Quantum Key Distribution: The Twin-Fields Scheme and Quantum Repeaters

Charlie Bushman
Carleton College, Department of Physics, Northfield, MN 55057
(Dated: April 10, 2021)

I. INTRODUCTION TO QUANTUM KEY DISTRIBUTION

The field of quantum cryptography is built on two foundational principles from quantum mechanics that give QKD protocols (theoretically) absolute security. The first principle is the no-cloning theorem which simply states that it is impossible to create an identical copy of a particle. In other words it is impossible to copy quantum information, which means that it can be used to securely transmit information without the possibility of someone else copying it.
The second principle is that a quantum particle can only be known to hold one bit of information at any given time. This means that a quantum bit ("qubit"), which is a continuous variable, can only be known to hold a 1 or a 0 in a certain basis. It is also true that this information will change if measured against a different basis so reading a string of qubits will almost always leave signs of tampering which are obvious to the intended recipient. Taken together, these principles allow for two parties to exchange a secret key over a public network without any third party being able to reliably figure out the key. Many protocols exist for distributing such "quantum keys", the first of which was created in 1984.

A. BB84

In the BB84 QKD protocol, Alice begins with two binary strings, a and b, of length n. She makes an n qubit state,

$$|\Psi\rangle = \bigotimes_{i=1}^{n} |\Psi_{a_i b_i}\rangle \,, \tag{1}$$

that is the tensor product of these n Hilbert spaces where each $|\Psi_{a_i b_i}\rangle$ could be any of the four:

$$\begin{aligned} |\Psi_{00}\rangle &= |0\rangle \\ |\Psi_{10}\rangle &= |1\rangle \\ |\Psi_{01}\rangle &= |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ |\Psi_{11}\rangle &= |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \,. \end{aligned} \tag{2}$$

Alice then sends these n qubits (written as $|\Psi\rangle$) to Bob who then measures them in randomly chosen bases and confirms receipt to Alice. Knowing that Bob has received the qubits, Alice can now disclose the original bases she used for encoding the qubits over a public and classical channel. Bob then throws out all the qubits he measured in the wrong basis and selects a few of the correct bits to compare with Alice's to ensure that his qubits have not been tampered with. If these match up, then the remaining bits that Bob has measured in the correct basis should be the same as those which Alice have so they now have a shared secret key. From here they can continue with classical cryptographic techniques.
The simplest implementation of the BB84 protocol uses photons polarized to 0°, 90°, 45°, and 135° (corresponding to $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$) sent through optical cable.[7] The BB84 implementation with such polarized photons is shown broken into communication steps in Fig. 1.

B. Other QKD Protocols

Many other QKD protocols have been developed since the inception of BB84, including the twin-fields scheme which will be discussed later in this paper. Two other protocols worth mentioning briefly here are decoy-state QKD[2] and KMB09[3], developed in 2003 and 2009 respectively.
The decoy-state QKD scheme proposed by Won-Young Hwang was a major development over BB84 because it was the first scheme to fully address the problem of photon number splitting (PNS) attacks. In BB84, it is possible to carry out statistical attacks such as PNS which become more and more effective over larger distances. This is because increase in distance also increases the intrinsic quantum bit error rate which allows attacks to more easily stay hidden in the noise created by transmittance. The decoy-state scheme has Alice send multiple pulses at different intensities instead of just one and then after measurement by Bob, reveal which pulse was the true qubit. The rest were just decoys to throw off PNS attacks by making them much more easily revealed, even over larger distances.
KMB09 is another development on the principles of BB84 proposed by Muhammad Mubashir Khan which increases the upper bound on the distance achievable while retaining security. In KMB09, Alice and Bob use mutually unbiased bases to encode their qubits which introduces a minimum index transmission error rate (ITER) whenever an eavesdropper is present. The ITER increases greatly for higher dimensional photon states. So the use of higher

QUANTUM TRANSMISSION														
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	↗	↕	↘	↔	↕	↕	↔	↔	↘	↗	↕	↘	↗	↗	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

FIG. 1. An example of 15-qubit BB84 being carried out between Alice and Bob. Here R and D stand for rectilinear and diagonal bases, corresponding to 0°-90° and 45°-135° polarization axes. The public discussion happens over a classical channel. In this case, $k = 6$ bits are matching in the end and $k/3$ are compared to verify.

dimensional photon states allows for more noise in the channel because we are no longer relying on the ∼25% quantum bit error rate that would be the expected result of an eavesdropper in BB84, but with minimal noise in the channel. This increase in allowable noise corresponds to higher achievable distances.

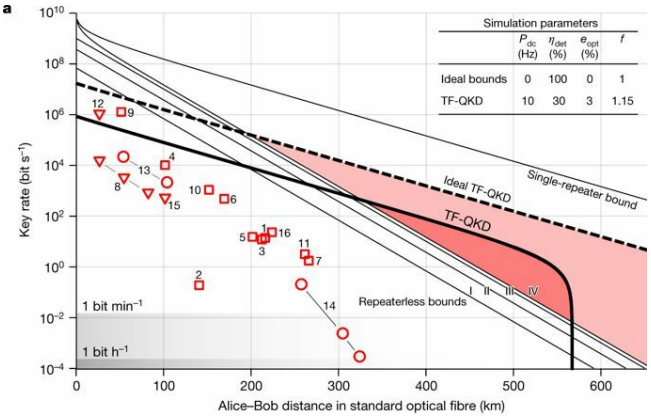

FIG. 2. A logarithmic graph of distance versus log key generation rate. Lines I, II, III, and IV are theoretic bounds on some older models for QKD and the curves composed of shapes are their experimental results. TF-QKD is shown with an ideal upper bound and a more realistic bound that dies off quickly at around 575km. Interestingly, the single-repeater scheme greatly outperforms all others, especially at greater distances.

II. THE RATE-DISTANCE LIMIT

Currently the largest barrier to practical applications of QKD is known as the rate-distance limit, which has been shown to hold for optical QKD protocols without quantum repeaters.[4] This limit on secret key bit generation decays exponentially with distance, making the best-performing schemes for QKD nearly useless (∼1 bit/hr) at distances around 600km. This exponential limit can be seen for a variety of QKD schemes, including the twin-fields scheme and quantum repeater schemes which are discussed later in this paper, in Fig. 2 as well as experimental values denoted by the red shapes.

Figure 2 experimentally verifies that the tested QKD schema will have some exponentially decaying upper bound,[8] but proving that this upper bound exists for all QKD schema is a difficult task, of which a brief overview is given below.

In keeping with the conventions of Takeoka et al., let the private capacity of a quantum channel $\mathcal{N}_\eta$ with transmittance $\eta \in [0, 1]$ be denoted by $P_2(\mathcal{N}_\eta)$. Then the point-to-point bound over a lossy optical channel is given by Eq. 3,

$$P_2(\mathcal{N}_\eta) \leq log_2(\frac{1+\eta}{1-\eta}), \tag{3}$$

in units of key bits per mode. We can also define the squashed entanglement on a channel $\mathcal{N}_{A'\to B}$ by Eq. 4,

$$E_{sq}(\mathcal{N}) = \max_{|\phi\rangle_{AA'}} E_{sq}(A;B)_{\rho}, \tag{4}$$

where $\rho = \rho_{AB}$ is a bipartite entangled state defined by $\rho_{AB} = \mathcal{N}_{A'\to B}(|\phi\rangle\langle\phi|_{AA'})$. The theory that follows, given in Eq. 5, is that the squashed entanglement on a channel $\mathcal{N}$ is an upper bound on the private key capacity of that channel.

$$P_2(\mathcal{N}) \leq E_{sq}(\mathcal{N}). \tag{5}$$

It is also shown that the squashed entanglement on a channel $\mathcal{N}$ scales linearly with transmittance, η. This means that the private capacity of this channel is bounded by something with a decaying exponential dependence on distance, thus providing the rate-distance limit.

III. TWIN-FIELDS QUANTUM KEY DISTRIBUTION SCHEME

The twin-fields (TF) QKD protocol is unique among all other known repeaterless protocols because it exhibits a dependence on half the distance between communicating parties unlike others which exhibit a dependence on the full distance. This is acheived with a scheme that places an untrusted middle man Charlie between Alice and Bob with Charlie having no way to determine the secret key even with the information he has.

A. Background Theory

TF-QKD is set up according to the schematic in Fig. 3 where Alice and Bob are communicating with each other through Charlie, who could be a malicious party without affecting the security of the scheme (almost, see Appendix B). Alice and Bob both release phase randomized optical fields phase-encoded with secret bits and bases (as in BB84) which arrive at Charlie's station which is set up as an interferomter. From the single-photon interference that occurs, Charlie can infer whether the secret bits of the users are equal (00 or 11) or different (10 or 01) but cannot learn their absolute values (0 or 1). The result is then published by Charlie, allowing Alice and Bob to share their phase randomizations, $\rho_{a,b}$. When the phase randomizations align, the result of Charlie's measurement can be used to make a secret key in similar fashion to BB84.

In other repeaterless, point-to-point QKD schema, the key generation rate scales linearly with the channel transmittance, η, when $\eta << 1$ (giving an exponential distance dependence). However in TF-QKD, the key rate scales with $\eta^{1/2}$ which markedly improves the rate-distance upper bound in some regions. This is seen in

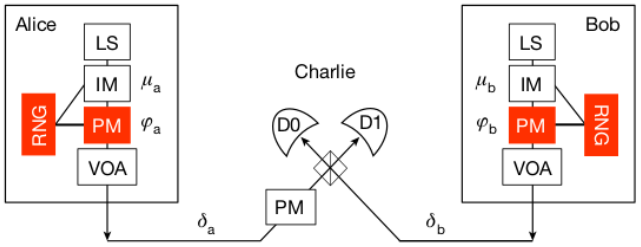

FIG. 3. Directly from source: "Set-up to implement TF-QKD. The light sources (LSs) at Alice's and Bob's stations generate pulses with intensities $\mu_{a,b}$ that are varied randomly by intensity modulators (IMs) to implement the decoy-state technique. Phase modulators (PMs) are combined with random number generators (RNGs) to encode each light pulse with phases $\phi_{a,b}$, which include bit and basis information as well as the random phases $\rho_{a.b}$. The variable optical attenuators (VOAs) set the average output intensity of the pulses to bright (classical regime) or dim (quantum regime). The pulses travel along independent channels, acquiring phase noise $\delta_{a,b}$, to then interfere on Charlie's beam splitter and be detected by the single-photon detectors D0 and D1. Charlie uses the bright pulses in the classical regime and the phase modulator in his station to phase-align the dim pulses that are emitted in the quantum regime, which provide the bits of the key."[4]

Lucamarini et al.[5] in the upper bound that they provide on the TF-QKD key rate, $R^{\neg\rho}_{TF-QKD}(\mu, L)$, in Eq. 6,

$$R^{\neg\rho}_{TF-QKD}(\mu, L) = \frac{d}{M}[R_{QKD}(\mu, \frac{L}{2})]_{\oplus E_M}, \tag{6}$$

where M is the number of phase slices (see next subsection), d is the duty cycle between the classical and quantum modalities (see Supplementary Information in Appendix B), and R_{QKD} is the key rate of a standard repeaterless QKD scheme (notably dependent on $L/2$).

B. Coordinated Phase Randomization

One of the unique aspects of TF-QKD that allows it to remain secure even with Charlie at the midpoint station being an untrusted entity is coordinated phase randomization. While it sounds scary, it is actually a fairly simple principle that allows Alice and Bob to add another layer of randomization to the photons they send, beyond the phase and bit encoding seen in BB84. In TF-QKD, Alice and Bob agree on an integer value M and then each independently split up the phase interval $(0, 2\pi]$ into M phase slices. Each chooses a phase slice, $\Delta_{k(a)}$ and $\Delta_{k(b)}$ respectively, and then once measurement has occurred Alice and Bob will share not only encoding bases but also phase slices. They keep only the measurements where the encoding bases are the same and the phase randomization is in the same slice. This guarantees that the bits measured will be the same, up to an error term introduced by the size of the phase slices.

This intrinsic qubit error rate (QBER), E_m, due to the twin qubits being off by up to a phase slice, is given by Eq. 7,

$$E_m = \frac{M}{2\pi}\int_0^{2\pi/M} sin^2(\frac{t}{2})dt = \frac{1}{2} - \frac{sin(2\pi/M)}{4\pi/M}, \quad (7)$$

where the QBER tends to 0 as $M \to \infty$. However, the probability of matching phase slices scales with $1/M$ so there is a trade-off between lessening quantum error and increasing number of matches. This trade-off is maximal with an M of 16, for which $E_M = 1.275\%$. Knowing this, we can now make sense of the $\oplus E_M$ in Eq. 6 as a correction on the private key generation rate for the QBER introduced by phase randomization.

C. Phase Evolution of Twin Fields

The main technical barrier to implementing TF-QKD currently is the phase evolution of the two qubits as they traverse their separate paths towards Charlie. The differential phase fluctuation can be written in terms of frequency and distance in Eq. 8,

$$\delta_{ba} = \frac{2\pi}{s}(\Delta v L + v\Delta L), \quad (8)$$

where s is the speed of the signals in the optical cables and ΔvL and $v\Delta L$ are the two terms which contribute to the QBER. In the term with Δv, L is assumed to be exactly equal between the two optical cables and in the term with ΔL, v is assumed to be constant between the two light sources. The first term is the difference in frequency between the two qubit sources times distance L (Alice to Charlie or Bob to Charlie). This term actually terms out to make a negligible contribution to the QBER because lasers' frequencies can be very well matched using phase locking techniques. The second term presents more of a problem because the actual paths that photons take through identical length cables can vary substantially. Even over distances an order of magnitude lower than the upper range of TF-QKD, the contribution this term makes to the QBER is significant. This is compensated for by sending two pulses instead of one for each qubit. The first is a 'bright' pulse that allows Charlie with his phase modulator to determine the phase of the following 'dim' pulse with respect to the other pulse coming from the other source. The bright pulse provides calibration and the dim pulse then provides the quantum information.

IV. QUANTUM REPEATERS

While a lot of work has been put into developing better and better repeaterless QKD protocols, the distance limitations on all of them provide a serious barrier against real-world applications. The creation of functioning quantum repeaters would leapfrog this barrier almost instantaneously and start bringing QKD into more common practice. However, the technical and theoretical obstacles in the way of implementing quantum repeaters are many and some seemingly insurmountable. Despite this, a lot of work has been done into the subject in recent years and one interesting potential model is given by Azuma et al. in their paper on all-photonic quantum repeaters.[6]

Unfortunately, this is the last topic to be covered in this paper and time was budgeted poorly so very little is known of this subject by the author. Purely from the abstract, it's worth noting that this design for quantum repeaters does not make use of 'quantum memory', something that is very common among other theoretic quantum repeater designs. They show in this paper that quantum memory is unnecessary if the repeater instead makes use of flying qubits and they provide a protocol based on photonic cluster state machine guns and a loss-tolerant measurement equipped with local high-speed active feedforwards. Anything that involves photonic cluster state machine guns must be worth reading about so the author will be sure to find out more about this at a later date.

V. DISCUSSION

We have now explored a good chunk of the theory behind QKD and some of the technologies used in its implementation but we have yet to ask the question of whether or not this is useful. In short, the answer to this question is no, for now.

The current state of cryptographic theory is that RSA, the classical scheme used by most modern communication protocols that need the highest level of security, is as close to unbreakable as we care to make it. While it remains unproven, breaking RSA is thought to be NP-hard which means that the difficulty of breaking it increases exponentially with the size of the inputs. However, NP-hard problems are often ones that lend themselves to quantum algorithms. In fact, Shor's algorithm for factoring has been proven to be efficient on quantum computers such that a large enough quantum computer could theoretically break RSA encryption in real time, rendering what would be classified as 'secure' communications insecure. The effects of this are obviously going to be sizeable.

With that in mind, it's worth looking at how close anyone is to having a quantum computer of this power. Luckily, it is still far away from the reaches of even the best funded labs, but progress towards that goal is not just being made, it is accelerating. So it is reasonable to assume that in the most extreme case, some of us could be seeing this as a real problem within our lifetimes. In this scenario, we will have a need for functional and accessible QKD protocols to communicate securely and for them to work across potentially global distances.

So we know that currently QKD protocols are irrelevant to communication security but that they could, potentially very suddenly, become critical. This places us in the interesting position of having to establish the technology and infrastructure to cope with this global problem before it happens. That is a daunting task. What gives me hope that it is achievable is that throughout the history of classical computing so far, the race between attackers and defenders has always remained fairly balanced. If one got out of hand, either the other would have to catch up or the whole system would go away. I think it's quite likely that QKD will be a part of this pattern rather than the thing that breaks it.

APPENDIX A

This appendix will house descriptions of various topics of interest to the rest of the paper or more in depth foundations than are given in the paper itself.

A. BB84 in Detail

BB84 is the first provably secure QKD scheme, published in 1984 by Charles H. Bennett and Gilles Brassard.[1] It has set the stage for all following development in the field and has a relatively simple framework that can be used as a good introduction to the mathematical framework behind QKD. We will consider two parties, Alice and Bob, who want to communicate and a third party, Eve, who wants to eavesdrop. Alice and Bob have access to a means of transmitting quantum information and a classical communications channel. Eve can look at everything on both channels, but for simplicity cannot interfere with the classical channel.

Alice begins with two binary strings, a and b, of length n. She makes an n qubit state given by the tensor product in Eq. 1 where each $|\Psi_{a_i b_i}\rangle$ could be any of the four states from Eq. 2.

What you'll now notice is that the basis of $|\Psi_{a_i b_i}\rangle$ is completely determined by b_i. In other words, b_i determines if $|\Psi_{a_i b_i}\rangle$ is written as $|1, 0\rangle$ or $|+, -\rangle$. Also, these bases are non-orthogonal, so it is impossible to experimentally determine which state a $|\Psi_{a_i b_i}\rangle$ is in. Now this $|\Psi\rangle$ (Eq. 1) is sent to Bob and arrives to him in state $\varepsilon(|\Psi\rangle\langle\Psi|)$ where ε is a stand-in for noise in the channel and any eavesdropping that Eve has carried out. So now there are two possibilities for the state of the problem, either Eve has made measurements on $|\Psi\rangle$ or not.

If Eve wants to make measurements on $|\Psi\rangle$, she will have to correctly guess the basis in which to measure each $|\Psi_{a_i b_i}\rangle$ or else risk collapsing the wavefunction into a different state. The probability of guessing correctly is one in two, so the probability of measuring $|\Psi\rangle$ without causing any change to the state is $\frac{1}{2^n}$, which quickly becomes unreasonable for sufficiently large n. Discrepancies between what Bob receives after Eve's measurements and what Alice has sent will cause the two of them to recognize the tampering and start over.

If instead Eve does not try to measure $|\Psi\rangle$, then she cannot possibly have a copy of $|\Psi\rangle$ by the no-cloning theorem. So Bob receives a $|\Psi\rangle$ and randomly generates a binary string b' of length equal to b. He then measures $|\Psi\rangle$ using b'_i as a basis at each $|\Psi_{a_i b_i}\rangle$. At this point Bob announces publicly that he has received $|\Psi\rangle$ meaning that it is now safe for Alice to publicly share the b that she generated initially. Alice and Bob compare b and b', throwing out any bits where $b_i \neq b'_i$. Alice then randomly chooses $k/2$ of the remaining k bits and compares with Bob over public channels to make sure they are the same (up to some error due to noise). If they are suitably close, they can proceed with key generation and other classical cryptographic techniques using the other $k/2$ bits that are still secret.[9] If they are too far removed, Alice and Bob will assume tampering by Eve and start over.

B. Quantum Coin Tossing

The last couple pages of Bennett's and Brassard's paper on the BB84 protocol explore a different problem in communication theory through the lens of quantum mechanics. This problem, traditionally known as the coin flipping problem, is how two un-trustful parties Alice and Bob can fairly flip a coin without giving either side the opportunity to cheat. This is achievable with just a classical communications line but it is not provably cheat-proof and advancements in the field of computability could give one or the other a chance to cheat. Interestingly, unlike in the case of QKD where the BB84 protocol is provably secure, their algorithm for coin flipping over a quantum channel could also be subject to cheating with sufficient advancement in quantum theory/technology.

Working on similar principles to BB84 QKD, quantum coin tossing begins with Alice randomly generating a string of bits and then encoding them all in one basis (the two options in the paper are called 'rectilinear' and 'diagonal'). These qubits are then sent to Bob who measures half in one basis and half in the other. Bob then sends his guess as to the basis that Alice originally encoded the qubits in, which is a 50-50 guess. Alice then reveals that Bob was either right or wrong and to confirm this to Bob, she sends her original string of bits. If the bits that Bob measured in what Alice claims is the correct basis match the corresponding bits that Alice sends, then Bob knows Alice could not have cheated unless she correctly guessed all of the random outcomes of the measurements Bob made in the wrong basis. Thus the algorithm is theoretically cheat-proof.

The problem with this technique is the Einstein-Podolsky-Rosen Paradox (EPR), more commonly known as entanglement. An EPR photon pair is entangled such that when the polarization of one is measured in a given basis, say the 0°-90° basis, then the other photon must have the other polarization, no matter how far away it

is from the measurement of the first. This means that if Alice were to generate an EPR pair, send one photon to Bob, and keep its counterpart between a pair of perfectly reflecting mirrors, then when Bob guessed correctly, Alice could measure her preserved photon in the other basis and report the opposite of that value to Bob, which will match up with what he measured in the basis he didn't guess. This process can be seen in the example given in Fig. 4.

Luckily for Bob, at the time this paper was written in 1984, the technology required to preserve the thousands of EPR photon pairs used in this algorithm was no where near where it would have to be for Alice to consistently cheat. More often she would lose some photons, have to guess their values, and lose if she guessed any wrong. Whether or not this technological limit is still in place today is beyond the scope of this paper, unfortunately.

APPENDIX B

Appendix B contains further reading suggestions for a more in depth look at certain subjects that couldn't be covered.

C. Proof of the Rate-Distance Limit on Repeaterless Optical QKD Protocols

The full proof of the rate-distance limit on repeaterless optical QKD protocols is given in detail in the paper by Takeoka et al.[4]. It requires quite a bit of familiarity with quantum/classical information theory and with the some other techniques employed in QKD protocols such as decoy states.

D. Twin-Fields Scheme Supplementary Information

Supplementary information on TF-QKD can be found at https://www.nature.com/articles/s41586-018-0066-6Sec3. This includes a more in depth look at the protocol itself and an exploration of potential security holes in the protocol.

ACKNOWLEDGMENTS

Thanks to Arjendu for assigning this project and for teaching me enough to understand it.

[1] Bennett, C.H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. International Conference on Computers, Systems, and Signal Processing **1**, 175-179, (1984).

[2] Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Physical Review Letters **91**, 5, (2003). http://dx.doi.org/10.1103/PhysRevLett.91.057901

[3] Mubashir Khan, High error-rate quantum key distribution for long-distance communication. New Journal of Physics, **11**, (6), (2009). http://dx.doi.org/10.1088/1367-2630/11/6/063043

[4] Takeoka, M., Guha, S. & Wilde, M. Fundamental rate-loss tradeoff for optical quantum key distribution. Nat Commun 5, 5235 (2014). https://doi.org/10.1038/ncomms6235

[5] Lucamarini, M., Yuan, Z.L., Dynes, J.F. et al. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature 557, 400–403 (2018). https://doi.org/10.1038/s41586-018-0066-6

[6] Azuma, K., Tamaki, K. & Munro, W. J. All-photonic intercity quantum key distribution. Nat. Commun. **6**, 10171 (2015). https://arxiv.org/abs/1309.7207

[7] Note that because photon polarization is a complex 2-dimensional Hilbert space, there is also a third pairing of bases $|R\rangle$ and $|L\rangle$, but they are extraneous in the case of this algorithm.

[8] This is a 'weak-converse' upper bound. This means that there are theoretic schemes for overcoming the bound, for example schemes involving trusted intermediaries, but these schemes are no longer provably secure because of the introduction of 'trusted' third parties.

[9] The simplest way to proceed once both Alice and Bob have a shared, secret string of bits is to simply use these bits as a one-time pad, a well known technique in classical cryptography.

Alice's bit string	1	0	1	0	0	1	1	1	0	1	0	1	1	0	0
Alice's random basis							Rectilinear								
Photons Alice sends	↕	↔	↕	↔	↔	↕	↕	↕	↔	↕	↔	↕	↕	↔	↔
Bob's random bases	R	D	D	D	R	R	D	R	R	D	R	R	D	D	R
Bob's rectilinear table	1					1					0				0
Bob's diagonal table		0		1						1			0		
Bob's guess							'Rectilinear'								
Alice's reply							'You win'								
Alice sends her original bit string to certify	1	0	1	0	0	1	1	1	0	1	0	1	1	0	0
Bob's rectilinear table	1					1					0				0
Bob's diagonal table		0		1						1			0		

FIG. 4. In this example of quantum coin tossing, Alice begins by randomly generating a bit string and then encoding this bit string in the rectilinear basis (corresponding to the $|1\rangle$-$|0\rangle$ basis, whereas 'diagonal' corresponds to the $|+\rangle$-$|-\rangle$ basis). Bob then chooses a random basis for each qubit and measures it. He then sends Alice his guess of bases used for the original encoding. Alice replies with the basis she used and the original bit string to certify. This method is cheat-proof (ignoring EPR) and offers both parties a 50-50 chance of winning.