Quantum Cryptography
Third Year Lab Report

Charlie Perkins, 10839865
Department of Physics and Astronomy, University of Manchester
(This experiment was performed in collaboration with Felipe Tcach, 10826579)
(Dated: March 5, 2024)

Algorithms in quantum computing are threatening the security of classical key distribution protocols such as RSA. Quantum key distribution protocols that have been proved effective as secure replacements can be expensive to build and configure. We explore the fidelity and efficacy of the BB84 and B92 protocols by calculating the probability of transmission of a single photon through affordable apparatus from experimental data. These values prompt 25,000 simulations of transmission. We find that BB84 and B92 are effective protocols, and with simple calibration methods, provide effective bit-rates of 270 ± 77 kbps and 192 ± 60 kbps respectively. This is sufficiently fast to replace RSA-2048, thereby maintaining decentralisation in private communication in a post-quantum internet.

1. INTRODUCTION

BB84 and B92 are Quantum Key Distribution protocols (QKD) that use single photons to share a common cypher, and thus require optic infrastructure. Many countries are deploying fibre-optic networks, which may serve as the basis for these secure channels. BB84 and B92 networks often require a system of filters, waveplates, polarisers, and beamsplitters to process the photons. High precision optics can be expensive, so developing countries and small businesses may not have the money to construct their own network. We aim to explore whether readily available and, relatively, low budget optics provide enough fidelity to make the use of BB84 and B92 viable.

2. THEORY

2.1. BB84

BB84 is a QKD protocol that can distribute a random binary string of any length with complete assurance of privacy [1]. The final shared key is therefore completely random, but could be used in a one-time pad (OTP), enabling the safe distribution of a symmetric key such as AES-256. Assuming key generation is singular and truly random, the OTP is unbreakable outside of brute-force [2].
A full proof of the BB84 mathematical principle is beyond the scope of this report, however there is some preliminary detail which must be covered. We suggest Ref. [3] for an overview of BB84.
BB84 distributes data via encoding bits into the polarisation states of single photons, of which there are two bases in which to encode the bit. Each base contains a '0' and '1' state, which are mutually orthogonal. Before the detector, the photon is resolved into a basis, chosen at random, giving 8 transmission scenarios. Each scenario has an associated probability of measuring a '1' and a '0'. After transmission, bits where the sender and recipient bases were not equal are discarded. Approximately 50% of the bases are different, therefore an initial binary string of length n will be approximately of final length $0.5n$ after successful key distribution.

2.2. B92

B92 is another QKD protocol, similar to BB84, however there are only two photon states, though not orthogonal to each-other. In this case, the final string is approximately 25% the length of the initial string. The full proof of B92 is not required for this report, and can be found in full from Ref. [4].

2.3. Single Photon Probability

We propose a method for interpolating the probability of a single photon resolving onto one of the two detectors in the BB84 and B92 protocols using collimated, polarised laser light. Assuming minimal light losses within the optics, the probability that a single photon transmitted from the point of the laser will resolve onto a given detector can be calculated. Since the proportion of photons from the laser which is split onto each detector must be invariant to whether the photons are transmitted continuously or singly, we can infer the 'single photon probability' from the ratio of continuous laser light on the detectors. We find that the equation for the probability that a photon will resolve onto detector a, p_a, is given by

$$p_a = \frac{V_a}{V_a + V_b}, \tag{1}$$

where V_a and V_b are the voltages measured on the detectors a and b respectively, given that the detectors have the same response.

2.4. Linear Polariser and Double Successive $\frac{1}{2}$-Waveplate Convolution

The convolution of the optics, which modifies the angle of polarisation of the photons, is relevant to the calibration of the apparatus. The full derivation simply follows from the convolution of the intensity distributions of a linear polariser with a $\frac{1}{2}$-waveplate. The resulting intensity pattern is given by

$$I(\theta) = I_0 e^{-\frac{(\theta-\theta_0)^2}{2\sigma^2}}, \tag{2}$$

where $I(\theta)$ is the measured intensity, I_0 is the maximum intensity, θ is the angle of rotation of the linear polariser, θ_0 is the angle of maximum intensity, and σ is the spread of the intensity.

3. METHODOLOGY

3.1. Apparatus

The apparatus (mostly ThorLabs EDU-QCRY1), with a value of about £3k, was setup as outlined in Fig. 1 [5]. Laser light was passed through a linear polariser and two rotating $\frac{1}{2}$-waveplates, before being cast into two perpendicular beams by a polarising beamsplitter. Thereafter, each beam passed through three neutral density filters with a combined strength of 1.1, and onto the photodiode sensors. The path lengths from the beamsplitter to each detector were of equal length.

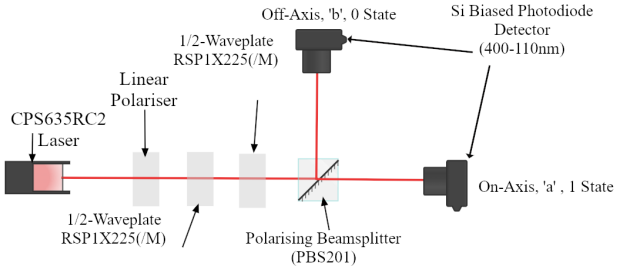

FIG. 1: A diagram of the experimental apparatus. The laser light has wavelength 650nm. Each $\frac{1}{2}$ waveplate, has a variable angle. Each photodiode has a 12V bias from an internal battery.

3.2. *Calibration*

The beamsplitter was first positioned by eye such that its face was normal to the path of light. It was then rotated around its z axis minutely until each exit beam was central on its respective photodiode sensor. The distance of the sensors to the beamsplitter was large enough that only small changes in the angle were sufficient for alignment. The linear polariser was rotated such that the intensity of light measured on the on-axis detector was at a maximum, whilst the $\frac{1}{2}$ waveplates were both set to $0°$. The main source of uncertainty on all measurements of the intensity, here and when mentioned later, was taken to be the fluctuation in the intensity of the laser beam. This was quantised by taking the peak-to-peak value of the continuous laser intensity as measured on an oscilloscope with a total duration of 2.5ms and 2500 samples. Three measurements were made for each detector, and the average taken as the uncertainty. Thus, we declare this error to be $\pm 0.04\%$. An intensity distribution for the intensity on the on-axis detector as a function of the linear polariser angle was produced. The data was fitted to Eqn 2 by optimising the value of θ_0 such that the χ^2 value was minimised, giving the angle to set the polariser.

3.3. *Measurement*

The laser was fired continuously through the apparatus. The first $\frac{1}{2}$-waveplate was set to $-45°$ and the second to $0°$. The notches on the rotary waveplates served as the indicator for the angular position, along with the incremental scale, which had been calibrated separately previously using Malus' Law and optimising the χ^2 value as before. Three measurements for each sensor were made using the same parameters for the oscilloscope as in the calibration. Each measurement was averaged, and the subsequent mean of the three averages was taken to be the value of the detector voltage. The uncertainty was taken to be the intensity fluctuations in the beam and was propagated through all subsequent calculations. This method was repeated for all 8 transmission scenarios: $-45°, 0°, 45°, 90°$, for the transmitter plate, and $0°, 45°$ for the receiver plate. Background intensities for each photodetector were taken, from which the detector voltages were adjusted to account for the differences in the detectors' positions. Finally, maximum voltages were found for each detector using the same procedure. One waveplate was rotated until a maximum was reached for a given detector, and repeated for the other. This gave a known maximum voltage for each detector, from which all previous measurements of the voltages could be scaled, such that any variation in the bias voltages was removed.

3.4. *Simulations*

Single photon probabilities for a photon being transmitted to the on-axis and off-axis detectors were calculated from Eqn 1. Along with their propagated uncertainties, a table of probabilities was created to be referenced by the simulations. The general method for simulating a transmission involves generating three random binary arrays of length $2n$ $(4n)$ for BB84 (B92), where n is the desired key length and the number generation is uniform. The three elements of equal index in the arrays gives the full state of a transmission scenario, from which the corresponding probabilities and uncertainties can be found. Next, the simulation determines whether a 0 or 1 is detected. To conserve experimental uncertainty, a new probability is generated from a standard distribution with a mean of the probability of the state, and standard deviation of the uncertainty. This subsequent probability is compared to a randomly generated float (the comparison value) from a uniform distribution between 0 and 1. If the generated probability is less than or equal to the comparison value, a 1 is measured, otherwise a 0. This is, in effect, a Monte Carlo simulation. The final measured bit is stored in a new array which is then contracted. 25,000 simulations of BB84 and B92 were produced for desired key lengths between 8bit and 249bits, distributed uniformly across the range of key lengths to be simulated.

4. RESULTS AND DISCUSSION

4.1. *Probabilities*

Transmission State	P, Probability	$\Delta P, \%$
$0°, 0°$	0.984	± 0.2
$90°, 0°$	0.002	± 0.2
$-45°, 45°$	0.001	± 0.2
$45°, 45°$	0.982	± 0.2

TABLE I: Probabilities of measurement of '1' state, where $0 \leq P \leq 1$. The format of the Transmission State is - 'angle of sender waveplate, angle of receiver waveplate'.

The relevant probabilities used in the simulations are given in Table I. P is the probability of measuring a '1' bit. Due to the nature of BB84 and B92, states of indeterminate value have been discarded. The probabilities are very close to 0 or 1, with small uncertainties, confirming good optic transmission. We note that polarising beamsplitters reflect P polarised light more than S. As such, we expect more light than intended to reach the off-axis detector, therefore the probability of detecting a '0' is higher than perfect transmission. This may explain why the probability of measuring a '1' $(0°, 0°, 45°, 45°)$, when desired, differs more from perfect transmission probability (0 or 1) than the '0' state. The difference in P for '1' is 0.017 on average, whereas is 0.0015 for '0'. An improvement therefore might be to use a non-polarising beamsplitter in combination with mutually orthogonal linear-polarisers on each exit beam.

4.2. *Simulations*

The results for the simulations of BB84 and B92 are presented in Fig. 2 and Fig. 3, respectively. The colour of the points denotes the number of incorrect bits, n - Pink:0, Red:1, Orange:2, Gold:3, Yellow:4, Light Green:5, Dark Green: 5. The scatter points follow an $\frac{x-n}{x}$ curve for $x, n \in \mathbb{Z}+$, where x is the initial string length. The 'width' of the spread of points, in Fig. 2 and Fig. 3, from the

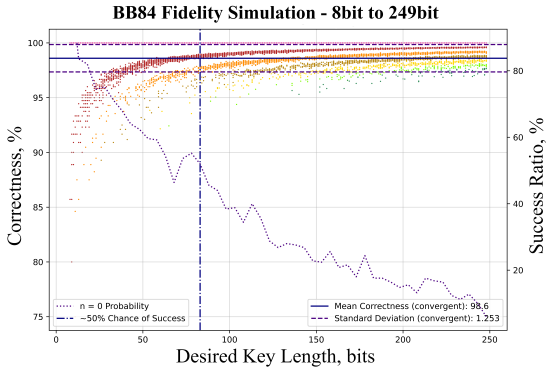

FIG. 2: Simulations of BB84 from 8bit to 249bit desired length. Average Correctness vs Desired Key Length (Left axis, scatter), Percentage of 100% Correctness vs Desired Key Length (Right axis, blue dotted line). The mean and standard deviation of the scatter are the displayed, see legend.

$\frac{x-n}{x}$ curve gives an insight into the variation in final string length from desired string length. Smaller desired string lengths tend to be more erratic with regards to the final length, so it is harder to determine the end string length. The dotted line represents the percentage of simulations that returned strings of 100% correctness, and is calculated over the mean of the previous 5 desired bit lengths. The average correctness for BB84 was 99.07%, (98.60%) overall (after 1^{st} $\frac{1}{3}$ points). For B92, this was 99.68% (99.52%) overall (after 1^{st} $\frac{1}{3}$ points). Additionally, the standard deviation on the correctness of BB84 was 1.22% (1.25%) overall (convergent), whereas it was 0.74% (0.86%) for B92 overall (convergent). This shows an apparent gain in fidelity from the use of B92 over BB84.

Both graphs depict a desired bit length at which the probability of getting a string with all bits correct is 50%, and therefore would require about 2 attempts to create a secure connection. We call this value the half-metric, n_0, and is the dash-dot line in Fig. 2 and Fig. 3. The half-metric for BB84 was found to be 83 ± 5 bits, and 233 ± 5 bits for B92, with the uncertainty coming from the bin size. It is clear that B92 has greater fidelity than BB84 for this setup. An OTP cypher must be greater than or equal to the length of the message to be encoded [2]. Since $83 < 233 < 256$ (with 256 being the AES key length), both B92 and BB84 would require distributing the key in multiple segments, which is not ideal, though B92 would require fewer attempts than BB84.

We introduce the effective bit-rate for a transmission, which is given by $\frac{n_0}{t}$, where t is the computation time to distribute n_0 twice. The effective bit-rates were found to be 270 ± 77 kbps for BB84 and 192 ± 60 kbps for B92, as averaged over 10,000 computations each, with the uncertainties derived from the standard uncertainties on the computation time and the error on the half-metrics. The code was written in C++ to remove performance issues associated with interpreted languages like Python. All the results, code, and analysis is open-source on the GitHub repository found in Ref. [6]. Though BB84 has a smaller half-metric, the final length has a 50% loss from the initial length, whereas B92 has 75% loss, resulting in the large speed difference between the two. RSA-2048 has an effective bit-rate of 330 kbps, which we calculate from Ref. [7]. Since the QKD protocols and RSA-2048 have effective-bit rates of the same order, it is likely that both BB84 and B92 would serve as effective replacements for RSA-2048, even in a system with relatively low budget apparatus. Thus both BB84 and B92 have a high efficacy in the real world, as potential decentralised encryption protocols.

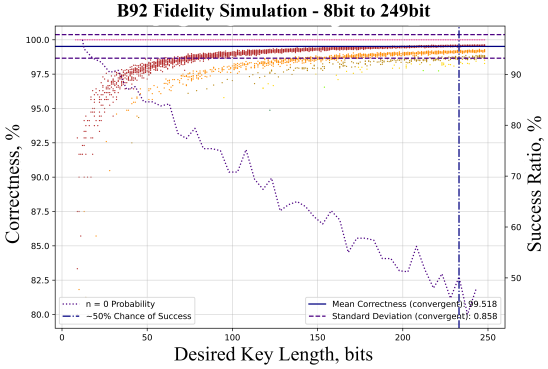

FIG. 3: Simulations of B92 from 8bit to 249bit desired length. Average Correctness vs Desired Key Length (Left axis, scatter), Percentage of 100% Correctness vs Desired Key Length (Right axis, blue dotted line). The mean and standard deviation of the scatter are displayed, see legend.

5. CONCLUSION

To conclude, it is possible to produce an effective quantum replacement for RSA-2048 by using either BB84 or B92. BB84 has worse fidelity, with an average correctness of $99.07 \pm 1.22\%$, and a half-metric of 83 ± 5 bits, but a greater effective-bit rate, at 270 ± 77 kbps. B92 has an average correctness of $99.68 \pm 0.74\%$, with a half-metric of 233 ± 5, meaning it can distribute keys of a greater size with the same number of attempts. However, B92's effective bit rate is only 192 ± 60 kbps, due to its computational intensity. Despite these differences, the speed is similar to that or RSA-2048, meaning that they would both be suitable replacements, even using budget optics. Thus, the means for an individual, small business, or developing nation to be able to encrypt their own data is conserved in a post-quantum world.

[1] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, p. 802–803, Oct 1982.

[2] A. Mermoud et al., *1. One Time Pad*, p. 3–5. Springer Nature Switzerland, 2023.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[4] C. H. Bennett et al., "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, p. 3–28, Jan 1992.

[5] ThorLabs, "Quantum cryptography analogy demonstration kit." Last accessed 14/12/23 from https://www.thorlabs.com/thorproduct.cfm?partnumber=EDU-QCRY1.

[6] F. Tcach and C. Perkins, "Quantum Cryptography." Last accessed 13/12/23 from https://github.com/Chaddyfynn/quantum-cryptography.

[7] W. Dai, "Speed comparison of popular crypto algorithms," Mar 2009. Last accessed 13/12/23 from https://www.cryptopp.com/benchmarks.html.