Quantum Random Number Generation

Neil McBlane

Master of Science

Informatics

School of Informatics

University of Edinburgh

2020

Abstract

Randomness is a vital resource in modern science and society: from machine learning to cryptography, random numbers play a key role in all manner of decision making processes. Quantum physics offers the only source of true, fundamental randomness, and quantum random number generation is one of the best developed areas in quantum computing.

This project provides a broad-strokes study of quantum protocols for random number generation, with a focus on providing non-experts with an understanding of their relevance and requirements for near-term implementation. Its key contributions are the production of four submissions to the Quantum Protocol Zoo [1], the development of a generic experimental framework for the quantum network simulator SimulaQron [2] and simulation of the randomness expansion protocol of Pironio *et. al.* [3] therein, and the proposal of a simplified Mermin-Peres Magic Square game [4].

Acknowledgements

First and foremost, I would like to thank Dr Petros Wallden for his continued and invaluable supervision throughout this project. I would like to thank my family for their unwavering support for the entirety of my university career, and in particular for their sharp eyes for a typo.

Finally, I would like to thank my friends, without whom I would not have enjoyed this journey as much as I have.

Table of Contents

Chapter 1

Introduction

Randomness is a fundamental resource across many fields of computer science and beyond. From machine learning and cryptography to deciding who gets the last biscuit, randomness is employed in making decisions without bias.

In some cases, only the appearance of randomness is required. Pseudorandom number generators (PRNGs) produce a series of numbers which appear to follow some probability distribution, but which are algorithmically generated and therefore fully predetermined. PRNGs are simple and fast, and are used extensively for tasks such as taking an unbiased sample from a dataset. Their determinism also offers the advantage of perfect reproducibility. Under certain conditions PRNGs can prove to be extraordinarily expensive: a lottery whose numbers are deterministically generated would have an unsustainably high win rate. More crucially, many protocols for encryption rely on randomness to make their output unpredictable [5].

True random number generators (TRNGs) create non-deterministic randomness by exploiting the complexity of physical processes. The coin flip is one such method, though modern systems circumvent the tedium of flipping billions of coins by using rapidly shifting processes like atmospheric noise [6]. There is a fundamental problem with many TRNGs, however: the randomness observed is often merely a reflection of an incomplete understanding of the system. In theory, the outcome of a coin flip could be perfectly predicted if a powerful enough model was constructed. Quantum mechanics, on the other hand, has non-determinism at its very core. Quantum random number generators (QRNGs) are a subset of TRNGs which exploit quantum physical systems to generate randomness. One could go so far as to claim they are the only source of true randomness.

Quantum random number generation is one of the most mature branches of quan-

tum computing. The earliest QRNGs, based on radioactive decay, date back to 1956 [7] and the field has since developed to include commercially available hardware [8] and online resources [9]. Moreover, recent theorems [10] have demonstrated that it is possible to use quantum-based protocols to augment the output of sources in a manner that is not possible classically. As quantum technology advances, it is likely that the implementation of such protocols will be possible in the near term.

This report outlines a study of protocols for random number generation, split into three key sections. Prior to the study, a selection of relevant topics in random numbers, quantum mechanics and quantum cryptography is introduced. As the ramifications of QRNGs span various fields - from quantum physics to cryptography - the first section of the study performs a critical and comparative review in a manner which aims to "translate" from the mathematical language of physics journals to something more familiar to the non-expert computer scientist. In this section, the format, target audience and style of the review is outlined and justified. To illustrate their characteristic behaviour and response to parameter choice, the second section examines simulations of a selection of protocol elements. An outline and justification of the software used is provided here. The third section proposes a protocol adaptation which aims to lower the technological barrier for implementation. Finally, a closing discussion is provided, highlighting the potential areas for future work.

1.1 Contributions

The contributions of this project to the field are:

- Non-expert summaries of three protocols for quantum random number generation, and a non-expert summary of quantum random number generation in general. All are proposed for addition to the Quantum Protocol Zoo [1].
- Simulation of key elements of protocols by Pironio *et. al.* [3] and Brando *et. al.* [11], including characterisation of behaviour under a range of protocol parameters, all using the SimulaQron [12] library in Python.
- Development of a framework for performing efficient experimentation of general protocols simulated with the SimulaQron library.
- Development of a simplified Mermin-Peres Magic Sqaure [4] quantum game, proposed for implementation on simpler technology than is required for the original game.

Chapter 2

Background

Given the fundamental unpredictability of quantum random number generators (QRNGs), much of the interest in the area comes from an intersection of the fields of quantum computing and cryptography (in an emerging field known as quantum cryptography, neatly). It is therefore worthwhile developing a baseline understanding of the properties of random numbers, their sources and how they relate to cryptography, and some basic properties of quantum mechanics which have significant ramifications for the field.

As this report focuses on protocols for random number generation, and not the generators themselves, an understanding of quantum physics at the level needed to construct full-scale quantum systems is not required. For a more in-depth comparison of the physical systems used to construct QRNGs see the review of Herrero-Collantes and Garcia-Escartin [13].

2.1 Randomness

Random numbers and their sources come in a range of forms, each of which have their own properties and suitable areas of application. In order to best understand the importance of QRNGs and the theory behind their protocols, it is therefore key to gain an understanding of the context in which they are found and the metrics used to describe them.

2.1.1 Sources of Randomness

Pseudorandomness Pseudorandom number generators (PRNGs) are the randomness source with which most will be familiar. In simple summary, these can be thought of as functions which take as input a number (the seed) and iteratively use deterministic operations to produce a series of numbers which appear to follow a given probability distribution. Significantly more detail can be found in Vadhan's monograph [14]. PRNGs are used by languages such as Python [15] and Java [16] when function calls to native random number generators are made.

Given the seed, the following sequence of numbers is entirely predetermined, so by definition these numbers are not random. This is not a problem in the cases where we may want to select a uniformly distributed subset of our dataset - a common practice in methods such as stochastic gradient descent and Monte-Carlo integration [17] - but makes them wholly unsuitable in adversarial contexts. Whilst security assurances for PRNGs can be made to some degree [18], quantum mechanics can do better.

True Randomness True random number generators (TRNGs) offer an alternative to algorithmically generated 'randomness'. For example, the Linux operating system extracts randomness from the unpredictable alignment of user inputs - keystrokes, mouse movements, and so on - with various system actions and timers [19]. Atmospheric noise [6] and other complex or chaotic physical systems have also been used to generate random numbers.

The benefits of quantum random number generators (QRNGs) in comparison to these more traditional methods can be understood from multiple perspectives. QRNGs provide security that cannot be broken by anyone, ever - no matter how powerful the computations they can perform. In addition, as unpredictability sits within the core of quantum mechanics, its simplest building blocks can be used to produce randomness - reliance on system complexity is no longer needed.

2.1.2 Measuring Randomness in Theory

The ideal source is uniformly random - every random number is equally likely to be the next one to come out - but most of the time this is not the case. Various metrics have therefore been defined to quantify the properties of random number sources.

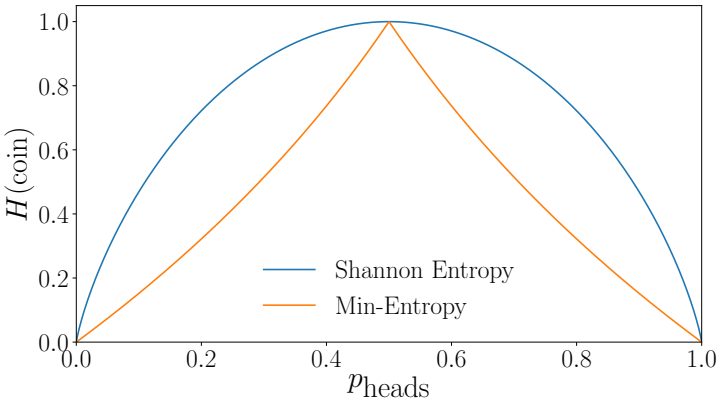


Figure 2.1: The Shannon entropy and min-entropy for a biased coin for the full range of probabilities for producing heads.

Entropy For a source X with distribution p_X which produces numbers x from some discrete alphabet $\mathcal{A}$, where each x has a probability $p_X(x)$ of being produced per query to the source, the Shannon entropy [20] is defined:

$$H(X) = -\sum_{x \in \mathcal{A}} p_X(x) \log_2 p_X(x) \tag{2.1}$$

One interpretation of Shannon entropy is that it quantifies the average 'surprise' at the output of a source. As Figure 2.1 demonstrates, if a coin is biased towards or away from heads its entropy decreases: the preferred outcome is likely to happen more often and an observer will be less surprised when it does. Correspondingly, Shannon entropy is maximal when every outcome is equally likely (i.e. for a uniform source).

An alternative form of entropy is the min-entropy, defined:

$$H_{\min}(X) = -\log_2 \left(\max_{x \in \mathcal{A}} p_X(x) \right) \tag{2.2}$$

If the probability distribution of some source was known and an adversary wanted to predict the output, the best strategy would be to go for the most likely outcome each time. The min-entropy therefore provides a measure of how 'guessable' a source is. In addition, for all sources $H_{\min}(X) \leq H(X)$ [21], so the min-entropy provides a more conservative estimate (it is in fact the worst-case estimate) of a source's randomness.

In cryptography, security in the worst case is sought, and an opponent playing the optimal strategy (i.e. guessing the most likely output) is a possible adversary. Thus min-entropy is the metric used in discussion of randomness sources.

Conditional Entropy It is important to consider how the information available to an adversary may impact their ability to guess a generator's output. For example, a TRNG's output may be influenced by its operating temperature. Defining E to be all relevant information available to an adversary, the conditional min-entropy of a source is thus defined:

$$H_{\min}(X|E) = -\log_2\left(\max_{x\in\mathcal{A}} p_X(x|E)\right) \tag{2.3}$$

If the information E is available, a source X is said to be a k-source if $H_{\min}(X|E) \geq k$.

Santha-Vazirani Sources A specific subset of min-entropy sources is also of interest in this project: the Santha-Vazirani (SV) source [22] is defined:

$$\frac{1}{2} - \delta \leq p_X(x)(x_i = 1|x_1, x_2, \ldots, x_{i-1}) \leq \frac{1}{2} + \delta \tag{2.4}$$

Where $p_X(x)$ is the probability distribution of source X, x_i is the i-th bit to be extracted from the source, $x_1, x_2, \ldots, x_{i-1}$ are all the bits that have been extracted so far and $\delta \in [0, 1/2]$ is the bias.

2.1.3 Measuring Randomness in Experiments

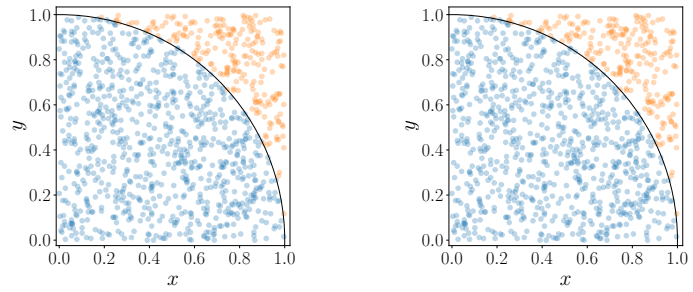
For a finite string of random bits, no test exists to conclusively verify that it has been produced by a truly random source [13]. The best that can be done is verification that the output of a given generator at least 'looks' random - i.e. it has properties that one would expect from a random source. In each of the tests described below, generator output is assumed to be represented as a bit string (e.g. "1001011").

Basic Measures Jennewein *et. al.* [23] introduce a set of rough tests for randomness. Although not rigorous (they lack any formal notion of sufficiency), they are a useful initial benchmark.

For a uniform source, the number of zeros and ones in a produced bit string should be roughly equal, and thus a simple test is whether:

$$\sum_{i}^{n} x_i \approx \frac{n}{2} \tag{2.5}$$

Where $x = (x_1, x_2, \ldots, x_n)$ is generated by source X. Multiple tests are always needed as strings like "010101010101" or "000000111111" do not intuitively seem random, but would pass such a test perfectly.



(a) PRNG, $\pi \approx 3.23046875$ (b) QRNG, $\pi \approx 3.15234375$

Figure 2.2: Monte-Carlo estimation of π using 2048 bytes from (a) Python's pseudorandom number generator [15] and (b) from the ANU's quantum random number server [9], paired and mapped to the 1024 datapoints in the range $[0,1]^2$. Both methods provide a good estimation of 3.14159265, the true value to as many significant figures.

The outputs of random sources should be uniformly distributed across all possible outputs, therefore if a string is divided into a series of substrings of length n then these should be uniformly distributed across the alphabet $\mathcal{A} = \{0,1\}^n$. Each substring can be cast as an n-bit integer then divided by 2^n to give a set of numbers in the range $[0,1]$. The ratio of the area of a quarter of the unit circle to the unit square is given by:

$$\frac{\text{quarter unit circle}}{\text{unit square}} = \frac{\pi}{4} \tag{2.6}$$

For a uniform 2D distribution of data points, a fraction $\pi/4$ of the total number should fall within a Euclidean distance of one from the origin. Pairing off the generated numbers into a set of data points and determining this fraction thus allows for one to (roughly) test the uniformity of a string as bias may be manifest as an increase or decrease in this ratio (Fig.2.2).

Substrings can also be used to estimate Shannon entropy H (Eq.2.1) and min-entropy $H_{\min}$ (Eq.2.2). For a uniform source U with alphabet $\mathcal{A} = \{0,1\}^n$, the probability of any given string s being produced is $P_U(s) = 1/2^n$ and so $H(U) = H_{\min}(U) = n$. For a given string x from source X split into substrings of length n, the probability of each substring in $\mathcal{A}$ (i.e. $p_X(s)$ for $s \in \mathcal{A}$) can be estimated empirically as:

$$p_X^{\text{est}}(s) = \frac{N(s)}{|\mathcal{A}'|} \tag{2.7}$$

Where $N(s)$ is the number of times s appears as a substring of x and $|\mathcal{A}|$ is the cardinality of the alphabet (i.e. the total number of substrings possible). From these values,

the Shannon entropy and min-entropy can be trivially estimated and compared to the expected value for a uniform source.

Randomness Test Suites Formal verification of (the appearance of) randomness requires the assessment to be stated as a hypothesis test [24], defining:

- The null hypothesis ($H0$) - the string being tested could be random.
- The alternative hypothesis (Ha) - the string being tested cannot be random.

Multiple suites exist [25, 26, 27, 28] which have constructed a series of such hypothesis tests. Given an input string, these suites step through a series of features (e.g. those described above) and pose the question: what is the probability that a truly random string would return this value? If the probability is within some threshold (defined for each test) then the null hypothesis can be accepted.

For brevity, only the NIST suite was run during this project. A full outline of the tests within the suite and guidelines for use can be found in [25].

2.2 Quantum Mechanics

Quantum mechanics is a rich and complex field of mathematics which underpins quantum physics. Fortunately, as non-determinism sits at its core, a comprehensive understanding is not required to explore its application to the generation and processing of random numbers. As cryptography is a key application for QRNGs, it is also important to explore the facets of quantum mechanics that have implications here. A detailed introduction to quantum mechanics with a view to quantum computation and information can be found in the textbook of Neilsen and Chuang [29], and a more general and comprehensive introduction in the textbook of Shankar [30].

2.2.1 Qubits

In general, quantum systems that can exist in d different discrete states are described by a d-dimensional Hilbert space: a form of complex vector space which satisfies a number of techincal properties [30]. A qubit is a unit vector in the Hilbert space of any quantum system for which $d = 2$.

Single Qubits To describe any object within a vector space, a set of orthonormal basis vectors is required. The 'computational' basis appears commonly in quantum computing, with basis vectors defined:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.8}$$

Where $|0\rangle$ is known as a ket and is used to represent a vector in some Hilbert space. A general qubit can therefore be described as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{2.9}$$

Where α and β are complex numbers and $|\alpha|^2 + |\beta|^2 = 1$. Complementary to the ket is the bra, which represents the conjugate transpose:

$$\langle\psi| = \alpha^*\langle 0| + \beta^*\langle 1| = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \tag{2.10}$$

Equivalently, the 'Hadamard' basis can be used to describe the qubit. This has orthonormal basis vectors:

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \qquad |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) \tag{2.11}$$

The corresponding qubit representation is:

$$|\psi\rangle = \alpha'|+\rangle + \beta'|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} \alpha' + \beta' \\ \alpha' - \beta' \end{pmatrix} \tag{2.12}$$

Where again $|\alpha'|^2 + |\beta'|^2 = 1$. Indeed any pair of orthonormal vectors can be used as a basis to describe a qubit.

Multiple Qubits It is straightforward to extend these concepts to multiple qubit systems. Each qubit occupies its own (potentially correlated) Hilbert space, and these are combined to form a product space using the tensor product. For n qubits in states $|\psi\rangle_1$, $|\psi\rangle_2$ up to $|\psi\rangle_n$ respectively, their combined state is described by:

$$|\Psi\rangle = |\psi\rangle_1 \otimes |\psi\rangle_2 \otimes \ldots \otimes |\psi\rangle_n \tag{2.13}$$

Where unambiguous the '$\otimes$' is often dropped for brevity and the two states combined into a single ket, for example:

$$|+\rangle_A \otimes |+\rangle_B = \frac{1}{2}\big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\big) \tag{2.14}$$

Measurement Choice of basis is closely linked to measurement in quantum mechanics. Observable quantities are described by Hermitian matrices (i.e. matrices for which the conjugate transpose is equal to the matrix itself), which by definition have real eigenvalues. The corresponding eigenvectors form an orthonormal basis with which a qubit can be described.

For an observable quantity, described by Hermitian matrix M, which has eigenvalues λ_1 and λ_2 and corresponding eigenvectors $|v_1\rangle$ and $|v_2\rangle$ a general qubit can be described:

$$|\psi\rangle = \alpha|v_1\rangle + \beta|v_2\rangle \tag{2.15}$$

When the measurement corresponding to this observable is made, either λ_1 or λ_2 will be seen with probabilities $|\alpha|^2$ and $|\beta|^2$ respectively - this is the fundamental source of non-determinism in quantum mechanics. Crucially, the qubit will also 'collapse' into the state $|\psi\rangle = |v_1\rangle$ if λ_1 is observed or $|\psi\rangle = |v_2\rangle$ if λ_2 is observed. In other words, the act of observation has a physical effect on the system.

Consider the so-called Pauli-X, Pauli-Y and Pauli-Z matrices, respectively defined:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.16}$$

These all have eigenvalues of ± 1. The eigenvectors of X and Z are the Hadamard and computational basis vectors respectively (Y will be of use at a later stage).

Consider a qubit in the state $|0\rangle$. If measured in the Z (computational) basis, the eigenvalue $+1$ and eigenstate $|0\rangle$ will be returned with certainty. If instead measured in the X (Hadamard) basis, either of ± 1 and $|\pm\rangle$ will be returned with equal probability. In other words, measurement of $|0\rangle$ in the X basis results in a perfect random number generator. Moreover, the physical state of the system has been observably changed by the measurement: if measured again in the Z basis, $|0\rangle$ would be returned with $1/2$ probability.

Entanglement It is possible to construct states which cannot be written as the tensor product of two separate states as above. These are said to be entangled, and have a

number of interesting properties. Consider the so-called EPR pair:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) \tag{2.17}$$

A strong correlation exists between the two qubits in this system. When measured in the computational basis, initially each qubit has equal probability of collapsing to either of the basis states. However, once the first of the pair has been measured, the second must necessarily be in the same basis state. This is in contrast to the state $|+\rangle_A \otimes |+\rangle_B$ described before, where the original product state contains within its superposition the possibility for each qubit to collapse down into opposing basis states.

Strikingly, the influence that measurement of one qubit has on the other is instantaneous: even if the pair are separated by many light-years in distance. Quantum mechanics is therefore said to be non-local. Whilst this may seem at odds with the physical speed limit imposed by relativity, reconciliation comes in the fact that no information can be transmitted this way. To a pair of parties stationed at either end of this distance, there is no way to know if the measurement result obtained from their qubit was predetermined by the measurement of their partner or was completely random until a classical message has been sent by the partner to inform them (which is so constrained by the speed of light). In other words, no signals can be transmitted faster than the speed of light.

2.2.2 Density Matrices

A more general way to describe quantum mechanics is through the formalism of density matrices. Unlike the so-called pure states described above, they allow for 'ensembles' containing a mixture of classical and quantum uncertainty. For a general state $|\phi\rangle$, the density matrix is defined:

$$\rho = |\phi\rangle\langle\phi| \tag{2.18}$$

Ensembles Compare the scenario where a qubit is prepared to be in the state $|+\rangle$ versus the scenario where with equal probability it is prepared to be in the state $|0\rangle$ or $|1\rangle$. As already seen, measurement outcomes in the Z basis for the former can be described as $(|0\rangle + |1\rangle)/\sqrt{2}$, but there is no equivalent notation for the latter as no superposition is taking place; the outcome is entirely predetermined by the party preparing the states.

In general, for a set of quantum states $|\psi_i\rangle$ where $i \in \{1 \ldots n\}$ and the i-th state is prepared with probability p_i, an ensemble is defined $\{p_i, \rho_i\}$ where ρ_i is the density matrix of the i-th state. The density matrix of an ensemble is defined:

$$\rho = \sum_i p_i \rho_i = \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{2.19}$$

Comparing the two scenarios described above, for example:

$$\rho_1 = |+\rangle\langle+| = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|0\rangle\langle 1| + \frac{1}{2}|1\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \tag{2.20}$$

$$\rho_2 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \tag{2.21}$$

Partial Trace Density matrices also provide a way to unpick entangled states into representations for their respective qubits. Consider the EPR pair described above, with one qubit held by Alice and the other by Bob. By definition it is not possible to represent this as the tensor product of two independent qubit systems. Expressing it instead as a density matrix:

$$\rho_{AB} = |\phi^+\rangle\langle\phi^+| = \frac{1}{2}\big(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\big) \tag{2.22}$$

The partial trace operator allows for the density matrix describing Alice's qubit only to be extracted from ρ_{AB} by "tracing out" Bob's components of the system. For some qubit basis $\{m_\alpha, m_\beta\}$, the partial trace of system i over an n-qubit system ρ corresponds to the operation:

$$\begin{aligned}\rho_{n/i} = \mathrm{Tr}_i(\rho) = {} & (I_1 \otimes \ldots \otimes \langle m_\alpha|_i \otimes \ldots \otimes I_n)\rho(I_1 \otimes \ldots \otimes |m_\alpha\rangle_i \otimes \ldots \otimes I_n) \\ & + (I_1 \otimes \ldots \otimes \langle m_\beta|_i \otimes \ldots \otimes I_n)\rho(I_1 \otimes \ldots \otimes |m_\beta\rangle_i \otimes \ldots \otimes I_n)\end{aligned} \tag{2.23}$$

Where I is the identity matrix, subscripts denote on which qubit in the system the operation is applied and $p_{n/i}$ is the n qubit system with the i-th qubit removed. As bases are related by unitary rotations and the trace is invariant under cyclic permutations, this operation is actually basis-invariant.

Applying the partial trace to the EPR pair shared by Alice and Bob, and choosing the computational basis for convenience, a description for the state held by Alice (ρ_A)

can be recovered:

$$\begin{aligned}\rho_A = \mathrm{Tr}_B(\rho_{AB}) &= (I_A \otimes \langle 0|)\rho_{AB}(I_A \otimes |0\rangle) + (I_A \otimes \langle 1|)\rho_{AB}(I_A \otimes |1\rangle) \\ &= \frac{1}{2}\big(\,|0\rangle\langle 0| + |1\rangle\langle 1|\,\big)\end{aligned} \tag{2.24}$$

Since $|0\rangle$ and $|1\rangle$ are orthonormal vectors.

Trace Distance The output of any QRNG may not necessarily be perfectly uniform. It is therefore important to define some metric capable of describing just how far from perfect a given protocol's output is. One such method of doing this is the trace distance, which quantifies distance as the probability that one could make a measurement capable of telling apart two states given the best possible basis for doing so [31].

For a general source X of n-bit numbers with alphabet $\mathcal{A}$ encoded as n-qubit systems $|x\rangle$, each of which occurs with probability $p_X(x)$, the output quantum state can be described as:

$$\rho_X = \sum_{x\in\mathcal{A}} p_X(x)\,|x\rangle\langle x| \tag{2.25}$$

For a uniform source U, each number x occurs with equal probability so the corresponding state becomes:

$$\rho_U = \frac{1}{|\mathcal{A}|}\sum_{x\in\mathcal{A}} |x\rangle\langle x| \tag{2.26}$$

The trace distance of these two states is defined:

$$D(\rho_X,\rho_U) = \frac{1}{2}\mathrm{Tr}\Big[\sqrt{A^\dagger A}\Big] \tag{2.27}$$

Where $A = (\rho_X - \rho_U)$. This allows for a simple way to quantify the uniformity of a given QRNG's output: a state ρ_X is ε-close to uniform if $D(\rho_X,\rho_U) \leq \varepsilon$.

2.3 Quantum Cryptography

Having introduced a number of key concepts in quantum mechanics, their relevance to cryptography - and in particular the role that random numbers play therein - can now be outlined. Further detail and a broader scope can be found in Vidick's lecture notes [31].

2.3.1 No Cloning Theorem

The physical effect of measurement on quantum states means that interception of a quantum message may leave a clear footprint on the quantum state. An obvious solution would be for an adversary to make their own copies of the message so as not to alert anyone downstream of their tampering.

The no cloning theorem [29] proves that there is no possible way for an adversary to make a copy of an unknown state. The proof is straightforward but not particularly illuminating in this context and so is omitted.

2.3.2 Side Information

In cryptography, privacy refers to the idea that some piece of information is secret to a specific set of parties: the ideal password is private in that it is only known by the intended users of an account and the service to which this account would like to connect. In the context of quantum cryptography, this translates to information about a quantum state being held only by the desired set of parties. Entanglement provides a subtle path for information to 'leak' out of a system.

Consider the QRNG X described in Sec.2.2.2. If some entanglement exists between the encoding qubits and their environment, then measurements made by an adversary on the environment may compromise the privacy of the generated numbers. This can be captured mathematically by combining the QRNG state density matrix $|x\rangle\langle x|$ with the correlated environment state $\rho_E(x)$ via the tensor product. If x is generated with probability $p_X(x)$, the system corresponds to the ensemble:

$$\rho_{XE} = \sum_{x \in \mathcal{A}} p_X(x) \, |x\rangle\langle x| \otimes \rho_E(x) \tag{2.28}$$

With ρ_E as the environment-only portion of the system - i.e $\rho_E = \mathrm{Tr}_X(\rho_{XE})$ - the impact of side information can be quantified using trace distance. The uniform state ρ_U (Eq.2.26) corresponds to the adversary having learned nothing - each possibility is equally likely. Therefore, a generator X is ε-secure against E if:

$$D(\rho_{XE}, \rho_U \otimes \rho_E) \leq \varepsilon \tag{2.29}$$

2.3.3 Monogamy of Entanglement

If entanglement can compromise the privacy of a quantum state, it is important to have some way to tell what entanglements exist within a given system. There is no single metric which can effectively quantify 'entangledness', but it is possible to construct states which are maximally entangled. These have a number of characteristic properties, and vitally if a pair of qubits is maximally entangled they cannot be entangled to any degree with a further qubit - this is the definition of monogamy of entanglement.

Basis Independence Maximally entangled states are perfectly correlated regardless of basis. Compare the EPR state introduced earlier to the so-called GHZ state when each is defined in both the Z and X bases:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) = \frac{1}{\sqrt{2}}\big(|{+}{+}\rangle + |{-}{-}\rangle\big) \tag{2.30}$$

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\big(|000\rangle + |111\rangle\big) = \frac{1}{2}\big(|{+}{+}{+}\rangle + |{+}{-}{-}\rangle + |{-}{+}{-}\rangle + |{-}{-}{+}\rangle\big) \tag{2.31}$$

As long as both qubits of the EPR state are measured in the same basis, they will return the same result. This is only true for any two qubits in the GHZ state if both are measured in the Z basis. In other words, the EPR state is maximally entangled and the GHZ state is not.

Quantum Games Entanglement enables quantum mechanical solutions to mathematical games that are not solvable classically. The CHSH game [32] is one such example. It is played in four steps by three parties - Alice, Bob and a referee:

1. Two independent, uniformly random bits, x and y are generated by a referee
2. x is sent to Alice, y to Bob
3. Alice and Bob, who cannot now communicate, come up with responses a and b respectively and send them to the referee
4. If $x \wedge y = a \oplus b$, the referee announces they have won, otherwise they have lost

Prior to the game, Alice and Bob are free to establish a strategy. Classically, the optimal method is for them to agree on an answer (either both say zero or both say one) and stick to it throughout - this will succeed 75% of the time. If instead they share a maximally entangled state then by agreeing on the correct set of measurement bases it is possible for them to do better. If Alice measures in basis X when $x = 0$ and Z when

$x = 1$, and similarly Bob measures in basis $1/\sqrt{2}(X+Z)$ (i.e. his basis vectors are the eigenvectors of the matrix $1/\sqrt{2}(X+Z)$) when $y = 0$ and $1/\sqrt{2}(X-Z)$ when $y = 1$ then it can be shown [33] that they will win just over 85% of the time. Moreover, since this result relies on the qubits being maximally entangled, it provides another method of verifying that a given system does not have any outside entanglements.

Any real-world implementation will suffer from noise, reducing the strength of the correlation and therefore the success rate. It is not possible to tell if a sub-optimal score is due to intermittent peeking via entanglement or just a consequence of noise, but bounds on the "amount" of entanglement possible can be made [3].

2.3.4 Generating Randomness

Given that games such as those described above require quantum systems to succeed, if certain elements of adversarial interference can be ruled out then it is possible to certify that a given amount of "quantumness" has occurred. For instance, any success rate above 75% (a "super-classical" result) in the CHSH game implies that entangled qubits must have been used some of the time.

As quantum systems are fundamentally non-deterministic, it can therefore be expected that some randomness exists within the results of these games. The utility of this was first noted by Colbeck [10] and has since evolved into formal proofs for various quantum games [3, 34].

The benefit of these methods for producing randomness is that they are device independent - few assumptions are required about the inner workings of the apparatus used for implementation. The complexity of quantum computing makes this a key factor - trust often comes from transparency and so the ability to verify correctness without a detailed understanding of how a device works is vital. Careful construction of protocols and their implementation ensures that experiment results alone are enough to certify the expected process has indeed taken place.

Randomness Extraction Commonly, randomness sources are available which have a high min-entropy but whose output is not uniformly random or is correlated with an adversary. Seeded randomness extractors [35] are classical functions which combine a string x of length n from a k-source X with a uniformly random seed of length d to produce an output which is close to private and uniformly random. Strong seeded randomness extractors do so in a manner that leaves the seed uncompromised, and thus

the final output string can have this appended for additional performance.

Formally [31], a (k,ε)-strong seeded randomness extractor is a function defined:

$$\text{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m \tag{2.32}$$

Such that for a k-source X, any output state $\rho_{\text{Ext}(X,U_d)E}$, where U_d is the uniform source of d-length seeds, is ε-secure against E. The exact relationship between the input values n, k, the required d and the output length m depends on the randomness extractor implementation used. The bounds [36] on these quantities are:

$$d \geq \log(n-k) + 2\log(1/\varepsilon) + O(1) \tag{2.33}$$

$$m \leq k + d - 2\log(1/\varepsilon) + O(1) \tag{2.34}$$

2.4 Related Work

Various reviews of quantum random number generation have been conducted prior to this project [13, 37, 38]. These differ from the research goals of the project in two key aspects. They are written with a predominant focus on the physical processes used for the generation of randomness, touching only briefly on post-processing protocols such as those considered in this project. In addition, as they are published in physics-based journals, the target audience for each is highly disparate from the non-expert computer scientist which this project aims to write for.

At the time of writing, no publications making use of the SimulaQron library [12] to simulate such protocols are apparent. This report therefore aims to provide a sense of the effectiveness of the software in implementing the features required.

Starting with Colbeck in his PhD thesis [10], a large number works have presented protocols for device independent quantum post-processing of random number generators which make use of quantum games. Most commonly, some form of the CHSH game is used to provide guarantees of the quantum nature of any apparatus required. In this manner, protocols have been developed which can output uniformly random and private strings from non-uniform min-Entropy [39, 40] and Santha-Vazirani [11, 41, 42] sources. In addition, protocols which can take as input uniformly random and private strings of a given length and output equivalently random and private but longer strings have been developed [3, 43, 44]. Some authors are making a shift towards realistically implementable protocols. Early iterations often required that

any measurement apparatus be used once then discarded - meaning that the number of devices scaled polynomially (or worse) with the length of input - or that any system used to implement the protocol be completely free of noise [39, 40]. Later works have relaxed these stipulations: offering robustness to noise and requiring only a finite number (i.e. 2, 4, 8 and so on) of devices [3, 11, 41, 43].

The Mermin-Peres Magic Square [4] is another form of quantum game. Recent results have proved its suitability for randomness generation [45]. At the time of writing, formal protocols making use of these are not apparent - likely due to the relative simplicity and effectiveness of the CHSH game. Nevertheless, this prevents a potential avenue for exploration.

Chapter 3

Critical and Comparative Review

The first stage of the project reviewed a selection of protocols for quantum random number generation. In this section, the motivations, intended audience and format of the review will be outlined. In addition, the chosen protocols will be detailed and compared in order to justify their inclusion. A mock-up of the full web-based wiki pages can be found in the project directory.

3.1 Quantum Protocol Zoo

The Quantum Protocol Zoo [1] is a project by Veriqloud [46], the Quantum Internet Alliance (QIA) [47] and various other sponsors. It aims to construct a centralised resource for quantum network protocols, accessible to users across a range of backgrounds. The core philosophy of the Zoo is that each protocol should be written in a manner approachable to software engineers, computer scientists and physicists alike - in contrast to the quantum theory heavy presentation necessary for journal publication.

The Zoo is constructed as a series of functionality and protocol pages. Functionality pages describe a general task (e.g. key distribution) and protocol pages a specific way to perform that task (e.g the BB84 protocol). In addition, a glossary is provided for common technical terms - jargon is avoided where possible but providing an explanation of frequently used concepts mitigates obfuscation.

Each type of page has its own standardised structure. Functionality pages must provide in brief a description of the required task, any available use cases, a list of corresponding protocols and the properties common to each protocol. Further information can be provided if required. Protocol pages provide much more information, including a standardised description of the assumptions made by the protocol, the hardware and

network requirements and an outline of performance. The bulk of each protocol page consists of a non-technical outline of the steps taken in the protocol, a pseudocode outline and a table of notation to connect these concepts together. By summarising each protocol in such a manner, the Zoo aims to 'translate' their description from the language used in physics journals to something more familiar to the potential end users.

3.2 Protocol Reviews

In total, one functionality page and three protocol pages were completed during this project. A mock up of how these would appear on the Zoo is available in the project directory as a pdf, with internal hyper-references and external hyperlinks to mimic full integration with the website.

In order to best convey the steps taken to produce these pages, one will be deconstructed in full. The remainder will be summarised and compared in order to justify their inclusion on the Zoo.

3.2.1 Randomness Expansion

Randomness expansion takes as input a private, uniformly random string and outputs a longer string which is (close to) private and uniformly random. Such a protocol is useful in the case where one already has access to a private source for true randomness, but whose use is prohibitively expensive or whose access is limited.

Both protocols considered are certified (provide guarantees about the security and randomness of their output) and device independent. They need only for the devices to be unable to communicate with each other during any measurements (to guarantee that any correlations are due to entanglement only) and for the devices to have no prior knowledge of the input bit string. In addition, both protocols require a finite number (two and eight respectively) of devices and are noise tolerant. This is important for any realistically implementable protocol.

Finite Randomness expansion The protocol of Pironio *et. al.* [3] enables quadratic expansion (i.e. for an n-bit input, the output length is $\theta(n^2)$) of a private, uniform seed using two measurement devices. Whilst this has since been superseded with developments that are more effective, its relative simplicity aligns well with the philosophy of the Zoo as a pedagogical resource.

After an initial summary and justification, the first section for each protocol is an outline of the assumptions required by any proofs made by the authors:

Assumptions

- Quantum theory is correct.
- The measurement devices do not interact during measurements.
- The measurement devices are not correlated with the input string.
- The adversary does not have access to a quantum memory.

Correctness of quantum theory is a common requirement, occasionally relaxed to the requirement that the only relevant theorem which still holds is that signals cannot be transmitted faster than the speed of light. Such details are minor technicalities, but worth acknowledging due to their commonality. Points two and three have already been discussed above. Point four is a possible weakness in the protocol: it allows an adversary who is capable of maintaining connection between entangled qubits for a long period of time (a challenging task) a potential backdoor into the system.

Following this, an outline of the protocol, free of mathematical detail and with minimal technical language (glossary terms excepting), is constructed:

Outline

In this protocol, Alice has an initial private random string (the seed) and has been provided with two identical measurement devices by Eve. Each of the devices has two settings and can produce two outputs. Prior to beginning the protocol, Alice has to decide with which confidence she would like her output string to be private from Eve, and which strong randomness extractor she would like to perform post-processing with. She then splits her seed into two portions - the sizes of which are determined by the chosen randomness extractor.

Alice then takes two bits from the start of the first portion of her initial string and uses these to choose the settings of her measurement devices (i.e. if the pair is $(0,1)$ then she sets the first device to setting 0 and the second device to setting 1). She prepares an EPR state and shares it across the two measurement devices, then performs measurements using each device with the chosen settings and records the output. She repeats this process until this portion of her input string has been exhausted, resulting in a binary string of recorded outputs of equal length to the input.

Using the input and output strings, Alice estimates the violation of the CHSH inequality her experiment has produced. This allows her to place a bound on the conditional min-entropy of the output string with respect to both the input string and any information Eve may have.

Finally, Alice passes her output string, the second portion of her initial seed and the determined min-entropy bound to a strong randomness extractor to generate a processed string which is (close to) uniform and private from Eve with the confidence specified at the beginning of the protocol. As Alice has kept her seed private throughout and the randomness extractor used is a strong one, she can then simply append her entire seed to the output of the randomness extractor to produce a final expanded string, which is guaranteed to be longer than the seed so long as a super-classical CHSH game has occurred.

Common technical terms which have not yet been added to the glossary are highlighted in red to reflect the convention of the wiki for proposed pages which do not exist. The key goal of this section is to provide some intuition as to how the protocol would be performed and what it can achieve, without the hindrance of complex and often

unfamiliar mathematics. A publication quality outline could benefit from the addition of a high-quality illustration of the process.

In order to link subsequent mathematics with the prior outline, a table of notation is required:

Notation

- n: number of measurement iterations
- x_i: measurement setting for device A on iteration i
- y_i: measurement setting for device B on iteration i
- A_bases: tuple of measurement bases for device A; $\text{A\_bases} = \{X, Z\}$
- B_bases: tuple of measurement bases for device B; $\text{B\_bases} = \{1/\sqrt{2}(X \pm Z)\}$
- a_i: measurement result for device A on iteration i (0 or 1)
- b_i: measurement result for device B on iteration i (0 or 1)
- s: string of measurement basis pairs; $s = (x_1, y_1; \ldots; x_n, y_n)$
- r: string of measurement result pairs; $r = (a_1, b_1; \ldots; a_n, b_n)$
- $\bar{r}$: output string from classical randomness extraction of r
- t: initial private random seed
- u: final randomness expanded string
- $\hat{I}$: experimental estimate of CHSH correlation
- k: lower bound on conditional min-entropy of measurement results r with respect to measurement settings s and any information held by an adversary
- f: function which takes as input a(n estimated) CHSH correlation and returns a per-use lower bound on the conditional min-entropy of the measurement results with respect to measurement settings and any information held by an adversary in the limit of a large number of uses (determined using semi-definite programming in Pironio *et. al.*)
- ε: term to account for finite statistics effects
- α: the chosen confidence with which the returned entropy lower bound is correct
- Ext: strong seeded (classical) randomness extractor

Given the mathematical complexity of the protocols required for quantum random number generation, the notation table appears somewhat clumsy. Nevertheless, such a format befits the pedagogical philosophy of the Zoo. As the protocols come from a range of authors and journals, each is originally published with disparate notation. For clarity, effort was made to ensure the notation be as standardised as possible across each page.

Hardware requirements are a key consideration for pages on the Zoo as it aims to be a resource for any potential end users. An important factor for each is the technological capability of the quantum network to which a user has access. Characteristic stages in the development of a quantum internet have been hypothesised [2], and these are used as the basis for this detail. In addition to the network capabilities, any other hardware and software requirements are outlined:

Requirements

- **Network stage**: Entanglement Distribution
- Random number generator
- Authenticated quantum channel
- Authenticated classical channel

- Hardware:
  - Multi qubit non-separable state preparation
  - Single qubit measurement
  - Single qubit gates

The language used in outlining these hardware requirements is standardised across the entire wiki, with the goal of allowing any interested party to "invert" their search for a protocol by listing the hardware they have available. In this project, all the requirements are essentially identical: an initial source of random numbers is needed to provide a seed, quantum and classical channels for transmitting information and qubits, and the hardware needed to prepare, manipulate and measure entangled states.

Next, the key properties of the protocol are summarised - these concern factors such as performance and security, as well as any features of particular note.

Properties

- Requires only two measurement devices.
- Devices can be untrusted.
- Imposes no constraints on input states or measurements (i.e. Bell inequality tested can be changed from what is specified here).
- Allows for devices to have an internal quantum memory.
- Length of expanded string dependent on magnitude of CHSH correlation (as this tells us how much min-entropy can be contained in the results string) and the choice of randomness extractor (as different constructions have varying degrees of performance).

Building on the outline and notation sections, the final development for communicating the details of a given protocol to a non-expert computer scientist audience is its "translation" to a pseudocode format. Effort is made to construct the pseudocode in a language that abstracts away from the quantum details of the process to underline that it is possible to present the protocols as algorithms approachable to those without experience of quantum theory. A consistent convention is adopted across all protocols created in this project.

Pseudocode

Input: t, α, Ext
Output: u

split t into $t = (t^{(1)}, t^{(2)})$ where $|t^{(1)}|$ and $|t^{(2)}|$ are determined by Ext
$n \leftarrow \left\lfloor \frac{|t^{(1)}|}{2} \right\rfloor$
initialise arrays r, s of length n
for $i \leftarrow 1$ to n **do**
    prepare state $|\Psi^+\rangle$ and share across devices A and B
    $x_i \leftarrow t_i^{(1)}$
    $y_i \leftarrow t_{i+1}^{(1)}$
    $a_i \leftarrow$ measurement result from device A in basis $\mathrm{A\_bases}[x_i]$
    $b_i \leftarrow$ measurement result from device B in basis $\mathrm{B\_bases}[y_i]$
    $s[i] \leftarrow (x_i, y_i)$
    $r[i] \leftarrow (a_i, b_i)$
$\hat{I} \leftarrow 0$

13: **for** $i \leftarrow 1$ to n **do**
14: $x_i, y_i \leftarrow s[i]$
15: $a_i, b_i \leftarrow r[i]$
16: $\hat{I} \leftarrow \hat{I} + \frac{4}{n}(-1)^{x_i \wedge y_i}(-1)^{a_i \oplus b_i}$
17: $\varepsilon \leftarrow 4\sqrt{-\frac{2\sqrt{2}}{n}\ln(1-\alpha)}$
18: $k \leftarrow nf\left(\hat{I} - \varepsilon\right)$
19: flatten r into an array of integers
20: $\bar{r} \leftarrow \mathrm{Ext}(r, t^{(2)}, k)$
21: $u \leftarrow (t, \bar{r})$

Finally, a section containing any further information which may be of use when implementing a given protocol is included. This may outline experimental implementations of the protocol, possible adaptations and any further reading deemed useful for a more advanced understanding.

Infinite Randomness expansion Coudron and Yuen [43] provide a protocol which enables arbitrary expansion of a private uniform seed, with security dependent on the length of the input. Explicitly, after k protocol rounds for a n-bit seed, the output length is a k-high tower of exponentials, defined:

$$\underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2^{\Omega(n^{1/3})}}}}}}}_{k-\text{times}} \tag{3.1}$$

The protocol output is $\exp(-\Omega(n^{1/3}))$-close to uniform and similarly secure. This is achieved via a construction which ensures the output of a given round is entirely uncorrelated with the input that was used to generate it. This allows the expanded output from one round of the protocol to be fed back in to another round - a process which can be indefinitely repeated for arbitrary gain.

Protocol Comparison This provides an interesting contrast for the Zoo. Whilst this protocol clearly carries an improved performance over that of Pironio *et. al.*, it comes at a cost of increased conceptual, computational and hardware complexity. Coudron and Yuen make use of various other results as sub-protocols which makes non-technical summary in a single page challenging. It may be the case that such a protocol would have been better suited to a richer wiki ecosystem, with more internal references to the sub-protocols as separate pages.

Table 3.1 summarises the key empirical factors for comparing the two protocols proposed for inclusion in the Zoo. Whilst the increase in performance of Coudron and Yuen undoubtedly makes it a more appealing prospect for implementation, its

correspondingly raised complexity makes it significantly more challenging to achieve. Given the number of sub-protocols called by Coudron and Yuen, a more exact analysis of computational complexity is difficult to achieve.

Nevertheless, the relative simplicity of Pironio *et. al.* makes its inclusion in the Zoo useful as a teaching resource. Since Coudron and Yuen build upon simpler protocols such as this, as a richer ecosystem for cross-referencing is built up on the Zoo, it may become easier to discuss protocols of such complexity.

	Expansion	Security	Devices	Noise Tolerant
Pironio *et. al.* [3]	$\theta(n^2)$	n/a[1]	2	Yes[2]
Coudron and Yuen [43]	∞	$\exp\left(-\Omega(n^{1/3})\right)$	8	Yes[3]

[1]Security is dependent on the specific choice of randomness extractor.
[2]System noise must still permit a super-classical CHSH result.
[3]No limit provided.

Table 3.1: Key performance metrics for the two randomness expansion protocols proposed for inclusion in the Quantum Protocol Zoo [1]. n refers to the number of bits in the seed. A protocol with security ε has output ε-close to uniform conditioned on the information of an adversary.

Both protocols considered use a constant number of devices and are tolerant to noise. As a result, an interested party could feasibly implement them in the near-term, fulfilling another goal of the Zoo. Despite the four-fold increase in number of devices required by Coudron and Yuen, the actual technology required is the same: an entangled state must be shared across two devices only, and measurements made in the X, Z and $1/\sqrt{2}(X \pm Z)$ bases.

3.2.2 Randomness Amplification

Randomness amplification takes a string from a weak source of randomness - one which contains correlations and may be at least somewhat predictable by an adversary - and converts it to a (potentially shorter) string which is (close to) uniformly random and private from any adversaries. Classically, it is only possible to extract uniform, private randomness by combining multiple weak sources together. Quantum protocols enable the extraction of such randomness from only a single weak source - useful in any situation where only some randomness has been provided but absolute security is required.

Whilst protocols exist for amplification of arbitrary min-entropy sources [39, 48], no development has yet achieved the task with only a finite number of devices. In each

case, the measurement devices required must be used once then discarded. As this is not realistic for any actual implementation, such protocols were not considered for inclusion in the Zoo. Santha-Vazirani (SV) sources are a subset of min-entropy sources for which various protocols have been developed to enable amplification using a finite number of devices [11, 41]. These are therefore of significantly more relevance to the Zoo.

The protocol of Brandao *et. al.* [11] provides a method for amplifying an arbitrarily weak SV source (i.e. an SV source with any $\delta \in [0, 1/2]$) using only eight measurement devices. In addition, the protocol is tolerant to noise and the steps required are relatively simple. These factors make it realistically near-term implementable and a strong candidate for inclusion in the Zoo.

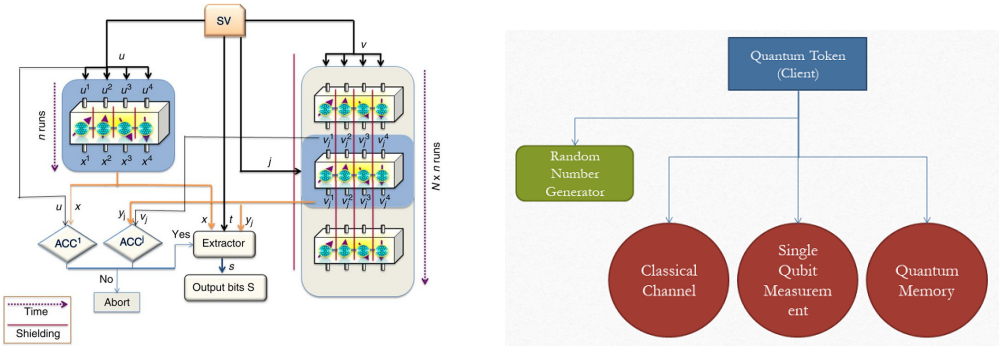
Their key contribution is a protocol structure which makes it possible to mimic three independent SV sources using the measurement results from a four-party analogue to the CHSH game. These results also act as a certification procedure: the protocol will abort if a result is returned which strongly suggests the expected quantum behaviour has not occurred.

The relative simplicity of this protocol again means it is not state of the art. Kessler and Arnon-Friedman [41] present a protocol capable of performing randomness amplification of an arbitrary SV source to produce a string which is (close to) private and random even if the source itself is fully known to an adversary. Table 3.2 compares the performance metrics of these two protocols. The protocol of Kessler and Arnon-Friedman [41] would make an excellent addition to the Zoo, but was not included in this project due to time constraints.

	Output Length	Public Source	Devices	Noise Tolerant
Brandao *et. al.* [11]	n/a[1]	No	8	Yes[2]
Kessler and Arnon-Friedman [41]	$\theta(n)$	Yes	2	Yes[3]

[1] Dependent on the specific choice of randomness extractor.
[2] Number of errors per elementary operation must be less than $\frac{1}{2}(\frac{1}{2} - \delta)$
[3] System noise must still permit a super-classical CHSH result.

Table 3.2: Key performance metrics for the two randomness amplification protocols proposed for inclusion in the Quantum Protocol Zoo [1]. The security of each is dependent on the randomness extractor used and both tolerate an SV source with any bias. n refers to the number of bits in the input and δ is the bias of the source.



(a) (b)

Figure 3.1: (a) A diagrammatic representation of the randomness amplification protocol of Brandao *et. al.* [11]. (b) A diagrammatic representation of the hardware requirements for the Quantum Tokens protocol on the Quantum Protocol Zoo [1]. Sub-protocol dependencies are shown in green and hardware requirements in red.

3.3 Discussion

Of the three protocol pages produced, finite randomness expansion and randomness amplification best suit the structure of the Zoo due to their relative simplicity and brevity. This is in contrast to the infinite randomness expansion page, whose use of numerous sub-protocols makes the summary somewhat clumsy. Perhaps this highlights the possible utility of a richer structure to the Zoo, where protocols which call upon one another can contain hyperlinks to connect together sections of pseudocode in a standardised manner.

Each page would have benefited from an amount of visual explanation. Brandao *et. al.* [11] provide an excellent diagram of their protocol (Fig.3.1(a)) - similar professional quality outlines would undoubtedly aid in understanding the randomness expansion protocols, particularly for those for whom the pseudocode is unfamiliar.

After completion of this section of the project, the Zoo was updated to include charts such as the one shown in Figure 3.1(b). These are visual representations of the hardware and software requirements of each protocol and help to illustrate dependencies in a standardised manner. Prior to publication on the Zoo, each page created during this project would have to be updated to include these charts.

The most obvious next step for development of quantum random number generation on the Zoo is the continued addition of protocol pages. Kessler and Arnon-Friedman's amplification protocol [41] as outlined above has already been suggested. Further sensible additions would include the sub-protocols used by Coudron and Yuen [43], amongst others.

Chapter 4

Simulations

In the second stage of the project, the finite randomness expansion protocol of Pironio *et. al.* was simulated in full, and a generic experimental framework developed for use in future simulations. All code can be found on the project directory.

4.1 SimulaQron

The simulations were built using the SimulaQron [2] library. Whilst a range of general purpose quantum simulation libraries have been developed [49], SimulaQron's ability to construct virtual quantum networks makes it best suited for representing the multiple device structure of the protocols. In particular, it straightforwardly enables simulation of a network over which entangled states can be shared.

4.1.1 Functionality

To run a SimulaQron script, a network of nodes connected by directed edges must first be constructed (Fig.4.1), where the direction of the edge indicates in which direction qubits can be sent. Once a network has been started, qubits can be prepared, entangled, shared and measured by running python scripts which connect to individual nodes and interact with the SimulaQron backend.

Measurements can only be made in the computational basis, so some manipulations must be performed when changing basis. As any measurement basis is related to the computational basis by a rotation only, one can mimic any measurement by applying the opposite rotation to the quantum state. This is a change in frame-of-reference which aligns the desired basis vectors with the original computational basis vectors.

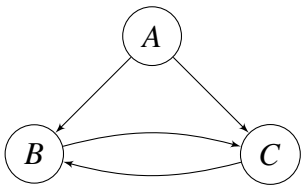


Figure 4.1: A simple SimulaQron network structure. Alice (A) can send qubits to Bob (B) and Charlie (C), and Bob and Charlie can share qubits amongst each other. Bob and Charlie are unable to send qubits back to Alice.

4.1.2 Experiment Framework

For efficient experimentation with the simulations, a Python framework was constructed to provide a single command line interface for controlling network, protocol and experiment parameters. This was in part necessitated by the need to overcome some of the shortcomings of the SimulaQron library. The file `utils.py` provides a number of helper functions of general use in the simulations, and in particular contains the `ExperimentManager` class. In addition to controlling the virtual nodes via separate threads, this takes care of the boilerplate code required to start and stop the SimulaQron network. By centralising the control of the network and backend, this framework helps to reduce the number of steps required to alter an experiment and therefore increases efficiency and reduces the chance of user error.

SimulaQron recommends simulations be run as a series of separate python scripts, controlled by a bash script. This structure has two key flaws for experiments on the scale of those in this project. Firstly, the native classical communication mechanism between nodes (required for sharing results) is not optimised for repeated use. Secondly, running separate scripts makes it difficult to control the 'flow' of qubits in the experiment. Each node is only capable of holding a finite number of virtual qubits (20 by default). If node Alice can prepare and send qubits to node Bob much faster than he is able to process them then qubits can very quickly build up and cause the backend to crash. It is possible to increase this cap, but this makes the backend more susceptible to timing out. Controlling the nodes via threads in a central script means that each can write to data structures which can be shared efficiently and the flow of qubits can be controlled easily with `Barrier` objects. More advanced mechanisms [50] may have increased simulation efficiency.

SimulaQron does not directly provide a control for how noisy a given network is, but allows the coherence time of the simulated qubits to be tuned. This serves as a useful proxy for noise as a qubit with shorter coherence time is more likely to

deviate from its expected state. The absolute value specified for coherence time is somewhat meaningless as it is defined relative to wall clock time, meaning the actual effect will vary from computer to computer. It is best therefore to tune coherence time by comparing to an experimental parameter clearly affected by noise (for instance, how super-classical the result of an honest CHSH game is) and to use it only as a relative measure (i.e. to compare "less" noise to "more" noise).

4.2 Randomness Expansion

4.2.1 Implementation

Random Seed The Australian National University (ANU) provide online access [9] to a truly quantum random number generator. For this project, the 1GB torrent (roughly 8 billion random bits) was downloaded. One thousand bit strings of length 100,000 were run through the NIST suite for verification. The assessment used every test apart from Maurer's Universial Statistical Test (which requires extremely long inputs) with default parameters selected for each and a significance level of 0.01. The expected number of samples (around 99%) passed each test (Fig.4.2).

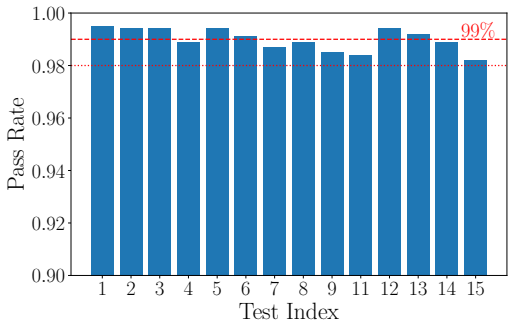
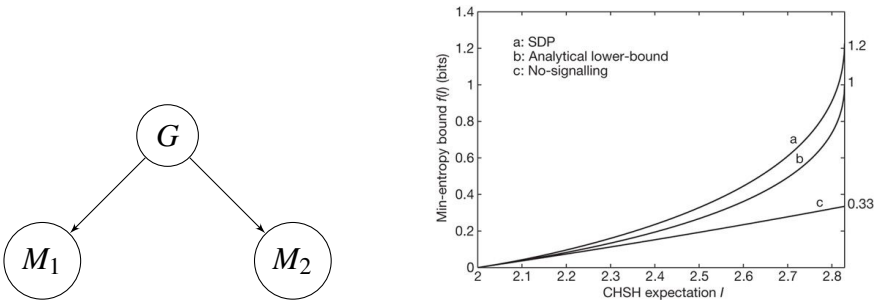


Figure 4.2: Pass rate for 1000 random bit string samples of length 100,000 from ANU's QRNG [9] all but one of the tests in NIST's benchmarking suite [25]. Default settings and a significance level of 0.01 are applied to each test. The expected pass rate is 99% (dashed line), NIST recommends a minimum pass rate of 98% (dotted line) for acceptance.

SimulaQron Network The network used to implement this protocol (Fig. 4.3(a)) consisted of a "generator" node, connected to a pair of measurement devices to which it could send EPR states. It would have been possible to have one measurement device



(a) (b)

Figure 4.3: (a) SimulaQron network for implementing finite randomness expansion [3]. A generator (G) can send (entangled) qubits to a pair of measurement devices (M_1 and M_2). The measurement devices cannot communicate. (b) Per-bit min-entropy bounds on the measurement results of the CHSH game used in the same protocol. Taken from [3]. The exact bound is the uppermost line, determined via semi-definite programming and not presented in the paper. Below this is an analytical estimate, $f(I) = 1 - \log\left(1 + \sqrt{2 - I^2/4}\right)$, which is used in this simulation.

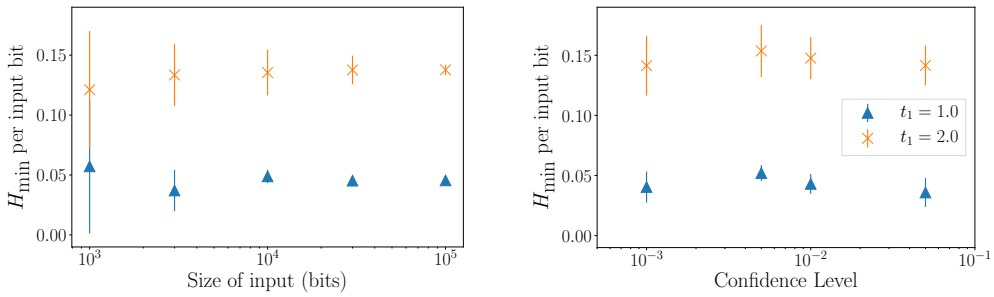
generate the entangled pair and send one of the qubits to the other device, but this architecture better represents the setup of the authors [3].

Protocol Full pseudocode for the protocol is outlined in Section 3.2.1, only a small number of adaptations are required for implementation in SimulaQron. The exact bound on the conditional min-entropy of the results generated by the CHSH game is determined by semi-definite programming and is not presented in the paper [3], an analytical bound (Fig.4.3(b)) was therefore used. The above bound is undefined if $\hat{I} - \varepsilon$ (see Sec.3.2.1) is greater than $2\sqrt{2}$, so values exceeding this have their per-bit min-entropy capped at 1.

Carter-Wegman hashing is used as a simple strong randomness extraction [31], with performance parameters $d = 2n$ and $m = k + d$ (where the confidence bound has been absorbed into the definition of k).

4.2.2 Results

This protocol can be broadly separated into two parts: entropy generation and post-processing. The former corresponds to the generation of a min-entropy bound string using the CHSH game measurement results, and the latter to the application of a randomness extractor to produce the final expanded string.



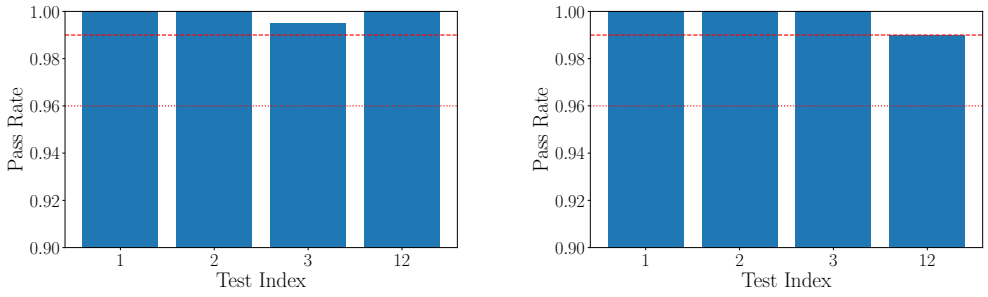
(a) (b)

Figure 4.4: Estimated min-entropy bound per input bit for a range of (a) input lengths with fixed confidence $\alpha = 0.01$ and (b) confidence levels with fixed input length $n = 10^4$. The specified coherence times (t_1) correspond to $\hat{I} \approx 2.3$ and $\hat{I} \approx 2.6$ respectively. The reported values and errors are the mean and standard deviation of (a) 10 experiments and (b) 5 experiments.

Entropy Generation In an honest system (i.e. no extra entanglement or device communication), the key factors to consider are the length of the seed, how noisy the system is and to which confidence correctness of the min-entropy bound is required. In each experiment that follows, the protocol is simulated and the determined min-entropy bound returned. This is repeated five times for each parameter setting (10 times for input length to get a better gauge of variance), with the values reported as the mean and the errors as the standard deviation.

For intermediate confidence level ($\alpha = 0.01$) and coherence times ($t_1 = 1.0$ and $t_1 = 2.0$, giving $\hat{I} \approx 2.3$ and $\hat{I} \approx 2.6$ respectively), changing input size in the range $n \in [10^3, 10^5]$ has a significant effect on the variance (to be expected as the CHSH game is stochastic) of the min-entropy bound but a nominal effect on its magnitude (Fig.4.4(a)). Given the output is expected to have length $\theta(n^2)$, a linear relationship between input length and the per-bit min-entropy bound should appear. Its absence in this experiment may be due to the more conservative lower bound used, or it may be simply that an insufficient number of bits have been input. It is not feasible to check this in the current project as a single simulation of 10^5 input bits already takes upwards of 4 hours to run. In addition, the experimental implementation of Pironio *et. al.* returned a min-entropy bound of 42 from an input size of 3016 bits [3], giving a per-bit min-entropy bound of 0.0139. This is (just) within the range observed in the simulations for $n = 3000$ and $t_1 = 1.0$, where a value of 0.037 ± 17 was obtained - a reassuring validation of the setup.

Typical confidence values are in the range $\alpha \in [0.001, 0.01]$. For intermediate input



(a) (b)

Figure 4.5: (a) Pass rate of 300,000 raw bits from the ANU QRNG [9], tested as 100 blocks of length 3000 on a subset of the NIST tests [25]. (b) Pass rate of 314,600 randomness expanded bits, seeded by the aforementioned raw bits and assessed on the same tests. The expected pass rate is 99% (dashed line), NIST recommends a minimum pass rate of 96% (dotted line) for acceptance.

length ($n = 10^4$) and coherence times ($t_1 = 1.0$ and $t_1 = 2.0$, giving $\hat{I} \approx 2.3$ and $\hat{I} \approx 2.6$ respectively), the effect of changing the confidence level is nominal for both magnitude and variance (Fig.4.4(b)). Beyond expected statistical fluctuation, the consequence of changing the value is nominal - this is most likely due to the $\theta(1/\sqrt{n})$ dependence of the statistical correction term ε - the only place where confidence is a factor.

Comparing the effect of coherence time on the per-bit min-entropy does not carry much meaning as coherence time is only a proxy control. It is not possible to unpick which changes in performance are due to noise acting on the protocol and which are due to coherence time affecting noise. A more advanced noise model is required for such analysis. The rate of error in quantum systems is typically dependent on the operation performed [51]. It would not be challenging to incorporate a simulated error channel into each of the SimulaQron operations to provide a standardised method of characterising protocol robustness to noise. In addition, one could construct an independent error model for quantum transmission, incorporating a simulated 'distance' by which virtual nodes are separated.

Post-processing To verify performance of the protocol, the randomness of a string sourced from the ANU QRNG [9] was assessed prior to and following randomness amplification. Using 100,000 bits to seed 50,000 protocol iterations, a min-entropy bound of 14,632 was obtained. Taking an additional 200,000 bits to seed Carter-Wegman hashing-based randomness extraction, a final protocol output of length 314,632 bits was obtained from an input of total length 300,000.

As such strings are relatively short in the context of randomness assessment, only a subset of the NIST test suite [25] was applied (Fig.4.5). Each string was divided into 100 blocks and passed through these tests. Default parameters were used for every test except `ApproximateEntropy` (test 12), for which `m` (block size) was set to 6. The confidence level was set to 0.01. Whilst it is unwise to make confident claims based on such a small sample size, both the raw and expanded strings pass each test at the expected rate. This provides an indication of the correctness of the protocol, but larger samples are required for more conclusive results.

4.3 Discussion

The initial simulation results are promising but the scope of the experiments is limited. Sensible values are obtained for each, but the expected polynomial expansion factor is not apparent. With more time or a more efficient implementation it may be possible to repeat with a much larger string size: indeed the ANU source is far from exhausted. Better study of the protocol's response to noise in the apparatus and wider network would be a valuable asset for implementation - the noise model as suggested above could prove of great benefit here, and could be used in a broad range of SimulaQron applications.

No study in this project is made of dishonest implementations. A key factor in all of the protocols outlined in this project is the security they guarantee. It would be worthwhile attempting a verification of this by studying how the protocol responds to maliciously entangled states.

The `ExperimentManager` class developed to aid in these experiments is generic enough to support simulation of arbitrary protocols. An attempt was made to repeat this study for the randomness amplification protocol of Brandao *et. al.*, however as the complexity of the randomness extractor required is beyond the scope of this project, only limited progress was made. Basic elements have nevertheless been constructed as a proof of concept, a future work could continue its development.

In addition, as the network connectivity required for this simulation is so simple, it would be possible to run on the architecture of available quantum chips [52, 51]. Whilst not directly relevant to the desired application on quantum networks, it would be interesting to see if the protocol is robust enough to function on actual quantum hardware.

Chapter 5

Protocol Development

All of the protocols discussed so far have made use of the CHSH game to generate quantum certified randomness. Whilst this is the most common form of game used, it is not the only one. In this section, an alternate quantum game is introduced and an adaptation proposed which may offer a lower technological barrier to implementation of certified device independent randomness protocols.

5.1 Mermin-Peres Magic Square

The Mermin-Peres Magic Square [4] is a game played by two parties, conventionally named Alice and Bob. As in the CHSH game, Alice and Bob are free to agree on a strategy but cannot communicate once the game starts.

Each round of the game requires Alice and Bob to fill part of a 3-by-3 grid with either $+1$ or -1. Alice is assigned a row at random and Bob a column. The requirements of each round are:

- Alice must place -1 an even number of times.
- Bob must place -1 an an odd number of times.
- Both players win if the cell that they share contains the same number, otherwise they lose.

The best possible classical strategy is to agree ahead of time what numbers to put in eight of the cells (Fig.5.1(a)) - given the game's requirements, it is not possible to agree on what to put in the ninth square. This gives a success rate of $8/9$ since the strategy only fails if both are given the row and column for which no number has been agreed.

The quantum strategy is for Alice and Bob to share two EPR pairs and to make the measurements as outlined in Figure 5.1(b), where the tensor product means that each

-1	-1	$+1$
$+1$	$+1$	$+1$
$+1$	$+1$	?

(a) Possible Classical Strategy

$+X \otimes I$	$+X \otimes X$	$+I \otimes X$
$-X \otimes Z$	$+Y \otimes Y$	$-Z \otimes X$
$+I \otimes Z$	$+Z \otimes Z$	$+Z \otimes I$

(b) Optimal Quantum Strategy

Figure 5.1: Classical and quantum strategies to the Mermin-Peres magic square game. (a) It is not possible classically to fill each cell of the square whilst satisfying the requirements - one will always be left blank. (b) Measurements on correlated states can be used to produce a unique perfect solution.

measurement is simultaneously applied to a different Hilbert space (and therefore a different qubit) and I is the identity matrix, meaning that no measurement is applied. For example, for Alice to make the measurement in the centre-left box, she simultaneously measures her first qubit in the X basis and her second qubit in the Z basis and places in the cell the product of the eigenvalues returned multiplied by -1.

It can be shown that this strategy results in a 100% success rate [53], moreover it has recently been proved that it is the only strategy [54]. This is another example of a super-classical result and can therefore be used to generate device independent, certified randomness. To date, no formal protocol has been published which makes use of the Mermin-Peres Magic Square (likely due to the relative simplicity of the CHSH game), so this remains a potential avenue for further work. Formal results for proving randomness generation have however been produced [45, 34].

5.2 Mermin-Peres Magic Rectangle

This project proposes a simplification of the Magic Square game, tentatively named the Magic Rectangle. It is possible to construct a smaller 3-by-2 (concretely, three columns and two rows) game for which a perfect classical solution does not exist but a quantum one still does. In the same vein as above, if Alice and Bob agree ahead of time which squares to fill, they can establish a strategy which will succeed with a rate of $5/6$ (Fig.5.2). It is not possible to do any better than this.

+1	+1	+1
−1	+1	?

Figure 5.2: The classical solution to the 3x2 Magic Rectangle suffers from the same problem as the Magic Square: if squares are filled with predetermined solutions, one must always be left blank.

A quantum solution is available, however. Again sharing two sets of EPR pairs, Alice can take any two of the rows in the Magic Square (Fig.5.1(b)) to be her measurement strategy, and Bob can act as he would in the standard game. As this is simply a subset of the original game, the proof of correctness carries through trivially.

5.2.1 Technological Advantage

The benefit of such a strategy is the technological advantage it can enable. Consider the measurement in the top left corner of the Magic Square: $+X \otimes I$ corresponds to one party measuring their first qubit in the X basis and leaving the second one untouched. Similarly, the top right measurement corresponds to measurement of only the party's second qubit in the X basis. If Alice were to perform her measurements in this order, she would have no need to perform the simultaneous measurement of the central box: its result is implied by the information she already possesses. The same is true of the measurements in row three, and in columns one and three.

The central row and column are more problematic, however. The solution will only hold if the party measuring these does so with simultaneous operations, otherwise the state will be sufficiently disturbed to destroy the guaranteed correspondence. In addition, these are the only entities containing Y basis measurements. Simultaneous measurement of multiple qubits carries with it an increased technological difficulty, as does introducing further measurement bases. Therefore, a quantum game which is able to omit one of the central row or column promises a lower technological barrier for implementation for one of the parties involved.

With the rules as specified above, it is not possible to achieve a super-classical strategy if a column is skipped: there is a trivial solution of placing -1 in every box. On the other hand, the 3-by-2 Magic Rectangle allows for just this: if Alice is assigned only

the single qubit measurements of rows one or three then Alice and Bob can achieve a solution to a game which classically has no perfect strategy.

5.3 Discussion

Whilst the existence of a super-classical solution is promising, the above outline is only a sketch of a proof and more rigorous analysis is needed before any significant implications can be drawn from the Magic Rectangle. For example, device independent protocols rely on the fact that only one solution exists to a given game. In this way, they can provide guarantees that no unobserved eavesdropping has occurred: otherwise the correct result could not have been obtained. Even with the assumption that Alice's devices are simply not capable of performing the measurements in row two (leaving only rows one and three as possible actions), it may well be that further quantum solutions exist which undermine any security in the protocol.

More generally, if further analysis indicates that the Magic Rectangle is not a viable game for random number generation, existing theorems indicate that the Magic Square is [45, 34]. As no formal protocols yet exist which make use of these results, this presents an open avenue for further development.

Chapter 6

Conclusion

As chapters three, four and five of this report constitute a full analysis of each of the project stages, including concluding remarks and points for future work, this section will serve only to reflect upon and summarise them in brief.

The first stage of the project set out to produce non-expert summary pages of a range of quantum random number generation protocols for submission to the Quantum Protocol Zoo [1]. To this end, three protocol pages were completed, plus an additional page outlining the general functionality achieved by such protocols. The obvious avenue for further work here is the development of more pages for similar protocols - particularly as developments in both quantum hardware and theory move towards realisable implementations.

In the second stage, a generic experimental framework was developed for the SimulaQron [2] library. With this, the finite randomness expansion protocol of Pironio *et. al.* [3] was simulated. Whilst the initial results are promising, further study is needed to draw any signification conclusions about the robustness of the protocol to parameter choice, system noise and attack by an adversary. In order to do so, limitations such as simulation inefficiency and the lack of a formal noise model must be overcome - however, these would appear to be achievable in the near term. In addition, the randomness amplification protocol of Brandao *et. al.* is proposed as a possible alternative study - with basic proof of concept components already achieved.

Finally, the Mermin-Peres Magic Square was outlined as an alternative randomness source to the CHSH game [4]. In particular, the sketch of a proof of how this could be adapted to suit a simpler implementation was given. Significant analysis of this proposal is required before formal conclusions can be drawn, but the existence of a super-classical solution to the game is promising.

Bibliography

[1] Quantum Protocol Zoo. https://wiki.veriqloud.fr. Accessed 5/08/2019.

[2] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288, 2018.

[3] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzmitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. Random numbers certified by bells theorem. *Nature*, 464(7291):1021, 2010.

[4] PK Aravind. Quantum mysteries revisited again. *American Journal of Physics*, 72(10):1303–1307, 2004.

[5] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[6] Randomness and Integrity Services Ltd. Random.org. https://www.random.org/clients/http/. Accessed 25/07/2019.

[7] Masatugu Isida and Hiroji Ikeda. Random number generator. *Annals of the Institute of Statistical Mathematics*, 8(1):119–126, 1956.

[8] ID Quantique. https://www.idquantique.com/. Accessed 8/08/2019.

[9] Australian National University. Quantum random numbers server. https://qrng.anu.edu.au/. Accessed 26/07/2019.

[10] Roger Colbeck. Quantum and relativistic protocols for secure multi-party computation. *arXiv preprint arXiv:0911.3814*, 2009.

[11] Fernando GSL Brandão, Ravishankar Ramanathan, Andrzej Grudka, Karol Horodecki, Michał Horodecki, Paweł Horodecki, Tomasz Szarek, and Hanna Wojewódka. Realistic noise-tolerant randomness amplification using finite number of devices. *Nature communications*, 7:11345, 2016.

[12] Axel Dahlberg and Stephanie Wehner. Simulaqrona simulator for developing quantum internet software. *Quantum Science and Technology*, 4(1):015001, 2018.

[13] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators. *Reviews of Modern Physics*, 89(1):015004, 2017.

[14] Salil P Vadhan et al. Pseudorandomness. *Foundations and Trends in Theoretical Computer Science*, 7(1–3):1–336, 2012.

[15] Python 2.7.15 documentation. 9.6. random - generate pseudo-random numbers. `https://docs.python.org/2/library/random.html`. Accessed 25/07/2019.

[16] Java Documentation. Random (java platform se 7). `https://docs.oracle.com/javase/7/docs/api/java/util/Random.html`. Accessed 25/07/2019.

[17] Christopher M. Bishop. *Pattern Recognition and Machine Learning*. Springer New York, 2016.

[18] Elaine B Barker and John Michael Kelsey. *Recommendation for random number generation using deterministic random bit generators (revised)*. US Department of Commerce, Technology Administration, National Institute of , 2007.

[19] Zvi Gutterman, Benny Pinkas, and Tzachy Reinman. Analysis of the linux random number generator. In *2006 IEEE Symposium on Security and Privacy (S&P'06)*, pages 15–pp. IEEE, 2006.

[20] Stephen Barnett. *Quantum information*, volume 16. Oxford University Press, 2009.

[21] Alfréd Rényi et al. On measures of entropy and information. In *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*. The Regents of the University of California, 1961.

[22] Miklos Santha and Umesh V Vazirani. Generating quasi-random sequences from semi-random sources. *Journal of computer and system sciences*, 33(1):75–87, 1986.

[23] Thomas Jennewein, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71(4):1675–1680, 2000.

[24] Graham Upton and Ian Cook. *A dictionary of statistics 3e*. Oxford university press, 2014.

[25] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, and Elaine Barker. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, Booz-Allen and Hamilton Inc Mclean Va, 2010.

[26] Pierre L'Ecuyer and Richard Simard. Testu01: Ac library for empirical testing of random number generators. *ACM Transactions on Mathematical Software (TOMS)*, 33(4):22, 2007.

[27] George Marsaglia. Diehard: a battery of tests of randomness. *http://stat. fsu. edu/geo*, 1996.

[28] Robert G Brown, Dirk Eddelbuettel, and Bauer David. Dieharder: A random number test suite. `http://webhome.phy.duke.edu/~rgb/General/dieharder.php`. Accessed 27/07/2019.

[29] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[30] Ramamurti Shankar. *Principles of quantum mechanics*. Springer Science & Business Media, 2012.

[31] Thomas Vidick. CS/PH 120 quantum cryptography. `http://users.cms.caltech.edu/~vidick/teaching/120_qcrypto/`. Accessed 1/08/2019.

[32] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical review letters*, 23(15):880, 1969.

[33] Boris S Cirel'son. Quantum generalizations of bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.

[34] Honghao Fu and Carl A Miller. Local randomness: Examples and application. *Physical Review A*, 97(3):032324, 2018.

[35] Luca Trevisan. Extractors and pseudorandom generators. *Journal of the ACM*, 48(4):860–879, 2001.

[36] Jaikumar Radhakrishnan and Amnon Ta-Shma. Bounds for dispersers, extractors, and depth-two superconcentrators. *SIAM Journal on Discrete Mathematics*, 13(1):2–24, 2000.

[37] Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi, and Zhen Zhang. Quantum random number generation. *npj Quantum Information*, 2:16021, 2016.

[38] Mario Stipcevic. Quantum random number generators and their applications in cryptography. In *Advanced Photon Counting Techniques VI*, volume 8375, page 837504. International Society for Optics and Photonics, 2012.

[39] Kai-Min Chung, Yaoyun Shi, and Xiaodi Wu. Physical randomness extractors: generating random numbers with minimal assumptions. *arXiv preprint arXiv:1402.4797*, 2014.

[40] Jan Bouda, Marcin Pawłowski, Matej Pivoluska, and Martin Plesch. Device-independent randomness extraction from an arbitrarily weak min-entropy source. *Physical Review A*, 90(3):032313, 2014.

[41] Max Kessler and Rotem Arnon-Friedman. Device-independent randomness amplification and privatization. *arXiv preprint arXiv:1705.04148*, 2017.

[42] Roger Colbeck and Renato Renner. Free randomness can be amplified. *Nature Physics*, 8(6):450, 2012.

[43] Matthew Coudron and Henry Yuen. Infinite randomness expansion with a constant number of devices. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 427–436. ACM, 2014.

[44] Umesh V Vazirani and Thomas Vidick. Certifiable quantum dice-or, testable exponential randomness expansion. *arXiv preprint arXiv:1111.6054*, 2011.

[45] Carl A Miller and Yaoyun Shi. Randomness in nonlocal games between mistrustful players. *Quantum information & computation*, 17(7):595, 2017.

[46] Veriqloud. `https://veriqloud.com/`. Accessed 5/08/2019.

[47] Quantum Internet Alliance. `http://quantum-internet.team/`. Accessed 5/08/2019.

[48] Kai-Min Chung, Yaoyun Shi, and Xiaodi Wu. General randomness amplification with non-signaling security. *Online]. Available: https://ix. cs. uoregon. edu/˜ xiaodiwu/papers/csw16. pdf*, 2016.

[49] List of QC simulators. `https://quantiki.org/wiki/list-qc-simulators`. Accessed 6/08/2019.

[50] Python 3.7.4 documentation. threading - Thread-based parallelism. `https://docs.python.org/3/library/threading.html`. Accessed 6/08/2019.

[51] IBM. Ibm q experience. `https://quantum-computing.ibm.com/`. Accessed 29/07/2019.

[52] Rigetti. Home. `https://www.rigetti.com/`. Accessed 29/07/2019.

[53] Gilles Brassard, Anne Broadbent, and Alain Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11):1877–1907, 2005.

[54] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Physical Review A*, 93(6):062121, 2016.