# Gravitational Attacks on Relativistic Quantum Cryptography

Jayson Lynch[*]

December 21, 2015

**Abstract**

This paper looks at the recent field of relativistic quantum cryptography, which uses quantum mechanics and relativity to produce guarantees about cryptographic security. We analyze some of their security assumptions in these protocols particularly those of Minkowski space-times and perfect knowledge of the communication path. We show how an attacker could use the gravitational bending of space-time to break these cryptographic protocols. We also discuss measures to make this more difficult and some situations in which these attacks are not feasible.

**Keywords:** Quantum Cryptography; Relativistic Quantum Cryptography, General Relativity

## 1 Introduction

In physical cryptography the objective is to obtain 'unconditional' security guarantees which are free from computational complexity assumptions but instead rely on physical laws. The laws of quantum mechanics allow us to set up physical situations where, for example, one can securely agree on a secret key over an insecure communication channel. Although quantum cryptography is quite powerful, it does have limitations. First, many quantum cryptographic protocols depend on having both communication channels and detectors with low noise or idealized qubit sources such as single photon emitters. Attacks which exploit the noise in real implementations have even been carried out experimentally [GLLL$^+$11]. One may wonder if additional physical assumptions can lead to more robustness of these cryptographic schemes. Second, the Mayer-Lo-Chau no-go theorem states that quantum bit-commitment is impossible [May97, LC97]. Relativistic quantum cryptographic protocols use the physical limitations imposed by the theories of quantum mechanics and relativity to ensure security. For example, there are quantum key distribution schemes that can operate in arbitrarily noisy channels [Mol11]. In addition, there are several relativistic quantum bit commitment schemes, showing we can produce cryptographic primitives known to be impossible with just the assumptions of quantum mechanics [Mola, LKB$^+$13, HK04, Ken99]. In this paper, we discuss some relativistic quantum key distribution schemes and consider some of their assumptions. In particular, we look at what might be done by an attacker if one does not assume space-time to be Minkowski and that the participants must measure their location. We then observe ways in which gravitational fields may be used by an attacker in such situations.

[*] MIT Computer Science and Artificial Intelligence Laboratory, 32 Vassar Street, Cambridge, MA 02139, USA, jaysonl@mit.edu.

## 2 Relativistic Quantum Key Distribution Protocols

The first relativistic quantum key distribution scheme seems to be Goldenberg and Vaidman [GV95] in 1995 where they use it to increase the security of schemes using orthogonal states. Molotkov and Nazin propose a new scheme in 2001 [Molb] which allows for key distribution in noisy channels. The scheme and arguments are significantly simplified in a later paper [Mol11] and proven to be work with arbitrarily large noisy channels. The protocol is implemented in an experiment with the help of Radchenko, Kravtsov, and Kulik [RKKM14]. We will use this protocol as our primary example when thinking about gravitational attacks, so we will describe it in some detail. This scheme is based on the Bennett '92 protocol [Ben92]. For this protocol Alice and Bob are assumed to exactly know their relative locations and thus the distance between them. They must also have synchronized clocks, which can be performed with the cryptographic setup. Bob begins the communication by sending a laser beam to Alice. Alice then takes the light and splits it, immediately sending back half of it as a reference beam. The other half she attenuates, encodes a quantum state in the polarization of the light, randomly decides to phase shift by a fixed amount, and sends after some fixed time delay $\Delta t$ which is less than their distance $t$ between Alice and Bob. Bob knows how long it should take the signal to get back to him and confirms that the reference beam arrives on time. He randomly decides whether or not to phase shift it and then puts it in a delay circuit to await the encoding signal. If the encoding signal also arrives on time, they are sent into the interferometer and will either interfere constructively or destructively. If they interfere constructively, giving a large signal, he makes a measurement and records the result. If this is not the case, Bob throws out that message. Since the lasers propagated at the speed of light and Bob knows how long they should take to travel to Alice and back, he can be assured that it is impossible for Eve to measure the encoding signal and then alter the reference beam. If Eve measures the signal beam without altering the reference beam, then Bob will not see the expected interference and know to throw out the signal. If Eve decides to interfere with the reference beam she cannot yet know anything about the signal beam. Whichever choice she makes, then Bob's measurement fails with probability 1/2. One more adjustment is needed to prevent Eve from preempting these communications and simulating both Bob and Alice. In each communication block Bob will randomly decide to initiate immediately or to wait. Alice and Bob can then compare a transcript of whether they had communicated at the early or late time in each block. It is easy to see that Eve cannot perform a single-bit intercept transmit attack, even in the presence of a noisy channel. Molotkov also gives a proof that the protocol remains secure against collection attacks, ones in which Eve intercepts the signals, performs some unitary transform on them possibly entangling qubits she keeps, and waits to make measurements on her entire ensemble of qubits gathered during the key distribution.

In a 2005 paper, Barrett, Hardy, and Kent [BHK05] introduce a relativistic quantum key distribution protocol based on Bell's Inequality and the monogamy of non-locality. They assume a perfect source and lossless channel, but introduce a more powerful 'postquantum' attacker. The postquantum attacker is allowed to violate quantum mechanics in a limited way which forbids superluminal signaling. Similarly, the postquantum attacher could be simulated by an attacker with limited access to manipulating the equipment in Alice and Bob's secure laboratories. In this model, Eve is allowed to provide to Alice and Bob samples in arbitrary quantum states before the protocol starts. These specially prepared quantum states will be used by Alice and Bob instead of the states they thought they had started with. One can imagine this being implemented by Eve having compromised Alice and Bob's initial quantum source, but not their other equipment. It is not possible to construct these states afterward, since they can depend on what transforms Alice and Bob make before sending them from their lab. This attack is foiled by Alice creating entangled pairs with her encoded information which will be sent to two space-like separated labs controlled by Bob. They will then perform measurements as in Bennett ‘84 or another classic quantum cryptography scheme, with the additional check that there is a Bell's Inequality violation. Since one each side of the entangled particles provides no information by itself, Eve cannot learn anything without having classically correlated the two particles. Thus Eve's information is bounded by the deviation from the expected Bell's Inequality violation toward classical correlation.

# 3 Attacks on Relativistic Quantum Key Distribution Protocols

The core tool in relativistic quantum cryptography is the inability of space-like separated regions to share information. For the speed of light to be relevant, the spatial locations of the participants is almost certainly important. This manifests itself in a few different style of assumptions which generally end up amounting to the same thing. The most standard seems to assuming the space-time geometry is (nearly) flat and that the participants know their precise location in space-time. This is generally used to ensure that there is a space-like separation between some events. Another useful property is that Alice and Bob have synchronized clocks, which is necessary for protocols that require checking elapsed times.

In daily life, knowing where one is seems like a simple and obvious assumption to make; however, the participants often need to know their location to a high precision which is not so simple in a relativistic setting. This is further complicated with the introduction of gravitation. In general, there are two different methods of determining one's location: odometry or reference locations. For odometry, one must start at a know location (perhaps Alice and Bob meet up in person) and then carefully tracks their velocity and acceleration, allowing them to calculate their position at any time. This method suffers from two issues. First, any errors in measuring one's velocity will lead to a spatial error that grows with the time elapsed and thus the distance traveled. Worse, if one can only measure acceleration, which is frequently the case, then errors accrue quadratically. Second, without external reference, being in a gravitational field is indistinguishable from accelerating proportional to that field. Thus, if one determines their acceleration by measuring it directly, and not by, say, calculating their thrust based on the fuel being used, then Eve could very well be constructing a gravitational field that convinces Alice and Bob they are farther apart than they actually are. Note, one may believe this isn't an issue, since Eve is in fact accelerating Alice and Bob with the gravitational field, and non-relativistically this would be correct. Unfortunately, since gravitational fields cause Alice and Bob's clocks to run slower, their perceived acceleration is greater than that measured by an outside observer. An extreme example of this is seen when crossing the event horizon of a black hole, where the falling party will see themselves fall right through the event horizon but an outside observer will see them slowing down and never reaching the event horizon. Localization based on other reference objects also suffers from some difficulties. First, one must know the relative locations of the reference objects to the necessary precision. Second, gravitational fields both slow and curve signals. Thus, it is conceivable that Eve can manipulate either distance or angle measurements of the reference points.

## 3.1 Gravitational attacks

We now split up two categories of attacks, those primarily manipulating the space in which Alice and Bob (or their agents) reside and those primarily interfering with the intermediate space. If Eve is able to manipulate the space Alice and Bob are in, she can potentially manipulate their measurements of location and time with respect to other participants. However, any gravitational field strong enough to alter Alice and Bob's measurements in a significant way should be detectable by measuring similar physical phenomena. Some care should be taken to think about what measurements need to be made and the precision of the techniques available, but we will not consider this style of attack in further detail.

Now we will look at some things that can be done by adding gravitational fields. Two useful phenomena that come out of general relativity are gravitational lensing and gravitational time dilatation. An observer far away from a gravitational field will see light curve in the presence of a gravitational field. They will also see light appear to slow down, and will note that any observers in that field will have clocks that run proportionately slower. Since the speed of light need only be constant in a local region, it is quite possible for it to take a longer time to traverse a region as seen by a far away observer. Similarly, a light beam may be taking a path that is a geodesic along the surface of space-time, but seems to be longer than is necessary if that region had been perfectly flat. We will now perform some rough calculations to show that Eve should be able to exploit these phenomena to fool Alice and Bob and subsequently break their cryptographic scheme.

Due to the difficulty of working with the Einstein Field Equations will will be making a number of simplifying assumptions which may not be valid for all setups of these cryptographic protocols, but hopefully suffice as a proof of concept for the attacks. We will be examining the Schwarzchild Metric, which is the solution to the Einstein Field Equations for a single, stationary point mass. As long as all of the masses are far away from each other compared to their effect, this approximation will hold. In general we will follow Hartle's notation and derivations [Har02]. The Schwarzchild Metric is described by the equation

$$ds^2 = -(1 - \frac{2M}{r})dt^2 + (1 - \frac{2M}{r})^{-1}dr^2 + r^2(d\theta^2 + sin^2\theta d\phi^2)$$

Where $M$ is the mass, $r$ is the distance from the mass, $s$ is the proper distance, $t$ is time, and $\theta$ and $\phi$ are spherical coordinates centered on the point mass. From this equation and the conservation of energy and momentum Hartle derives the relativistic orbit of a particle of (effective) mass $m$ at radius $r$ around the much larger central mass $M$ with gravitational constant $G$, speed of light $c$, proper time $\tau$ and angular momentum $L = mr^2 sin^2\theta \frac{d\theta}{d\tau}$.

$$E = \frac{m}{2}\left(\frac{dr}{d\tau}\right)^2 + \frac{L^2}{2mr^2} - \frac{GMm}{r} - \frac{GML^2}{c^2mr^3}$$

One could numerically integrate this solution, or, since we don't want our signals in orbit, we could take a far-field approximation (essentially saying $r$ is large so we'll do a first order Taylor series expansion around it) and obtain that the deflection of light around a mass is approximately

$$\Delta\phi = \frac{4GM}{c^2r} = 2\frac{r_s}{r}$$

The far-field approximation will similarly yield a time-delay of

$$\Delta t = \frac{2GM}{c^3}\left[\log\left(\frac{4r_ir_f}{r^2} + 1\right)\right]$$

Where $r_i$ and $r_f$ are radii at the source and destination of the signal, and $r_1$ is the ratio of the radius of closest approach to the Schwarzchild radius. Interestingly, the deflection of light depends not directly on the mass used, but instead on the ratio of the Schwarzchild radius to the distance of the photon from the center of mass. This means our critical parameter when dealing with deflection is really the mass density. For a normal mass like the Sun, we see a deflection of about one part in a billion near it's surface. However, if Eve is able to create micro-black holes then the deflection becomes entirely dependent on how precisely Eve can place her black holes. If one is worried about the far field approximation, we note that the higher order terms of the Taylor series will only help Eve by increasing the deflection. If we take the Plank mass $m_p = 2.18 * 10^-8kg$ to be the smallest black hole possible then the smallest Schwarzchild radius $r_{min} = \frac{2Gm_p}{c^2} = 3.23 * 10^-35m$, about twice as large as the Plank length. Thus if Eve can place things precisely, she can work with very small masses, which will take very little energy to move and be very hard to detect at any significant distance. Actually constructing Plank-scale black holes is left as an exercise for the reader.

We now suggest the following attack on Molotkov's cryptographic scheme. We will use three small black holes to reroute signals sent between Alice and Bob so they are sent on a longer triangular path created by the first two black holes and realigned by the third. Eve places herself in the middle of two such triangles. When Alice and Bob measure their distance, they will see the gravitationally elongated distance. Now when the protocol begins Eve delays Bob's signal normally. When Alice sends the return signal, the first beam is sent along the first elongated triangle; however, as soon as it passes, the black holes are readjusted so the second beam takes a shorter path by at least the time delay between them $\Delta t$. Eve is now able to look at both signals concurrently and perform the standard intercept-transmit attack. Eve then sends the signals on their way to be 'corrected' to have the correct delay by the second set of black holes. The same principles can be applied to the Kent protocol. The laboratories that are supposedly space-like separated had their measurements manipulated by micro black holes. Eve ensures one is actually closer than the other, allowing her to delay signal A, go to laboratory B, performs a manipulation, and then travel to laboratory A and perform another manipulation. In general, a gravitational field, even of very small strength, can make a photon take arbitrarily long to pass between two points (assuming their distance is large enough for quantum effects to be ignored).

### 3.2 Negative Energy Density

We would like to make a short note of another distinction. General Relativity admits both positive and negative curvature of space-time, corresponding to positive and negative energy densities in a region [Gut02]. It is not currently known whether large amounts of negative energy are physically realizable. However, it potentially allow wormholes, closed time-like curves [MTY88], and warp-drives [Alc94]. All of these should allow Eve to violate any reasonable security assumption based on special relativity. If Eve has access to this technology, we believe she will have much more interesting things to do than attempt to eavesdrop on Alice and Bob.

### 3.3 Counter measures

There are a number of strategies that Bob and Alice can employ to make it more difficult for Eve to perform a gravitational attack. First, Alice and Bob can set up gravitational detectors in their laboratories. This will prevent Eve from manipulating their local space-time to any significant degree. Further, it restricts the amount of mass at a given distance Eve is able to employ without detection. They can also set up gravitational wave detectors, since accelerating a mass will produce a gravitational wave. Unfortunately, gravitational waves produce very small effects and as long as Eve is able to carefully place her mass we saw she does not need to use large masses.

Earlier we discussed some of the difficulties with localization; however, Alice and Bob do have some advantages here. If they are able to detect or set up additional reference points, then for Eve to fool them about their distance from each other she must make make all (or at least most) of these measurements consistent and false. This potentially leads to a lot of agents setting up a lot of black holes if we want to keep Alice and Bob completely in the dark. To make this even less feasible, Bob and Alice can potentially deploy a measurement device a small distance away (one in which they are convinced Eve is not interfering, potentially just opposite ends of their Lab) and take simultaneous measurements from both of these locations. If these are sufficiently far or measurements are sufficiently precise, the number of corrections Eve needs to make now grows as the product of the number of reference and measurement points.

The final advantage we see Alice and Bob having comes from the fact that the cryptographic schemes so far tend to rely on ensuring that events are space-like separated and thus have some leeway. Let us assume Alice and Bob can measure their location to a precision $\delta$. Let us assume that their relevant separation is $t$. For example, this is the space-like separation between Alice's agents in a bit commitment scheme, or the time delay in the key distribution scheme. They then calculate that they should measure a separation $t_m$ if the space between them is Minkowski. They instead measure some $t'$. Since Eve can only make distances appear larger, we can now bound the error that can be introduced $t_e = t' - t_m + 2\delta$. Alice and Bob now determine whether they can tolerate that amount of change in their protocol. For example, if the time delay in Molotkov's secret key distribution protocol $\Delta t > 2t_e$ then Eve cannot delay the reference signal for long enough to manipulate both the encoding and reference signals without alerting Alice and Bob. In this case they can proceeded with safety. If $t_e$ is too large then they abort the protocol and either move, refine their parameters (perhaps by increasing $\Delta t$), or investigate the cause of the unexpected measurements.

## 4 Conclusion

In this paper we discuss a number of relativistic quantum key distribution protocols and examine their assumptions with respect to locality and space-time. We show that precise knowledge of one's space-time coordinates and the curvature of the space between the participants are non-trivial assumptions. We suggest possible gravity based attacks that might violate these assumptions and propose some counter-measures for these attacks. We would also like to note that many of the attacks simply relied on delaying signals to change the participants belief in their relative location, thus allowing two events to have a world-line between each other when they were assumed to be space-like separated. In general, this type of change does not need to use gravity and could be carried out with simple delay circuits. What methods would be more effective depends on the details of the protocol used by the participants and the resources of Eve. Hopefully this discussion will lead to thought and care with respect to how localization is performed in the context of relativistic quantum cryptography and the search for schemes that are more robust to different space-time geometries.

## Acknowledgments

I thank Scott Aaronson for teaching 6.S899 Physics and Computation, without which this paper would never have happened.

## References

[Alc94] Miguel Alcubierre. The warp drive: hyper-fast travel within general relativity. *Classical and Quantum Gravity*, 11(5):L73, 1994.

[Ben92] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121, 1992.

[BHK05] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Physical Review Letters*, 95(1):010503, 2005.

[GLLL$^+$11] Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature communications*, 2:349, 2011.

[Gut02] Alan H Guth. Inflation and the new era of high precision cosmology, 2002.

[GV95] Lior Goldenberg and Lev Vaidman. Quantum cryptography based on orthogonal states. *Physical Review Letters*, 75(7):1239, 1995.

[Har02] James B Hartle. *Gravity: an introduction to Einstein's general relativity*. Pearson Education India, 2002.

[HK04] Lucien Hardy and Adrian Kent. Cheat sensitive quantum bit commitment. *Phys. Rev. Lett.*, 92:157901, Apr 2004.

[Ken99] Adrian Kent. Unconditionally secure bit commitment. *Phys. Rev. Lett.*, 83:1447–1450, Aug 1999.

[LC97] Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410, 1997.

[LKB$^+$13] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden. Experimental bit commitment based on quantum communication and special relativity. *Phys. Rev. Lett.*, 111:180504, Nov 2013.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical review letters*, 78(17):3414, 1997.

[Mola]

[Molb]

[Mol11] SN Molotkov. Relativistic quantum cryptography. *Journal of Experimental and Theoretical Physics*, 112(3):370–379, 2011.

[MTY88] Michael S Morris, Kip S Thorne, and Ulvi Yurtsever. Wormholes, time machines, and the weak energy condition. *Physical Review Letters*, 61(13):1446, 1988.

[RKKM14] I V Radchenko, K S Kravtsov, S P Kulik, and S N Molotkov. Relativistic quantum cryptography. *Laser Physics Letters*, 11(6):065203, 2014.