Key Rate Analysis of a 3-State Twin-Field Quantum Key Distribution Protocol in the Finite-key Regime

Matt Young
Department of Computer Science
University of York
York, United Kingdom

Darius Bunandar
Lightmatter
Boston,
Massachusetts, United States

Marco Lucamarini
School of Physics, Engineering, and Technology
University of York
York, United Kingdom

Stefano Pirandola
Department of Computer Science
University of York
York, United Kingdom

***Abstract*—When analysing Quantum Key Distribution (QKD) protocols several metrics can be determined, but one of the most important is the "Secret Key Rate". The Secret Key Rate is the number of bits per transmission that result in being part of a Secret Key between two parties. There are equations that give the Secret Key Rate, for example, for the BB84 protocol, equation 52 from [1, p.1032] gives the Secret Key Rate for a given Quantum Bit Error Rate (QBER). However, the analysis leading to equations such as these often rely on an "Asymptotic" approach, where it is assumed that an infinite number of transmissions are sent between the two communicating parties (henceforth denoted as Alice and Bob). In a practical implementation this is obviously impossible. Moreover, some QKD protocols belong to a category called "Asymmetric" protocols, for which it is significantly more difficult to perform such an analysis. As such, there is currently a lot of investigation into a different approach called the "Finite-key" regime. Work by Bunandar et al. [2] has produced code that used Semi-Definite Programming to produce lower bounds on the Secret Key Rate of even Asymmetric protocols. Our work looks at devising a novel QKD protocol taking inspiration from both the 3-state version of BB84 [3], and the Twin-Field protocol [4], and then using this code to perform analysis of the new protocol.**

***Index Terms*—quantum key distribution, quantum information science, quantum communication, quantum cryptography**

I. INTRODUCTION

We begin by discussing two key concepts surrounding Quantum Key Distribution (QKD) protocols: One-Time Pad Cryptography and the No Cloning Theorem of Quantum Mechanics. One-Time Pad motivates the use of QKD protocols, whilst the No Cloning Theorem is crucial for the security of QKD protocols. Using these concepts, we then go on to discuss some key QKD protocols that motivate our work, followed by discussion of analysis of these protocols with a particular focus on the Secret-Key Rate. We will then introduce the work done by Bunandar et al. and show analysis performed by them on some of the aforementioned QKD protocols. Finally, we will discuss the ongoing work that we are undertaking.

II. ONE-TIME PAD CRYPTOGRAPHY

One-time Pad (OTP) [5] [6, p.32] is a well known encryption technique that provides information-theoretically secure encryption. This encryption technique uses some pre-shared key K to encrypt some Plaintext P into a Ciphertext C according to the following scheme:

$$C = K \otimes P \tag{1}$$

where $\otimes$ is the XOR boolean operation.

Say that some person Alice produces a Ciphertext $C = K \otimes P$ and sends the Ciphertext to some second party Bob. Bob can then decrpyt the message by applying the XOR operation with the same, pre-shared key K to the Ciphertext:

$$P = K \otimes C = K \otimes K \otimes P \tag{2}$$

Lets say that we have some Eavesdropper called Eve. Eve can intercept the Ciphertexts, but cannot decrypt them, as she does not have the key. Suppose Eve intercepts two transmissions that contain encrypted Plaintexts P_1 and P_2, using the same key K, which give the Ciphertexts C_1 and C_2 respectively. She can then perform a bit-wise XOR:

$$\begin{aligned} C_1 \otimes C_2 &= P_1 \otimes K \otimes P_2 \otimes K \\ &= P_1 \otimes P_2 \otimes K \otimes K \\ &= P_1 \otimes P_2 \end{aligned} \tag{3}$$

We can see that if P_1 and P_2 share common text eg. headers, then Eve can discern some amount of information from this attack[1]. Namely this allows Eve to determine where the two messages differ.

From this discussion, we can determine two important problems regarding the OTP scheme:

1) Keys must be pre-shared.
2) Keys must be "fresh" for each transmission.

QKD looks at solving both of these issues by providing key-distribution primitives, the security of which is predicated on the laws of physics, rather than assumptions about computational complexity, such as with RSA and the Integer Factorisation Problem [7] [8].

[1] For instance, note that all lower-case ASCII characters begin with the binary digits "011".

III. The No Cloning Theorem

A key aspect of the security of QKD protocols is the No-Cloning Theorem. In Classical Computing, it is very commonplace for bits to be copied, but this fundamental aspect of Classical Computing is not present in Quantum Computing. Penfield [9, p.209] provides some interesting arguments as to why the No-Cloning Theorem holds true.

Ultimately, the proofs shown by Penfield state that some ideal cloning operation that takes one qubit, and a blank qubit, and produces two qubits with the same value as the first qubit is impossible. The aforementioned cloning operation is only valid for states that are not superpositions of basis states, which makes sense, as this is effectively just Classical Information.

A similar, and very interesting concept is that of Quantum Teleportation [10, p.26], which allows for communication of some arbitrary quantum state from Alice to Bob. However, in the process the original copy that Alice possess is destroyed, and as such, the No-Cloning Theorem holds[2].

Quantum Teleportation has a lot of very interesting and important applications all across the fields of Quantum Computation and Quantum Information [11].

Quantum Teleportation tangent aside, the concept of the No-Cloning Theorem may seem to prevent us from performing some very useful actions, but perhaps it would be better to consider how the existence of the No-Cloning Theorem could be used in beneficial ways. Indeed, in the next section, we will discuss QKD protocols, which rely heavily on the No-Cloning Theorem for their security.

IV. QKD Protocols

One of the first QKD protocols was the BB84 protocol[3] [12]. This protocol uses the Basis states of the Z and X Bases. This choice was made because for any pair of Basis states, one from each basis, they are maximally non-orthogonal:

$$|\psi_Z\rangle \langle\psi_X| = |\psi_X\rangle \langle\psi_Z| = \frac{1}{2} \tag{4}$$

The protocol begins with Alice generating some random bit-string K, which will serve as the key to be distributed between Alice and Bob. The length of K is typically $2n$, where n is the desired final key length. This is because approximately 50% of K is lost in the process.

Alice now generates another random bit-string of length $2n$, this time called B. This bit-string represents Alice's random choice of either the Z or X Bases.

For each bit i, a qubit Q_i is prepared according to the below scheme:

$$Q_i = \begin{cases} |0\rangle\,, & K_i = 0, B_i = 0 \\ |1\rangle\,, & K_i = 1, B_i = 0 \\ |+\rangle\,, & K_i = 0, B_i = 1 \\ |-\rangle\,, & K_i = 1, B_i = 1 \end{cases} \tag{5}$$

This qubit-string is then transmitted to Bob.

For each qubit that Bob receives, he picks either the Z or X Basis at random, and uses that to measure the qubit. The measurement scheme used, where m_i is the measurement result and X_i is the resulting bit of Bob's key, is given below:

$$X_i = \begin{cases} 0, & m_i = |0\rangle \text{ or } m_i = |+\rangle \\ 1, & m_i = |1\rangle \text{ or } m_i = |-\rangle \end{cases} \tag{6}$$

Once Bob has measured all of the qubits transmitted by Alice, he announces such on a classical channel, which may not be secure, but is at least authentic.

Alice then reveals the bit-string B to Bob, and Bob reveals to Alice for which qubits he made the wrong measurements. They then discard those results, leaving on average n bits out of the $2n$ key bits originally generated. This process is called "sifting" and the resulting key is called the sifted key.

Additional steps can be performed after this to further improve the security of the protocol, namely, Parameter Estimation, Error Correction, Error Verification, and Privacy Amplification [2, p.2] [13, p.80].

Now, let us consider some eavesdropper Eve that is sitting in the middle of both of the quantum and classical channels. She can do whatever she likes with the qubits she intercepts along the quantum channel[4] and she can only observe the transmissions on the classical channel.

The most powerful attack we could conceive of would be an attack where given some incoming qubit from Alice $|\psi_A\rangle$, and an ancillary qubit of Eve's, she could perform the operation:

$$|\psi_A\rangle |0\rangle \xrightarrow{\mathcal{C}} |\psi_A\rangle |\psi_A\rangle \tag{7}$$

This would allow Eve to make a copy of the qubit that is completely independent of the qubit sent by Alice, and copies of that qubit ad infinitum, but as we know from previous discussion, the No-Cloning Theorem prohibits this.

Another QKD protocol of interest is the 3-State protocol [3], which uses only 3 of the 4 states used by BB84, usually the $|0\rangle$, $|1\rangle$, and $|+\rangle$ states.

For this protocol, Alice generates a random bit-string B of length $8n$. For each bit i, she prepares a qubit Q_i according to the following scheme:

$$Q_i = \begin{cases} |0\rangle \text{ or } |1\rangle\,, & B_i = 0 \\ |+\rangle\,, & B_i = 1 \end{cases} \tag{8}$$

where in the case that $B_i = 0$, Alice randomly prepares Q_i in one of the two states $|0\rangle$, $|1\rangle$ with equal probability. She then transmits this qubit-string to Bob.

[2]Quantum Teleportation also illustrates how Quantum Mechanics can't be used to transmit information faster than the speed of light.

[3]Named after Bennett and Brassard who discovered the protocol, and the year in which they published their work, 1984. A quick look over a list of currently known QKD protocols and one might notice that this is quite a common naming scheme.

[4]This ultimately gives Eve a level of attack called a Coherent attack [14, p.7], which is the most powerful type of attack possible.

For each qubit Bob receives, he chooses the Z or X Basis randomly with equal probability to make a measurement with. Once Bob has measured all of his received qubits, he communicates such to Alice over the classical channel. She then publishes the bit-string B over the channel, and Bob announces to Alice which qubits he made incorrect measurements on. They then discard these results, leaving $4n$ results.

Results from qubits measured in the X-Basis are automatically considered check-bits, and Alice announces n of the results from measurements in the Z-Basis to be check-bits. They use these $3n$ check-bits to calculate the Quantum-Bit Error Rate (QBER), which indicates how much interference from Eve there is. Above some threshold value for the QBER, there is too much interference from Eve, and Alice and Bob abort the protocol. This leaves n results measured from the Z-Basis, which give sifted key bits S_i when Bob measures the $|S_i\rangle$ state.

Note that this protocol is not as resource efficient as the normal BB84, as that only requires $4n$ qubits for Parameter Estimation, whereas the 3-State protocol requires $8n$, however the proportion of qubits used for Parameter Estimation for the 3-State protocol is 3 times larger than that used for BB84, and hence a better estimate of the QBER can be obtained.

Also note that in a practical implementation of BB84, should one of the four laser sources fail, the 3-State protocol can be used instead, until such a time that a repair is made [3, p.1].

V. Analysis of QKD Protocols

Typical analysis of QKD protocols provides several useful metrics. Some examples of these metrics are the "Security Threshold", and the Secret Key Rate.

The Secret Key Rate describes how many bits, that remain secret from Eve, are distributed between Alice and Bob. This is usually per transmission, or with physical implementations in consideration, per second[5].

The Security Threshold is the value of the QBER for which the Secret Key Rate becomes 0. This illustrates how much interference there can be from Eve, but also from other sources of error such as noise.

For the BB84 protocol, the Secret Key Rate per channel use is given by [14, p.7]:

$$R_{BB84} = 1 - 2H_2(Q) \tag{9}$$

where Q is the QBER, and H_2 is the Binary Shannon Entropy, given by:

$$H_2(p) = -(p\log_2(p) + (1-p)\log_2(1-p)) \tag{10}$$

If we take eq.9 and set the rate to 0, we get a value of $Q = 0.11$. This means that if there is more than 11% error then the protocol should be aborted.

[5]Bits per second is comparable to the widely seen measures of network speed like Mbps (Mega-bits per second), and so this unit of measurement would perhaps be useful for scientific communication with less technical audiences.

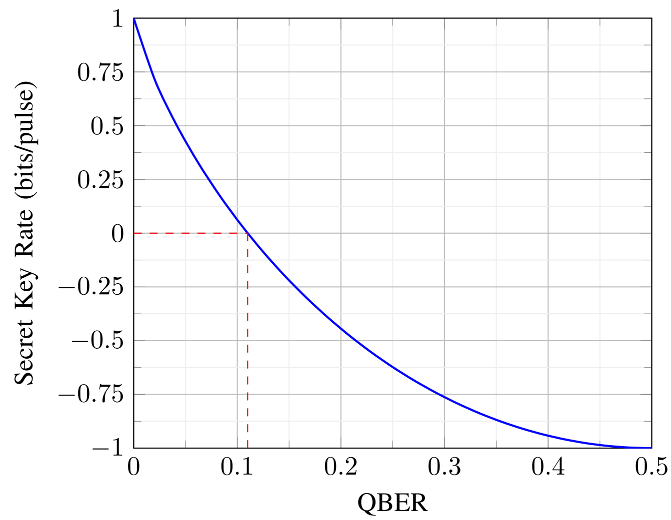


Fig. 1. Plot of eq.9, the Secret Key Rate of the BB84 protocol per channel use. The red dashed line represents the point at which the Secret Key Rate becomes 0, and it's corresponding QBER of 0.11.

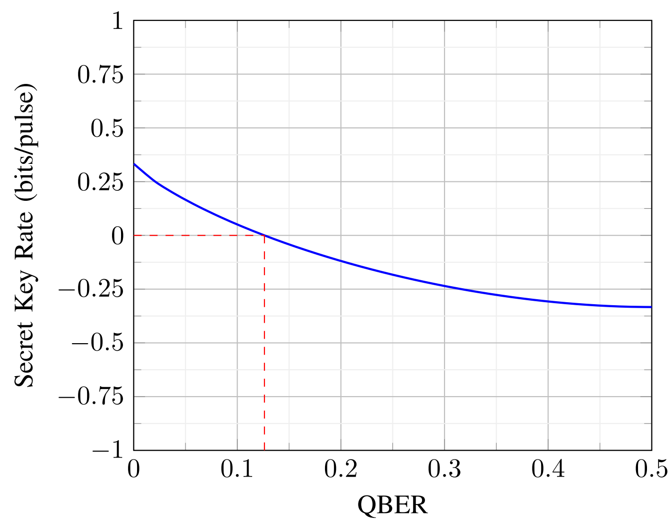


Fig. 2. Plot of eq.11, the Secret Key Rate of the 6-State protocol per channel use. The red dashed line represents the point at which the Secret Key Rate becomes 0, and it's corresponding QBER of 0.1262.

Similar analyses can be performed for other protocols, for instance for the six-state protocol [15] the Secret Key Rate is given by [14, p.8]:

$$\begin{aligned} R_{6state} = \frac{1}{3}\Bigg(1 + \frac{3Q}{2}\log_2\frac{Q}{2} \\ + \left(1 - \frac{3Q}{2}\right)\log_2\left(1 - \frac{3Q}{2}\right)\Bigg) \end{aligned} \tag{11}$$

Setting the Secret Key Rate to 0 this gives a Security Threshold of 12.62%.

VI. Finite-Key Analysis of QKD Protocols

The analyses in the previous sections assume that an infinite number of transmissions are sent between Alice and Bob. However, in a real world implementation of QKD, this is clearly impossible. In addition, some QKD protocols, known as Asymmetric protocols, are much more difficult to analyse. Symmetric and Asymmetric protocols are discussed further in [2, p.2]. As such, finding some other way to perform analysis on QKD protocols through some other means is an important question.

Protocol	Symmetry
BB84 [12]	Symmetric
3-State [3]	Asymmetric
B92 [16]	Asymmetric
MDI [17]	Symmetric
Twin-Field [4]	Symmetric

TABLE I
Symmetry types of different QKD protocols

Bunandar et al. [2] present an approach that uses Von Neumann Entropy, and Smooth Min-Entropy [13] to formulate Semi-Definite Programs (SDPs) [19], which when solved, provide lower bounds on the Secret Key Rate[6]. These analyses provide results for finite numbers of transmissions, and as such we say that they are in the "Finite-Key Regime".

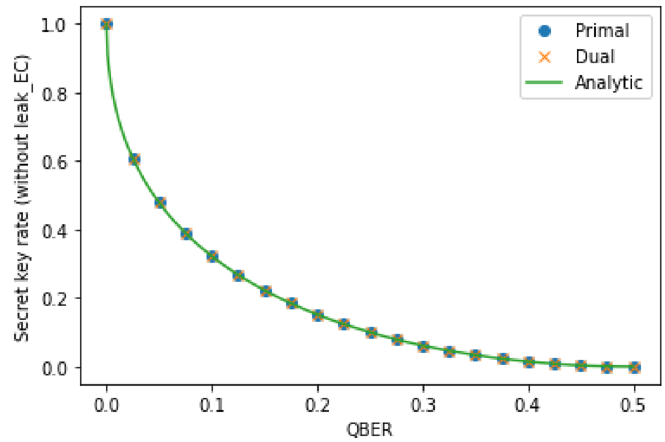
To prove the efficacy of their methodology, they calculate the Secret Key Rate of BB84 using the asymptotic equation given by eq.9, and then calculate Secret Key Rate values for certain QBER values, and plot them together to compare the two. This is shown in fig.3(a). They then go on to perform analysis on the Twin-Field protocol [4] which is shown in fig.3(b)[7].

VII. Ongoing Work

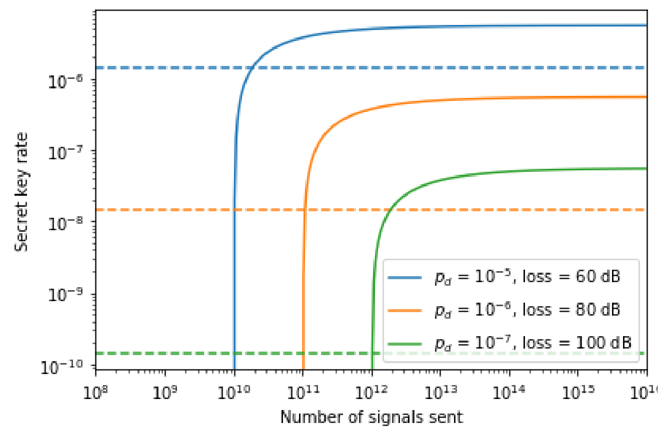
Our work looks at creating a 3-State variation of the Twin-Field protocol. This protocol will then be analysed using the methodology presented by Bunandar et al. The results of these analyses will then be used to benchmark an optics based implementation of the proposed 3-State Twin-Field protocol.

The work into the proposed 3-State Twin-Field protocol is motivated by the fact that to encode 4 Basis States, experimentalists need to use 4 voltages on a phase modulator. As the voltages increase, they become harder to implement, and so if we were able to work without the higher 4th voltage, implementation would be easier. Working with only 3 states also reduces the number of modulated states from 12 to 9 which allows for better data sampling[8], and therefore gives better statistics for each group [21].

Further work will then look at using the methodology provided by Bunandar et al. to analyse QKD protocols within networks of users, rather than just point-to-point communications between two parties.



(a) BB84 Analysis



(b) Twin-Field protocol analysis

Fig. 3. In both graphs, the Secret Key Rate is given per pulse. 3(a) Analysis of BB84 through eq.9 and the method shown in [2]. leak_EC refers to the number of bits revealed to Eve during the Error Correction phase. 3(b) Analysis of the Twin-Field protocol. The dashed lines represent the PLOB bound [18] for their respective values of signal loss. P_d refers to the "Dark Count". Fig.3(b) was generated using code provided in private communications with D. Bunandar.

References

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, "Advances in quantum cryptography," *Advances in optics and photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[2] D. Bunandar, L. C. Govia, H. Krovi, and D. Englund, "Numerical finite-key analysis of quantum key distribution," *npj Quantum Information*, vol. 6, no. 1, p. 104, 2020.

[3] C.-H. F. Fung and H.-K. Lo, "Security proof of a three-state quantum-key-distribution protocol without rotational symmetry," *Physical Review A*, vol. 74, no. 4, p. 042342, 2006.

[6] The work by Bunandar et al. uses code publicly available: https://github.com/dbunandar/numerical_qkd. This code uses python in the form of Jupyter Notebooks, and can use MATLAB and commercially available SDP solvers to accelerate code execution. At the time of writing, this code is provided under the MIT Licence.

[7] It is worth noting that in a real world implementation, typically around 10^8 transmissions are sent, and lower values for the signal loss are expected [20].

[8] 4 states $\times$ 3 intensities = 12 modulated states, which would be reduced down to 3 states $\times$ 3 intensities = 9 modulated states.

[4] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, 2018.
[5] C. Matt and U. Maurer, "The one-time pad revisited," in *2013 IEEE International Symposium on Information Theory*. IEEE, 2013, pp. 2706–2710.
[6] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, ser. Chapman & Hall/CRC cryptography and network security. Bosa Roca: Chapman and Hall/CRC, 2014.
[7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[8] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 1994, pp. 124–134.
[9] P. Penfield, "Information and entropy," May 2022. [Online]. Available: https://eng.libretexts.org/Bookshelves/Electrical_Engineering/Signal_Processing_and_Modeling/Information_and_Entropy_(Penfield)
[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.
[11] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, "Advances in quantum teleportation," *Nature photonics*, vol. 9, no. 10, pp. 641–652, 2015.
[12] 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. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0304397514004241
[13] R. Renner, "Security of quantum key distribution," *International Journal of Quantum Information*, vol. 6, no. 01, pp. 1–127, 2008.
[14] S. Priandola, "Quantum cyber-security," Feb 2020.
[15] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters*, vol. 81, no. 14, p. 3018, 1998.
[16] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical review letters*, vol. 68, no. 21, p. 3121, 1992.
[17] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical review letters*, vol. 108, no. 13, p. 130503, 2012.
[18] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature communications*, vol. 8, no. 1, p. 15043, 2017.
[19] C. Helmberg, "Semidefinite programming," *European Journal of Operational Research*, vol. 137, no. 3, pp. 461–482, 2002.
[20] S. Pirandola, private communication.
[21] M. Lucamarini, private communication.