Generating Quantum Random Numbers Using Entanglement in Low Earth Orbit

Ayesha Reezwana (cqtayes@nus.edu.sg)
National University of Singapore https://orcid.org/0000-0001-8172-1392
Tanvirul Islam
National University of Singapore
Xueliang Bai
The university of Sydney
Christoph Wildfeuer
FHNW University of Applied Sciences and Arts Northwestern Switzerland
Alexander Ling
National University of Singapore
James Grieve
National University of Singapore https://orcid.org/0000-0002-2800-8317

Article

Keywords: Quantum, physical, Earth orbit, QRNG

Posted Date: July 27th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-690179/v1

Generating quantum random numbers using entanglement in low Earth orbit

Ayesha Reezwana* and Tanvirul Islam
Centre for Quantum Technologies, 3 Science Drive 2, National University of Singapore, 117543 Singapore

Xueliang Bai
ARC Training Centre for CubeSats,UAVs, and Their Applications(CUAVA), School of Physics, The university of Sydney

Christoph F. Wildfeuer
FHNW University of Applied Sciences and Arts Northwestern Switzerland, School of Engineering, 5210 Windisch

Alexander Ling
Centre for Quantum Technologies, 3 Science Drive 2, National University of Singapore, 117543 Singapore and
Department of Physics, National University of Singapore, Blk S12, 2 Science Drive 3, 117551 Singapore

James A. Grieve†
Quantum Research Centre, Technology Innovation Institute, Abu Dhabi and
Centre for Quantum Technologies, 3 Science Drive 2, National University of Singapore, 117543 Singapore

We describe the implementation of a quantum random number generator (QRNG) on-board a nanosatellite deployed to low Earth orbit (LEO). The generator samples shot noise from an entangled photon-pair source based on spontaneous parametric down conversion, linking the entropy of the QRNG to fluctuations in the vacuum field. We present analysis of data acquired in lab-based acceptance testing as well as on-orbit, and use the source to implement a prototype for an off-grid randomness beacon.

I. INTRODUCTION

Quantum random number generators (QRNGs) access the inherent randomness of quantum processes as a source of entropy, in order to produce an unbiased and unpredictable output. These devices have been shown to have many prospective use cases, notably in cryptography [1], simulation [2], telecommunications [3], and financial systems [4]. QRNGs may be particularly appropriate for small-scale and resource-constrained platforms, where other physical entropy sources are scarce.

In contrast to other physical random number generators, the unpredictability that is a natural consequence of quantum mechanics provides an abundant and uncomplicated source of randomness. Despite this relative availability, it is non-trivial to extract randomness from a quantum source due to the presence of technical noise arising from the imperfect nature of the measurement devices [5].

In recent years, there have been many successful demonstrations of quantum random number generators in laboratories [6–8], and several commercial products have entered the marketplace [9]. In this work, we describe the implementation of a quantum random number generator on an orbiting nanosatellite, SpooQy-1 [10]. In addition to the tasks noted previously, orbiting random number generators may find utilization in "prepare-and-measure" quantum key distribution (QKD) schemes [11], and can enable the implementation of a resource known as a randomness beacon [12]. While a number of randomness beacons are currently accessible via the internet [12, 13], an orbiting beacon would be available to remote infrastructure with only sporadic, high-latency internet access (for example, monitoring stations connected via store-and-forward satellite services [14, 15]). Such installations could then make use of beacon pulses, for example in time-stamping algorithms to increase the integrity of record-keeping, or for auditable input to a sampling process [16].

The primary goal of the SpooQy-1 mission is to demonstrate a compact and sturdy entangled photon pair source in space; a stepping-stone towards the development of cost-effective satellite-to-ground or satellite-to-satellite QKD. Due to its status as a secondary mission objective, our QRNG implementation is based on measurements made on the same polarization entangled photon-pair source.

In this manuscript, we provide a brief overview of this instrument, along with the randomness extraction procedure and related experimental results. We assess the quality of the generated data using randomness testing suites (including the popular "Dieharder" package [17]) on a large volume of extracted random bits and validate the "Dieharder" test results using Kolmogorov-Smirnov test (KS test) [18]. Finally, we describe a proof-of-concept implementation of a secure public randomness beacon, and demonstrate the retrieval of beacon data via two distant ground stations, located in Switzerland and Singapore.

II. SOURCE DESIGN AND IMPLEMENTATION

SpooQy-1 demonstrates generation of polarization entangled photon-pairs via a violation of the CHSH inequality [20]. To this end, the satellite payload is equipped with a quantum light source compatible with the stringent constraints of the

* cqtayes@nus.edu.sg
† james.grieve@tii.ae

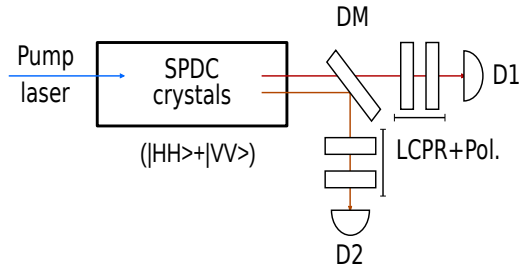

FIG. 1: A simplified block diagram of the random number generator, based on entangled photons generated via spontaneous parametric down conversion in nonlinear crystals (SPDC crystals). D1 and D2 represent detector systems that can perform polarization measurement using a combination of liquid crystal polarisation rotators (LCPR) and polarizing filters (Pol), on the photon-pairs after separation by a dichroic mirror (DM). A detection and counting circuit records the number of coincident events per second. The quantum shot noise of the coincident count is used as the entropy input to our QRNG.

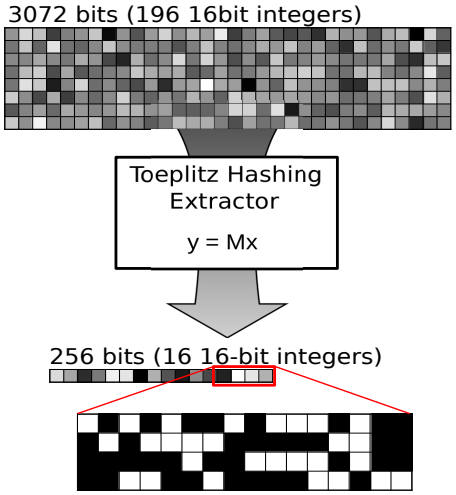

FIG. 2: A visualization of the random number extraction process. 256 uniform random bits (y) are generated from 3072 input bits (x), captured as 196 16-bit integers. The extraction is performed using a 256×3072 Toeplitz matrix [19] (M), which simultaneously removes any bias from the input sequence, and excludes the impact of non-quantum noise sources.

CubeSat bus [21], as well as a detector package capable of performing the required two-photon polarization correlation measurements. Detailed design of the source, analysis, and preliminary results can be found in the PhD dissertation of A. Villar [22].

Figure-1 shows a simplified block diagram of the entangled photon pair source and detection system. The source generates polarization entangled photons using spontaneous parametric down conversion (SPDC), a nonlinear optical process in which high energy photons with a small probability split into pairs of lower energy photons following conservation of energy and momentum [23]. After separation by wavelength, two liquid crystal polarization rotators (LCPRs) are used to select measurement bases, with avalanche photo diodes (D1,D2) employed to detect individual photons. On-board electronics identify photon-pairs by selecting detection events coincident within a 2 ns timing window [22].

Entangled photons are produced in Bell-like states such as

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) \tag{1}$$

When the same measurement bases are selected for both photons, the majority of the coincident events are attributed to entangled photon pairs. Accidental coincidences attributed to other sources (e.g. detector dark counts, stray light) are rendered negligible by the use of a sufficiently short timing window (in this work they account for $\sim 2\%$ of the signal [22]). We select the diagonal basis to measure both of the photons. This re-enforces the quantum nature of the correlations, which for this geometry are approximately twice as strong as they would be in a classical device. As it is based on coincident events, this detection scheme can be used to minimize contribution from other entropy sources which would otherwise dominate the single detection channels. Randomness in the resulting event rates originates from spontaneous vacuum fluctuations, and we use this signal as our raw entropy source.

The number of detected coincident events per unit time follows a Poisson distribution [24], with an easily characterized mean value. We extract uniform random numbers from this signal using a Toeplitz hashing extractor [19]. Our approach resembles work described by Sanguinetti et al. [5], where random numbers are generated by sampling a coherent illuminating beam with a mobile phone camera.

For a coincidence rate λ with X a random variable corresponding to the number of events observed in one second, the probability of observing a particular measurement n is given by

$$Pr[X = n] = \frac{e^{-\lambda}\lambda^n}{n!} \tag{2}$$

The quantum entropy corresponds to the min entropy of this distribution, given by

$$H_{\min}(X) = -\log_2\left(\frac{e^{-\lambda}\lambda^{\lfloor\lambda\rfloor}}{\lfloor\lambda\rfloor!}\right) \tag{3}$$

While the contribution of classical noise is already limited in our implementation, in most cases, a properly designed randomness extractor is necessary to eliminate any information a hypothetical adversary might gain via knowledge or control over this classical noise component. Such an extractor is also useful in distilling a uniform distribution from a Poissonian source, as in this case.

If k bits are used to encode each event X then from equation (3) each such event has entropy at least $H_{\min}(X)$.

If each bit encoding X contains g bits of entropy then the randomness extraction ratio is,

$$g = \frac{H_{\min}(X)}{k} \tag{4}$$

Where, $g < 1$.

To extract random bits with unit entropy per bit we use a Toeplitz hash based extractor. Here, a $l \times m$ Toeplitz matrix M is used to extract l high entropy bits from m low entropy bits, where l/m approaches the extraction ratio g.

If x is a Boolean vector of length m representing the low entropy bits and y is the extracted l high entropy bits then,

$$y = Mx \tag{5}$$

Here, the Boolean vector x is constructed by concatenating the binary encoding of several events drawn from the random variable X so that the length m is achieved.

In this case, the output bits y are uniformly random with probability [5]

$$1 - \varepsilon \geq 1 - 2^{-(gm-l)/2}. \tag{6}$$

Where, security parameter, $\varepsilon > 0$ is the probability of failure for the randomness extraction.

In our experiment, coincidence data is encoded in $k = 16$ bit registers. From analysis of $47,422$ seconds of data generated using a ground-based identical copy of the source, we estimate the quantum randomness per bit as $g \geq 1/4$. We employ a Toeplitz matrix with dimensions $l = 256$ and $m = 3072$, yielding 256 bits of extracted randomness per 192 16-bit registers and achieving a rate of 80 bits/minute. From equation (6) we expect the generated random bits to deviate from perfect randomness with probability at most 2^{-256}. This means that we must collect and process 2^{256} random bits before being able to predict the next bit, assuming full control over or knowledge of the classical noise of the original source.

Figure 3(a) depicts detector coincident counts collected for 125 minutes in a laboratory setting using a source identical to that on the satellite. We see a slow moving trend (red line) which we trace to gradual fluctuation of the power supply. After removing the low frequency component using Fast Fourier Transform (FFT) we obtain data exhibiting a Poisson distribution (mean 1785 and Fano factor [26] close to 1, Figure 3(c)). This suggests that the remaining data consists of shot noise [5]. While resource constraints on the satellite do not permit the use of FFT algorithms to remove the low frequency component, the use of only short-duration data blocks (192 samples of the coincident event rate) may enable us to disregard these low-frequency contributions. This is confirmed by Figure 3(b), in which Fano factors of 200-point data blocks are shown to be close to 1, a signature of Poisson statistics reinforcing the absence of significant low-frequency noise.

A 35.6 kB sequence of random data generated in the laboratory is evaluated using the "Dieharder" test suite, and the result validated by KS test with the analysis summarized in Figure-4. In this analysis, the expectation for a random source is that the p-value for each test should be distributed in the interval [0.01, 0.99]. We use the KS test to confirm the distribution of p-values and our source appears to conform to the metric showing the empirically obtained p-values remain

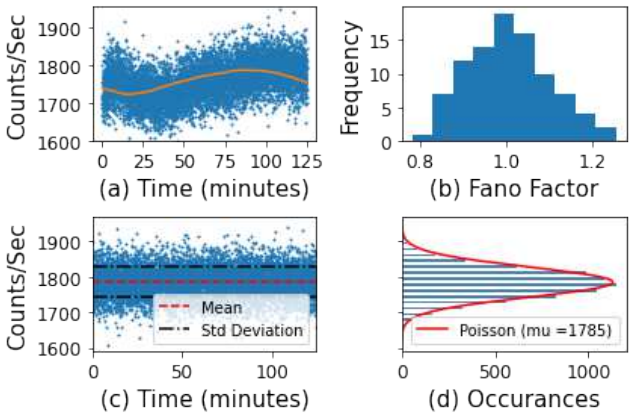

FIG. 3: Analysis of coincidence data obtained in a laboratory setting. (a) Raw coincident event rate and the moving average of the data points (red line) indicate the presence of a low frequency component to the noise. (b) Histogram of Fano factors taking 200 point blocks of the data, in which Poisson statistics are evident. (c) The same data after removing low frequency components by Fast Fourier Transform (FFT) filtering. (d) The filtered coincidence data fit to a Poisson distribution (red curve), indicating the remaining fluctuations are consistent with shot noise.

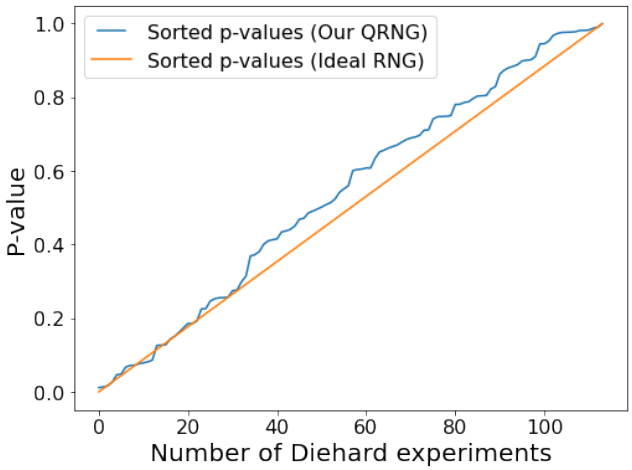

FIG. 4: Evaluating the (statistical) randomness of bits produced by our QRNG. Data generated in laboratory setup passes all tests in the "Dieharder" suite (i.e. $0.01 < p < 0.99$), illustrated here in the form of the KS test [18] (blue line) alongside a hypothetical ideal randomness source (orange line). This qualitative test sorts p values and plots them alongside values uniformly distributed over the interval [0,1].

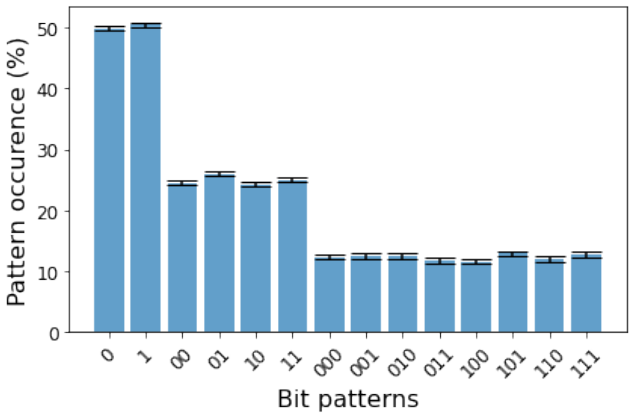

FIG. 5: Analysis of 66 runs containing total 16896 bits generated in orbit. For a limited data set of this size, tests such as "Dieharder" provide little meaningful insight. Instead, it is useful to compute the relative frequency of occurrence of all binary sub-strings of length $1, 2, 3, \ldots$ (the so-called Borel normality condition [25]). This analysis indicates a uniform distribution within error bars limited by finite sample size.

close to the theoretical ideal curve.

III. EXPERIMENT IN ORBIT

The experiment is repeated on-board SpooQy-1, after deployment in Low Earth Orbit. Due to the limited duty cycle of satellite operations and communication bandwidth we are restricted to retrieve at most 256 random bits per trial. It is non-trivial to analyze the randomness of such small datasets, for example, the "Dieharder" test is unsuitable [27]. However, one may estimate the quality of randomness of such short sequences of bits by observing the frequency of occurrence of sub-strings of a particular length (namely the Borel normality condition) [25], with a perfectly random sequence expected to produce a uniform distribution for each length. Figure-5 shows an analysis of 16896 random bits (i.e. the result of 66 trials), with the relative frequency matching this expectation. For example, asymptotically the occurrence of both 0 and 1 should be 50%, and the occurrence of each of the strings $00, 01, 10$, and 11 should be 25%. In our analysis of 66 trials, the occurrence of 0 and 1 is $49.88(37)\%$ and $50.50(37)\%$ respectively. The sequences $00, 01, 10$, and 11 were observed with frequencies $24.55(43)\%$, $26.06(47)\%$, $24.31(45)\%$, and $25.07(46)\%$ respectively.

IV. PROTOTYPE RANDOMNESS BEACON

A randomness beacon is a public, periodically updated source of randomness provided as a resource for a variety of tasks which require a random input [12]. The beacon publishes "pulses" of random bits on a pre-defined schedule, which are typically broadcast over the internet.

We implemented a prototype randomness beacon with a 24 hour refresh interval on-board the nanosatellite SpooQy-1, with the goal of demonstrating the feasibility of distributing such a beacon to off-grid infrastructure. There are a few established functionality principles that a randomness beacon must satisfy in order to be useful [12]. These include the signing of each "pulse" using a public key traceable to the beacon originator, in order that the provenance of the beacon pulse can be confirmed. Pulses must also bear references to their parent in order to facilitate verification of the beacon's integrity. While these features should be straightforward to implement on a dedicated satellite, SpooQy-1's primary mission objectives laid stringent resource constraints on the QRNG subsystem. However, we were able to reinforce several standard elements of the satellite's on-board radio to meet these requirements.

The on-board radio (Nanocom AX100, GOMspace) broadcasts a beacon signal at 30 second intervals, and is able to contain a simple data structure consisting of up to 256 generated random bits. The radio implements a hash-based message authentication code (HMAC), linking beacons to the satellite's private key [28]. Alongside a timestamp, our data structure includes the current randomness beacon data in the form of 256 bits of full-entropy randomness. As computing a hash of the previous beacon data would be too computationally expensive for our highly constrained platform, we opt instead to include the full 256 random bits from the previous beacon, satisfying the requirement for linking to previous pulses.

The satellite beacon is encoded using a proprietary data format, which can be decoded by the GOMspace GS100 ground station receiver [29]. Beacons were recorded at two ground-stations, located at Windisch (Switzerland) and on the National University of Singapore campus (Singapore). As our satellite was deployed from the ISS (International Space Station) orbit (inclination 51.6°, period $\sim$90 minutes), we typically observe six passes per day over the Switzerland site, and up to four passes over the Singapore site. Since the two ground stations are in different time zones, it yields a possibility for us to receive the same beacon at two different stations approximately 10 times in 24 hours. Ground track, locations of our ground stations and randomness beacons received by the ground stations are shown in Figure 6.

As micro-satellite based broadband internet proliferates [30], there may be an increased demand for satellite based cryptographic infrastructure of this sort. To be truly useful, an orbital randomness beacon would require a higher refresh rate than demonstrated in this work (for example, the NIST beacon [12] updates every 60 s), robust cryptographic authentication and rigorous linking of sequential pulses [31]. While it was not possible to implement all of these on SpooQy-1, we believe that our proof of concept demonstration shows that such beacons can be hosted on-board low-resource satellites using existing technologies.

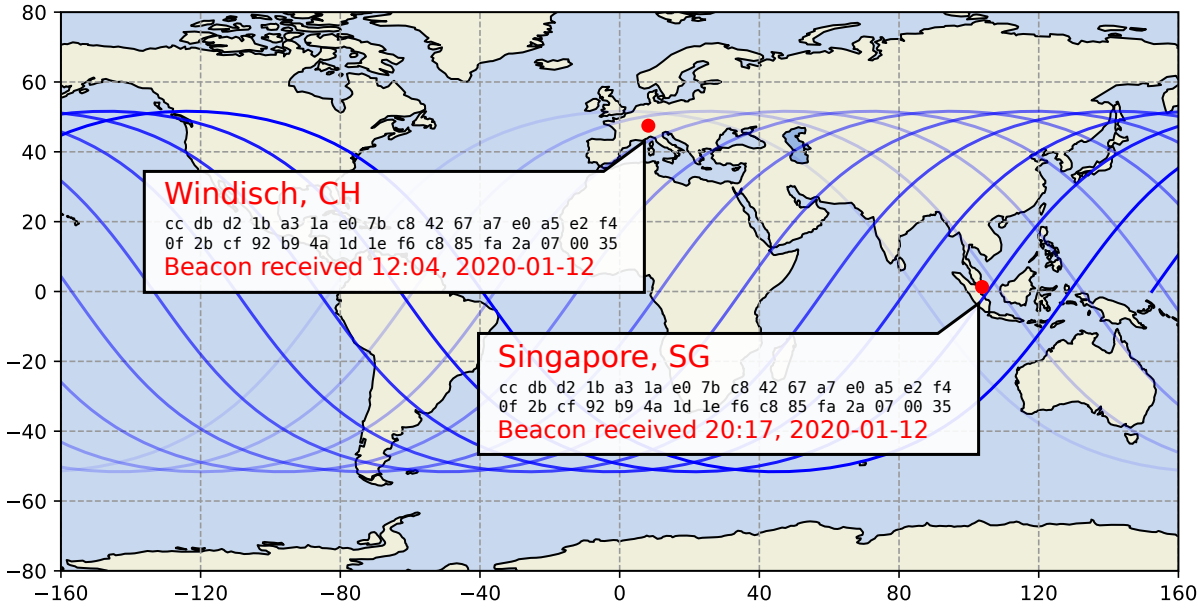

FIG. 6: Demonstration of a prototype orbiting randomness beacon. The ground track of our satellite is plotted against the world map, indicating the locations of our ground stations in Windisch (Switzerland) and Kent Ridge (Singapore). With an inclination of 51.6° and orbital period ∼90 minutes, the satellite is able to communicate with both ground stations 10 times within a 24 hour period. As our prototype randomness beacon updates every 24 hours, we are able to confirm the reception of identical beacons at both locations.

V. CONCLUSION

In conclusion, we have implemented a quantum random number generator on-board an orbiting nanosatellite. As the entropy is derived from an entangled photon source, it may in future be possible to certify the quantum origin of the bits via the successful violation of the CHSH inequality.

As a proof of concept we demonstrate that quantum random number beacons can be implemented on-board nanosatellites using existing technologies. The burgeoning flourish of satellite based tenchnologies in broadband network, cryptographic infrastructure reinforces the necessity of establishing an orbiting public randomness beacon that leads to contribute in other promising applications such as in public lottery, voting protocols, contract signing and zero knowledge proofs.

ACKNOWLEDGEMENTS

This research was carried out at the Centre for Quantum Technologies, National University of Singapore, and supported by the National Research Foundation, Prime Minister's Office, Singapore under the grant NRFCRP12-2013-02.

[1] W. Schindler, in *Cryptographic Engineering* (Springer, 2009) pp. 5–23.
[2] W. K. Hastings, Biometrika **57**, 97 (1970).
[3] L. Bello, *Debian open ssl predictable random number generator*, Tech. Rep. (Technical report, Debian. org, 2008).
[4] B. Schneier, *Schneier's Cryptography Classics Library: Applied Cryptography, Secrets and Lies, and Practical Cryptography* (Wiley Publishing, 2007).
[5] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, Physical Review X **4**, 031056 (2014).
[6] L. Shen, J. Lee, J.-D. Bancal, A. Cerè, A. Lamas-Linares, A. Lita, T. Gerrits, S. W. Nam, V. Scarani, C. Kurtsiefer, *et al.*, Physical review letters **121**, 150402 (2018).
[7] Y. Shi, B. Chng, and C. Kurtsiefer, Applied Physics Letters **109**, 041101 (2016).
[8] M. Herrero-Collantes and J. C. Garcia-Escartin, Reviews of Modern Physics **89**, 015004 (2017).
[9] "Quantum random number generators: A ten-year market assessment," (2021), report IQT-QRNG-0121, Inside Quantum Technology.
[10] A. Villar, A. Lohrmann, X. Bai, T. Vergoossen, R. Bedington, C. Perumangatt, H. Y. Lim, T. Islam, A. Reezwana, Z. Tang, *et al.*, Optica **7**, 734 (2020).
[11] C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing **175**, 8 (1984).

[12] J. Kelsey, L. T. Brandão, R. Peralta, and H. Booth, *A reference for randomness beacons: Format and protocol version 2*, Tech. Rep. (National Institute of Standards and Technology, 2019).

[13] G. Wang and M. Nixon, in *2020 IEEE International Conference on Blockchain (Blockchain)* (IEEE, 2020) pp. 442–449.

[14] N. Hamamoto, Y. Arimoto, Y. Hashimoto, T. Ide, and M. Sakasai, in *Proceedings of 1994 3rd IEEE International Conference on Universal Personal Communications* (IEEE, 1994) pp. 418–422.

[15] M. Allery and J. Ward, in *3rd European Conference on Satellite Communications-ECSC-3, 1993.* (IET, 1993) pp. 230–235.

[16] A. Hevia and C. Gómez, Communications of the ACM **63**, 49 (2020).

[17] R. G. Brown, D. Eddelbuettel, and D. Bauer, Open Source software library, under development (2013).

[18] F. J. Massey Jr, Journal of the American statistical Association **46**, 68 (1951).

[19] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Physical Review A **87**, 062327 (2013).

[20] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Physical review letters **23**, 880 (1969).

[21] K. Durak, A. Villar, B. Septriani, Z. Tang, R. Chandrasekara, R. Bedington, and A. Ling, in *Advances in Photonics of Quantum Computing, Memory, and Communication IX*, Vol. 9762 (International Society for Optics and Photonics, 2016) p. 976209.

[22] A. V. Zafra, *Building entangled photon pair sources for quantum key distribution with nano-satellites*, PhD dissertation, National University of Singapore (2019).

[23] D. C. Burnham and D. L. Weinberg, Physical Review Letters **25**, 84 (1970).

[24] L. Mandel, Proceedings of the Physical Society **74**, 233 (1959).

[25] C. ian Caludet, in *Developments in Language Theory* (World Scientific, 1993) p. 113.

[26] K. Rajdl, P. Lansky, and L. Kostal, Frontiers in Computational Neuroscience **14** (2020).

[27] P. L'Ecuyer and R. Simard, ACM Transactions on Mathematical Software (TOMS) **33**, 1 (2007).

[28] *Ax100–Long-range software configurable VHF/UHF transceiver*, GOMSPACE (2016).

[29] "Nanocom gs100 datasheet," GOMSPACE; gs-ds-nanocom-ax100-3.3.docx3.3; 12 August 2016.

[30] I. Levchenko, S. Xu, Y.-L. Wu, and K. Bazaka, Nature Astronomy **4**, 1012 (2020).

[31] M. J. Fischer, M. Iorga, and R. Peralta, in *Proceedings of the International Conference on Security and Cryptography* (IEEE, 2011) pp. 434–438.