Hacking a Quantum Random Number Generator

Smith, P. R.[1,2], Marangon, D. G. [1], Lucamarini, M. [1,3], Yuan, Z. L. [1], & Shields, A. J[1].

[1]Toshiba Europe Ltd, 208 Cambridge Science Park, Milton Road, Cambridge CB4 0GZ, United Kingdom

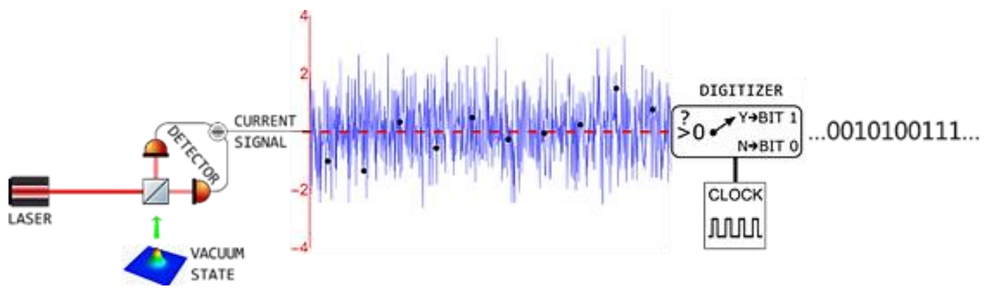
[2]Cambridge University Engineering Department, 9 JJ Thomson Avenue, Cambridge CB3 0FA, United Kingdom

[3]Department of Physics and York Centre for Quantum Technologies, University of York, York YO10 5DD,United Kingdom

1 Background

Continuous variable quantum random number generation

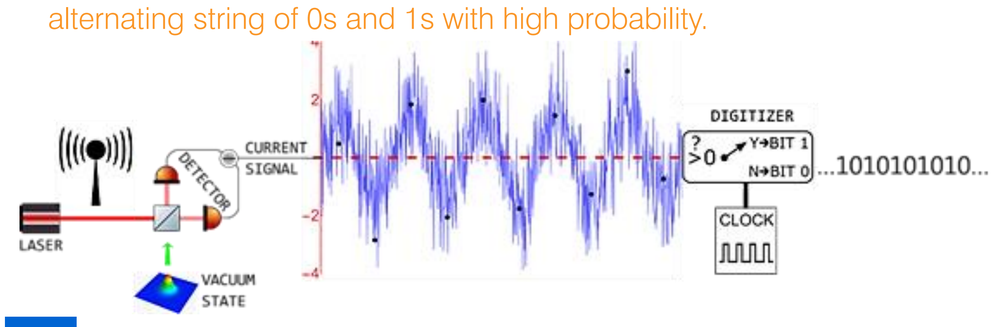
- In the absence of attack, we expect the output of the balanced homodyne detector(BHD) to be Gaussian distributed, with zero mean.
- After thresholding at 0 V, Alice's output will be a random string of 0s and 1s.



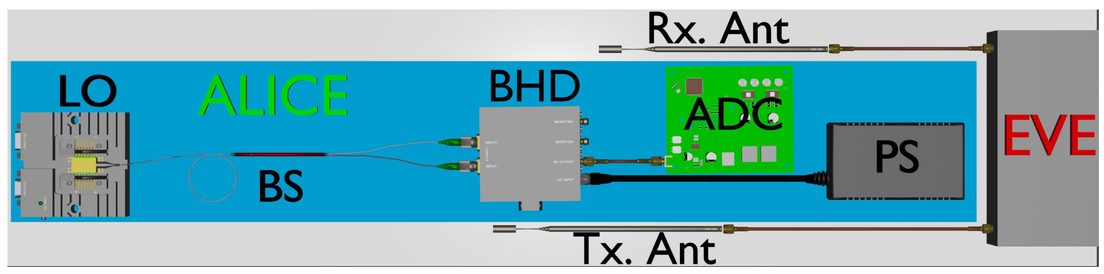
2 Concept

- Eve attacks by injecting an electromagnetic signal, which is superimposed on the BHD output, inducing a shift in the mean of the Gaussian distribution.

➢ Eve's simplest attack strategy is to inject a sine wave at half Alice's sampling rate, such that after thresholding Alice's output will be an alternating string of 0s and 1s with high probability.



3 Experimental Setup

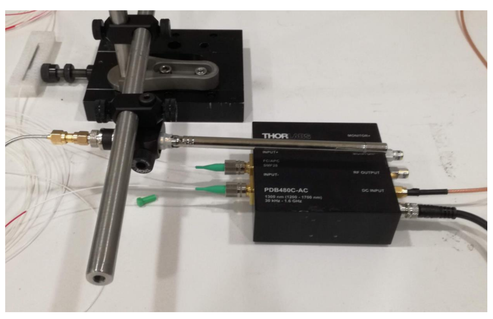


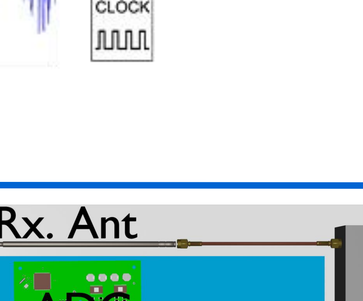
- Alice uses a typical CV-QRNG setup, with an unmodified shielded commercial balanced homodyne detector.
- Eve passively picks up Alice's clock and synchronizes with Alice's ADC with one antenna (Rx) and actively injects her signal with the second antenna (Tx).

4 Eve Injecting a Sine Wave

- Eve injects a sine wave at half Alice's sampling frequency and predicts the output will be an alternating string of 0s and 1s.
- Eve can improve her control of Alice's output by increasing the power of her injected signal.
- The attack would also become more effective if Alice were to reduce her LO power

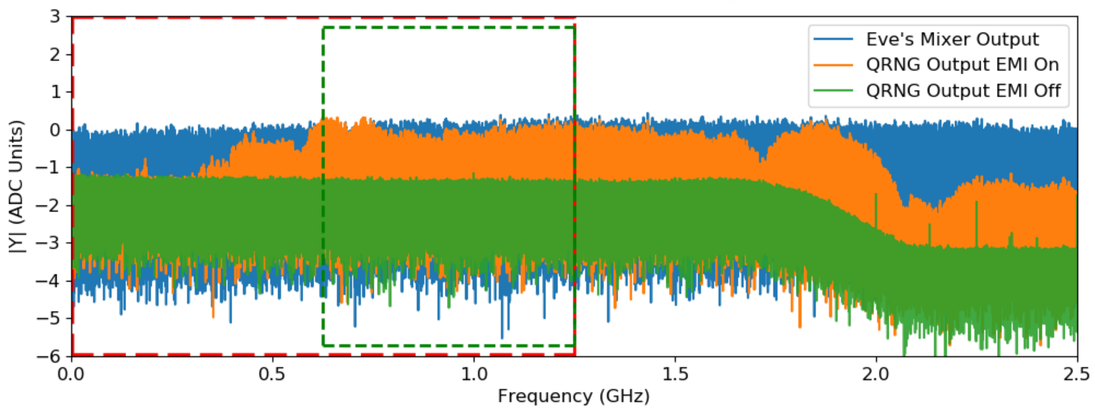
➢ Eve takes control of the QRNG output and predicts 100% of the output correctly.





5 Eve Injecting a Random Pattern

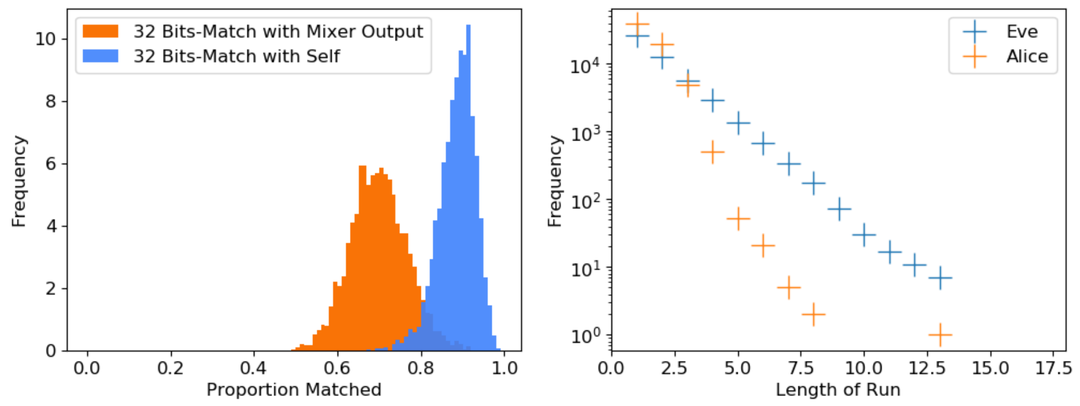
- Statistical tests run on the raw output will be unable to detect the attack if Eve can inject a random pattern.
- To inject a random pattern, Eve uses a mixer to multiply a random NRZ pattern by a carrier sine wave and transmits this signal (c.f. BPSK).



- If Alice uses the band from 0 Hz to 1.25 GHz to generate her output, Eve can transmit her pattern by setting her carrier wave frequency to 1.25 GHz and mixing this with a 2.5 GHz pattern.
- Alice's setup is poor at picking up injected signals below 500 MHz and the longer runs are lost.

➢ For 3000 random 32 bit patterns, an average of 69.8% of the bits in the pattern injected by Eve match the output measured by Alice.

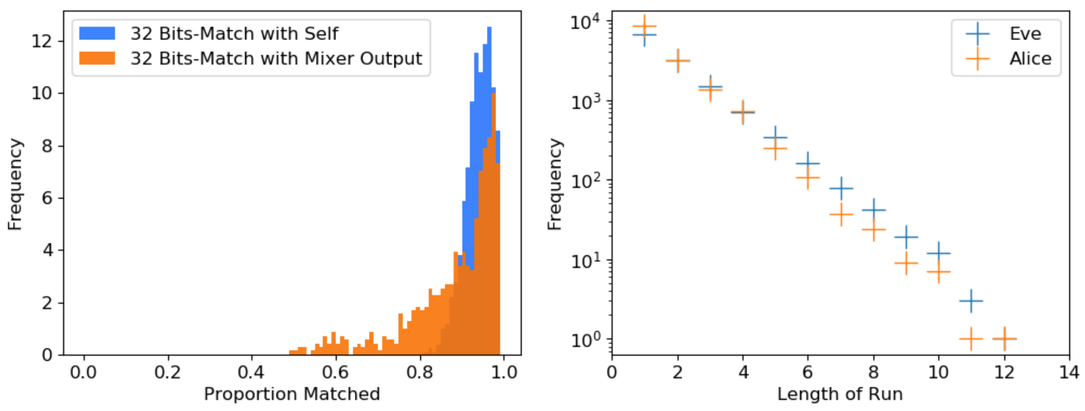
➢ Comparing Alice's output strings to the first 32 bits within them, the match rises to 89%.



- If Alice uses the band from 625 MHz to 1.25 GHz to generate her output, Eve can transmit her pattern by setting her carrier wave frequency to 625 MHz and mixing this with a 1.25 GHz pattern.
- The RF frequency response of Alice's setup is relatively flat throughout this region, meaning that Eve is more successful in transmitting her pattern and the longer runs are preserved.

➢ For 3000 random 32 bit patterns, an average of 88% of the bits in the pattern injected by Eve match the output measured by Alice.

➢ Comparing Alice's output strings to the first 32 bits within them, the match rises to 94%.



Conclusion:

Eve can take full control of a CV-QRNG output through electromagnetic injection.

If perfected, this attack would be undetectable with statistical randomness tests.

Smith, P. R., Marangon, D. G., Lucamarini, M., Yuan, Z. L., & Shields, A. J. (2021). Out-of-Band Electromagnetic Injection Attack on a Quantum Random Number Generator. Physical Review Applied, 15(4), 044044.

This work was supported by the Industrial Strategy Challenge Fund (ISCF): 106374-49229 Assurance of Quantum Random Number Generators. P.R.S. Gratefully acknowledges financial support from the EPSRC (Award No. 1771797) CDT in Integrated Photonic and Electronics Systems and Toshiba Europe Limited.