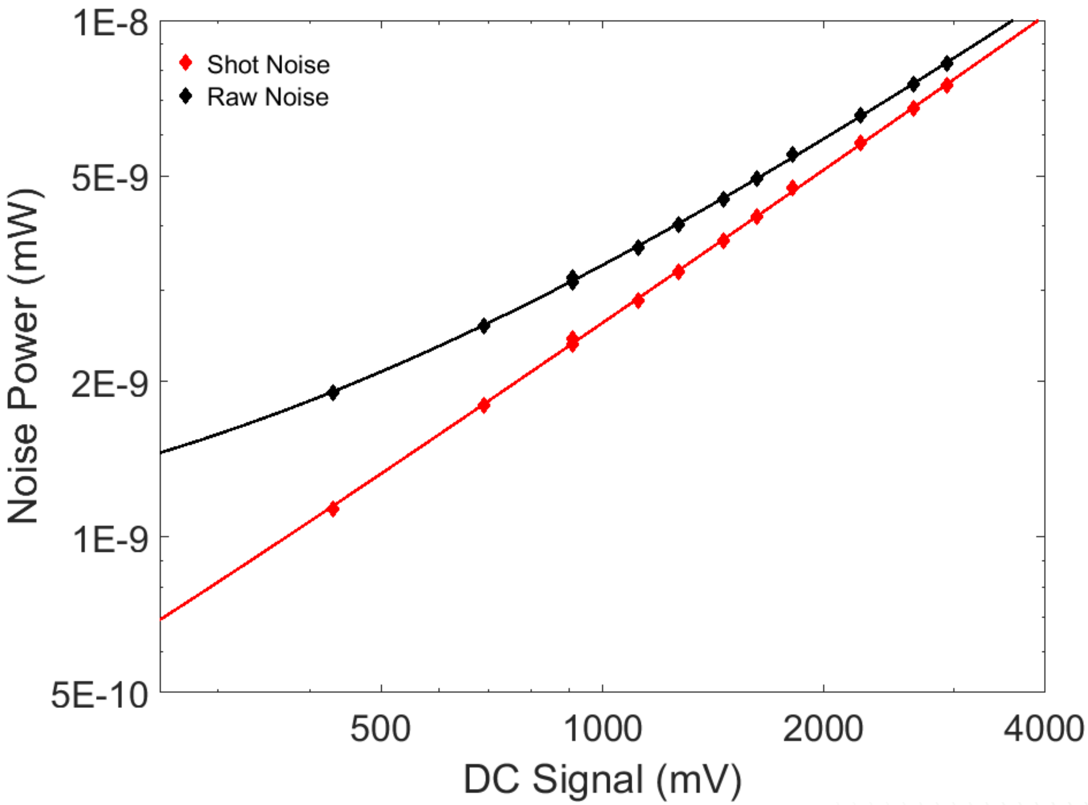


Quantum vacuum noise measurements



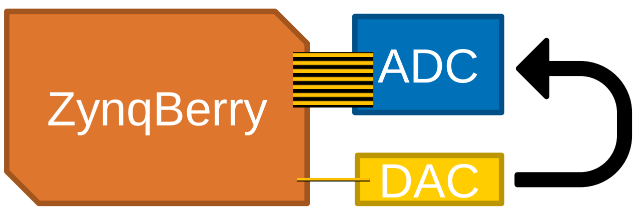
Quantum vacuum noise measurements

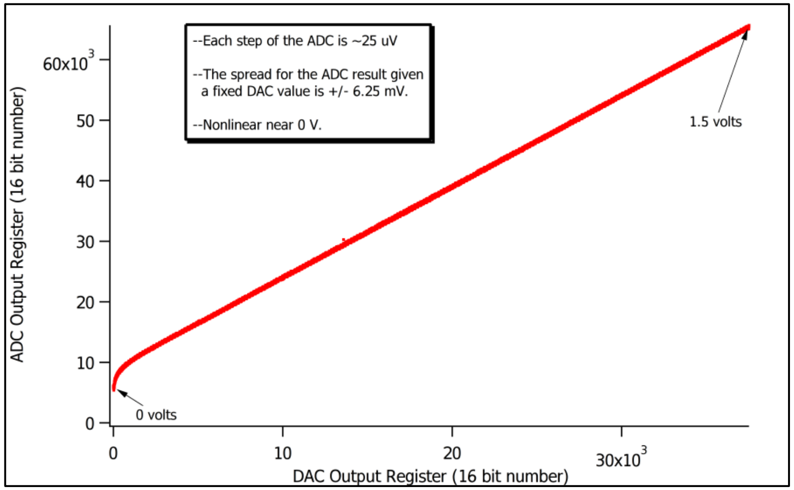
- Linear noise dependence on optical power => white noise



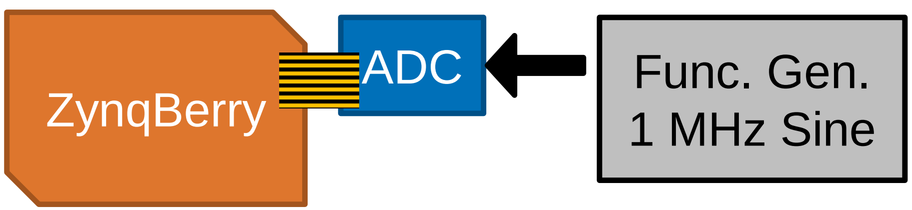
Data Acquisition Performance

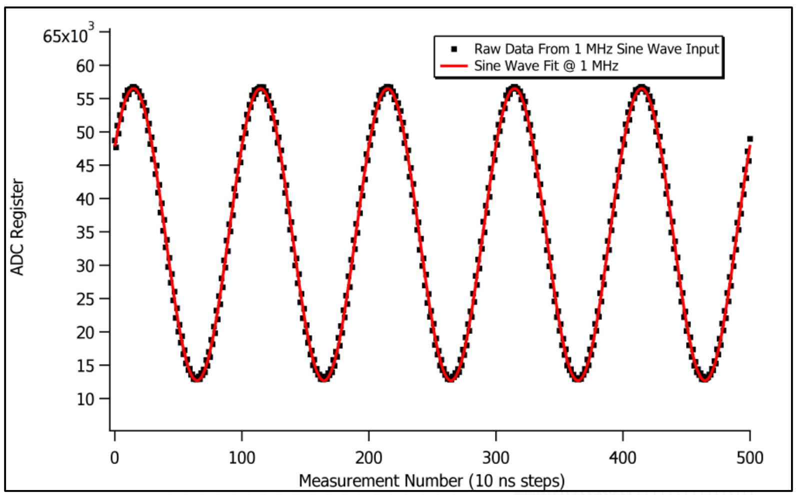
Loopback Test





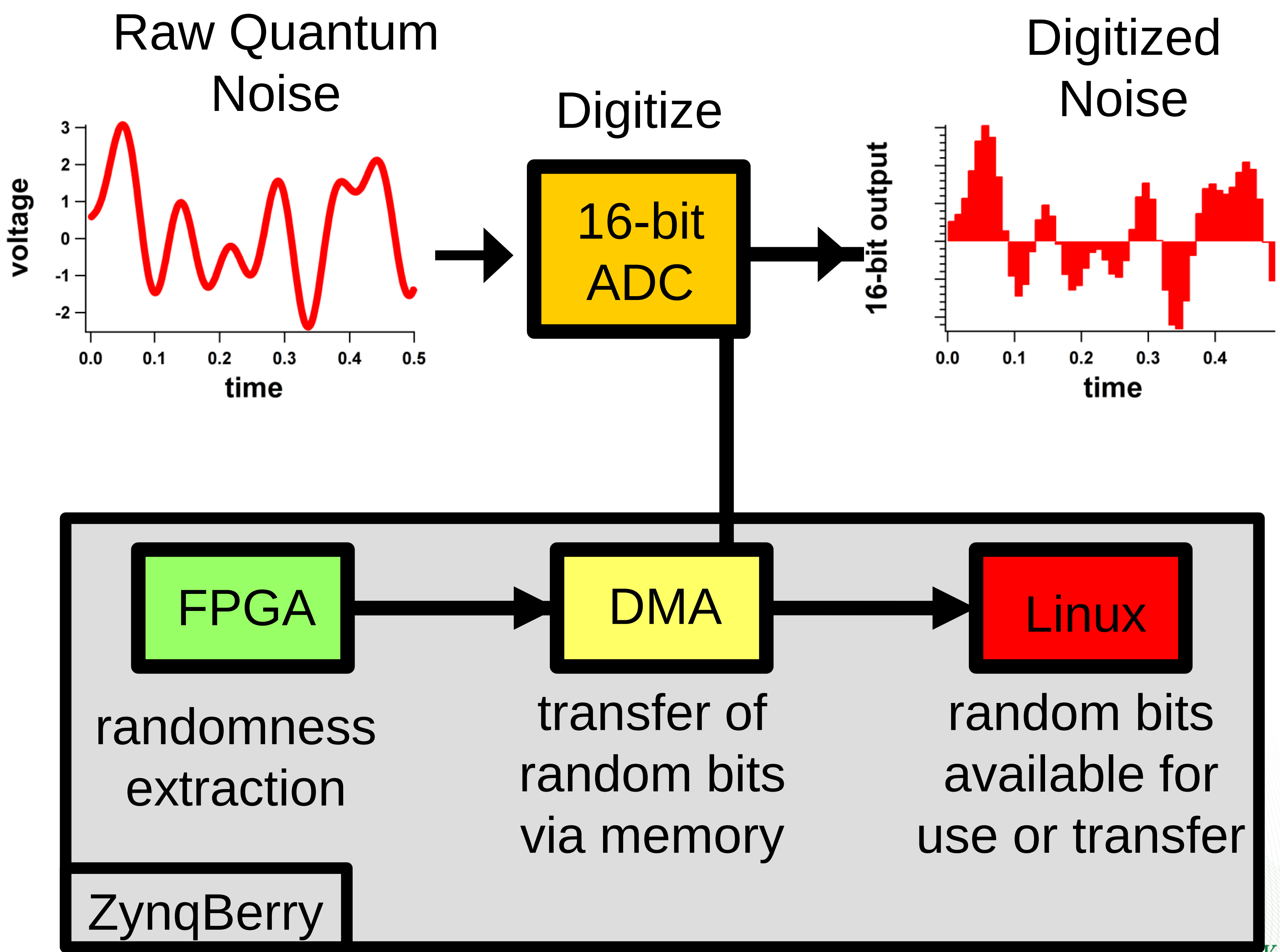
ADC Capability





Raw Bitrate: **1.3 Gb/s***
FPGA ->DMA -> Linux User Space

-Improvement expected
*No Processing


Raw Quantum Noise
voltage
time
Digitize
16-bit ADC
Digitized Noise
16-bit output
time
FPGA
randomness extraction
DMA
transfer of random bits via memory
Linux
random bits available for use or transfer
ZynqBerry

Randomness Extractors take in *n* bits, consume *n*-*m* bits, and produce *m* bits with enhanced randomness.

What we want to do:

Toeplitz matrix — raw bits — Extracted bits

$$\begin{pmatrix} t_m & t_{m+1} & \cdots & t_{m+n-2} & t_{m+n-1} \\ t_{m-1} & t_m & \cdots & t_{m+n-3} & t_{m+n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ t_2 & t_3 & \cdots & t_n & t_{n+1} \\ t_1 & t_2 & \cdots & t_{n-1} & t_n \end{pmatrix} \times \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_{n-1} \\ d_n \end{pmatrix} = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_{m-1} \\ r_m \end{pmatrix}$$

...traditional serial computation can only achieve ≈1 Mbps.

Using parallel operations an FPGA can achieve >1 Gbps.

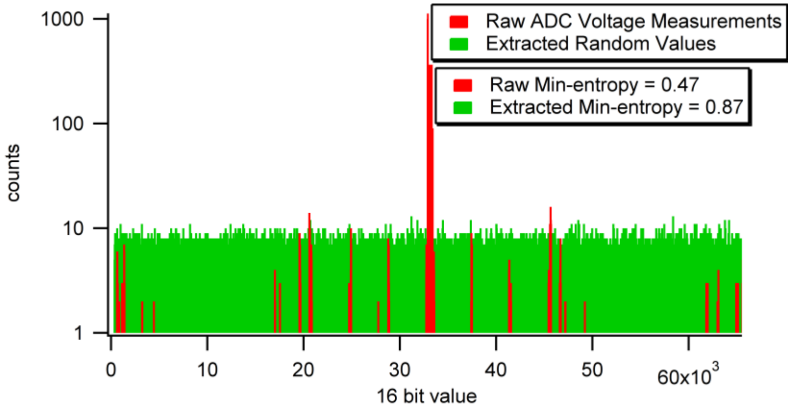
$$\sum_{k=0}^{K} \begin{pmatrix} t_{m+\ell k} & t_{m+\ell k+1} & \cdots & t_{m+(\ell+1)k-2} & t_{m+(\ell+1)k-1} \\ t_{m+\ell k-1} & t_{m+\ell k} & \cdots & t_{m+(\ell+1)k-3} & t_{m+(\ell+1)k-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ t_{\ell k+2} & t_{\ell k+3} & \cdots & t_{(\ell+1)k} & t_{(\ell+1)k+1} \\ t_{\ell k+1} & t_{\ell k+2} & \cdots & t_{(\ell+1)k-1} & t_{(\ell+1)k} \end{pmatrix} \times \begin{pmatrix} d_{\ell k+1} \\ d_{\ell k+2} \\ \vdots \\ d_{\ell k+n-1} \\ d_{\ell k+n} \end{pmatrix} = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_{m-1} \\ r_m \end{pmatrix}$$

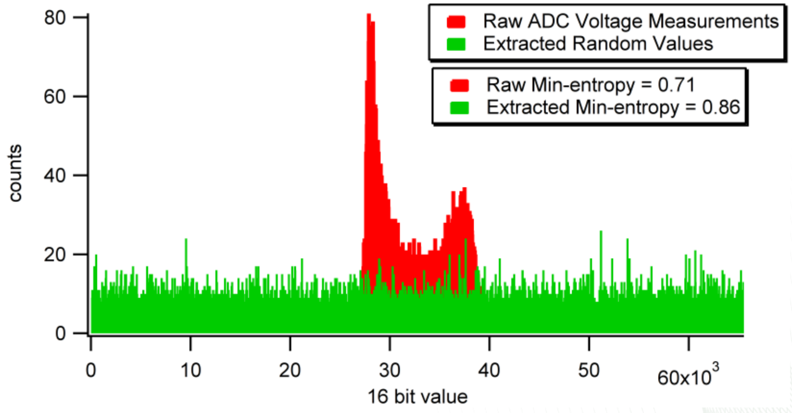
Each *k* step of *K*=*n*/16 steps happens in parallel.

OAK RIDGE National Laboratory

Our ADC is 16-bit operating at 100 Mhz.
The Toeplitz extraction reduces n=1560 raw bits to m=1024 extracted bits.
The maximum bitrate possible is 1.05 Gbps.
We have achieved 1 Gbps.

16 bit values from test and lab sources before and after extraction:





OAK RIDGE National Laboratory

Conclusions

Low cost LEDs can be shot noise limited with cheap power supplies and minimal conditioning

Low cost transimpedance amplifier can amplify quantum vacuum fluctuations

Shot noise is a barometer for bias

Can be used to control bias:

- Variable voltage attenuators
- Variable digital potentiometer
- Spatially dependent beam differencing