CHAPTER 4

THE IMPRACTICALITY OF THE ONE-TIME PAD FOR EVERYDAY QUANTUM-SECURED COMMUNICATIONS

Here, we will justify our choice to use the Advanced Encryption Standard running in Galois/Counter Mode (AES-GCM) for encrypting data in chapter 3, as it will form the foundation for the rest of this thesis. Since its inception, quantum key distribution (QKD) has been seen as a method for achieving mathematically unbreakable communications by using it in conjunction with the one-time pad (OTP) [100, 101]. While the importance of a provably-secure method for sharing a single-use key is undeniable for the most sensitive of communications [102, 103], the impact on everyday security is less clear. Many recognise that, for the time being at least, it will be necessary to continue using computationally-secure alternatives, because even cutting-edge QKD systems still have relatively low secret key rates [104–106]. However, very little has been said on when these alternatives can be superseded by the OTP, if at all.

In sections 4.1 and 4.2, we present two arguments as to why it is unlikely that single-qubit discrete-variable quantum key distribution (DV-QKD) will ever be used with OTP encryption in generic networks. Although there are steps that can be taken to improve these odds, they will be challenging to accomplish before the deployment of quantum-safe cryptography becomes a critical concern, and commercial entities will need to be persuaded that the financial impact is worth bearing.

Of course, there are other forms of QKD to which our arguments may not apply. Full analyses of continuous-variable quantum key distribution (CV-QKD) [107], higher-dimensional QKD [108, 109] and floodlight quantum key distribution (FL-QKD) [110, 111] are outside the scope of this thesis, however some preliminary details will be given in section 4.4.1.

It should also be noted that responsibility for everyday information-theoretic security does not fall solely on the shoulders of QKD. Advances must also be made with respect to the OTP,

and section 4.3 summarises the developments required for it to become a widespread method of encryption, assuming there exists some efficient way of distributing key.

4.1 The Effect of the Classical Channel on Key Generation

We begin by considering an element of QKD that has not been focused on in the past. It is implicitly assumed that networks in need of quantum security will have enough capacity to support the classical QKD channel, however this is not necessarily true. We introduce the following condition which, while seemingly arbitrary in the amount of unsecured data, is a logical starting point that enables the development of a more refined model for fully evaluating the classical requirements imposed by QKD.

Condition 4.1: *Assume an unsecured link constantly operates at half its classical capacity, and quantum signals can be injected without generating any secondary artifacts that affect this. We can encrypt all data using a QKD-keyed OTP without artificially capping the classical data rates or increasing the network capacity, so long as $R_{c/s} \leq 1$, where $R_{c/s}$ is the number of bits that must be sent across the classical QKD channel for every bit of secret key that is generated.*

The Gottesman-Lo-Lütkenhaus-Preskill (GLLP) security proof against general attacks on Bennett-Brassard 1984 (BB84) [112] provides an equation for the secret key rate that can be re-written in terms of physical parameters [113] such that

$$R_{s/p} \geq \zeta \left[-Q_\mu H_2\left(E_\mu\right) + Q_1 \left[1 - H_2\left(E_1\right)\right]\right] \tag{4.1}$$

Here, $R_{s/p}$ is the number of secret bits transmitted per weak coherent pulse. If N is the number of pulses transmitted by Alice then ζ is the fraction of these that contribute to the sifted key (~ 0.5 for vanilla BB84, or less if decoy states are used). $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function, while E_μ and E_1 represent the total and single-photon quantum bit error rates (QBERs) respectively. Q_μ is the probability of Bob experiencing a detection given he and Alice used the same basis and

$$Q_n = Y_n \frac{\mu^n}{n!} e^{-\mu} \tag{4.2}$$

where Y_n is probability of Bob experiencing a detection given Alice transmitted an n-photon state. Therefore Q_1 corresponds to single-photon states.

The number of classical bits that must be communicated for every pulse is given by

$$R_{c/p} = \frac{|\Omega| + |\Upsilon| + |\tau| + |\text{✗}|}{N} \tag{4.3}$$

where $|\Omega|$ is the number of bits required both to announce the bases and identify any pulses that failed to arrive, $|\Upsilon|$ is the number of bits that must be communicated during the error correction

procedure, $|\tau|$ is the length of the authentication tag, and $|\text{✗}|$ is the number of extraneous bits that would not normally be considered in theoretical treatments of QKD, such as those required for channel characterisation and packet switching, both of which will be addressed in more detail later.

After accounting for the number of bits $|k_{\text{init}}|$ that will be used as the initial secret key in the next round of the protocol, we find that

$$R_{\text{c/s}} = \frac{R_{\text{c/p}}}{R_{\text{s/p}} - |k_{\text{init}}|/N} \leq \frac{|\Omega| + |\Upsilon| + |\tau| + |\text{✗}|}{N\zeta\left[-Q_\mu H_2\left(E_\mu\right) + Q_1\left[1 - H_2\left(E_1\right)\right]\right] - |k_{\text{init}}|} \tag{4.4}$$

From this, it is clear that condition 4.1 cannot be fulfilled by DV-QKD in its current form. Consider the limiting (and highly unrealistic) situation where we replace Alice's attenuated laser with a deterministic single-photon source, meaning no decoy states are required and $Q_1 = Y_1$. Through fluke or otherwise, Bob's bases match Alice's perfectly, meaning $\zeta = 1$. Contact between the two parties is a one-off event that will never be repeated, so $|k_{\text{init}}| = 0$. We use a lossless, error-free channel which does not rely on any extraneous communication, and give Bob perfect single-photon detectors, meaning $|\Omega| = N$, $|\Upsilon| = |\text{✗}| = 0$ and $Y_1 = 1$. $H_2(x) \to 0$ as $x \to 0$, so

$$R_{\text{c/s}} \to 1 + \frac{|\tau|}{N} \tag{4.5}$$

Of course, equation 4.5 only marginally violates condition 4.1, as we require $N \gtrsim 10^5$ for finite-key security [114] and $|\tau|$ does not typically exceed 128 bits. However our model fails to quantitatively address the impact of this on the classical data rates or network capacity. In addition, the assumptions made by condition 4.1 are not necessarily appropriate for many real-world networks, as user demand can fluctuate over time.

To address the above, a more general approach is required. Consider an arbitrary symmetric cipher that can be used to encrypt $|m|_{\max}$ bits of data for every $|k_{\text{C}}|$ bits of key. If each run of a QKD protocol uses $R_{\text{c/s}}|k|$ classical bits to generate $|k|$ bits of key, then $\frac{|k||m|_{\max}}{|k_{\text{C}}|}$ bits of data can be encrypted per run.

The network is defined to have a constant level of off-peak traffic from time $t = 0$ to $t = t_1$, and a constant level of on-peak traffic from $t = t_1$ to $t = t_2$. In practice, there will still be some variation on the demand within these windows, however it should be small relative to the difference between the two, as one would expect in a "9-to-5" office building, for example. There is no encryption-related penalty for capping the data rates further than absolutely necessary, so these levels of on-peak and off-peak traffic may be considered upper bounds.

During off-peak periods, the adjusted channel capacity per unit time (recall, the total channel capacity minus the number of bits consumed by communication protocol headers) can be expressed as

$$\varsigma = \varsigma_{\text{V}} + u_{\text{V}} \tag{4.6}$$

where $\varsigma_\vee$ is the number of bits of unencrypted off-peak data that are transmitted per unit time and $u_\vee$ is the unused remainder.

To encrypt all the off-peak data using keys generated by QKD, we require

$$u_\vee \geq \frac{R_{c/s}\varsigma_\vee |k_C|}{|m|_{max}} \tag{4.7}$$

Rearranging and substituting equation 4.6 into equation 4.7 gives

$$\boxed{\varsigma_\vee \leq \frac{\varsigma}{1+\frac{R_{c/s}|k_C|}{|m|_{max}}}} \tag{4.8}$$

Therefore, for encrypted data,

$$\varsigma t_1 = \varsigma_\vee t_1 \left(1+\frac{R_{c/s}|k_C|}{|m|_{max}}\right) + u'_\vee t_1 \tag{4.9}$$

Similarly, for on-peak periods,

$$\varsigma = \varsigma_\wedge + u_\wedge \tag{4.10}$$

where $\varsigma_\wedge$ is the number of bits of on-peak data being transmitted per unit time and $u_\wedge$ is the unused remainder.

When encrypting the on-peak data using keys generated by QKD, we can take advantage of $u'_\vee$ to share additional key before it is required, reducing the amount that needs to be transmitted during on-peak times. As a result, we mandate

$$u_\wedge (t_2 - t_1) + u'_\vee t_1 \geq \frac{R_{c/s}\varsigma_\wedge |k_C|}{|m|_{max}} (t_2 - t_1) \tag{4.11}$$

Rearranging and substituting equations 4.9 and 4.10 into equation 4.11 gives

$$\varsigma - \varsigma_\wedge \geq \frac{R_{c/s}\varsigma_\wedge |k_C|}{|m|_{max}} - \underbrace{\left[\varsigma - \varsigma_\vee \left(1+\frac{R_{c/s}|k_C|}{|m|_{max}}\right)\right]}_{\dagger} \frac{t_1}{t_2 - t_1} \tag{4.12}$$

We assume † is non-zero, as otherwise equation 4.12 reduces to the trivial case. This means equation 4.8 restricts † to always be positive, hence

$$\boxed{\frac{t_1}{t_2 - t_1} \geq \frac{\varsigma_\wedge \left(1+\frac{R_{c/s}|k_C|}{|m|_{max}}\right) - \varsigma}{\varsigma - \varsigma_\vee \left(1+\frac{R_{c/s}|k_C|}{|m|_{max}}\right)}} \tag{4.13}$$

We can put these equations in context by measuring $R_{c/s}$ for a real system. The ID Quantique Clavis[2] is a natural choice, given the work done in chapter 3. In table 4.1, we give values both for a

TABLE 4.1: Average number of classical bits transmitted by the ID Quantique Clavis^2 per secret bit ($\overline{R}_{c/s}$) for both the minimum and maximum attenuations at which key is reliably generated.

Round Type	Quantum Channel Loss (dB)	$\overline{R}_{c/s}$
Initialisation	$0.00\,^{+0.01}_{-0}$	196.4 ± 0.4
Standard	$0.00\,^{+0.01}_{-0}$	195.9 ± 1.1
Initialisation	9.00 ± 0.01	757.3 ± 9.6
Standard	9.00 ± 0.01	753.9 ± 9.9

near-lossless channel and at 9 dB attenuation (recall, the highest loss that we can tolerate before key generation becomes intermittent). The former was implemented by placing Alice and Bob next to each other and establishing a direct connection with the shortest fibre available that, to within the precision of the powermeter, had 0 dB loss. At the time of taking measurements for the latter, Alice and Bob were located in separate nodes for metropolitan network tests. The fibre between them contributed 1.4 dB of loss, and the remaining 7.6 dB was introduced using a variable optical attenuator. The number of classical bits broadcast by the QKDSequence control software can be measured using Wireshark, and the Clavis^2 keeps track of the number of secret bits generated in each round. The average $R_{c/s}$ was then calculated from these two values, for a 256-bit initial shared secret.

There are a number of reasons why the results in table 4.1 are so extreme. First, the potential for the classical channel to be a limiting factor has, to the author's knowledge, never previously been scrutinised at this level, so commercial systems are unlikely to have been optimised and there may be scope to reduce the communication resources consumed by the Clavis^2. However, there are also some fundamental restrictions. The Transmission Control Protocol (TCP) [115] forms the basis of the Clavis^2 public channel. It divides data into a series of packets, adding a minimum of 160 bits to each in the form of a header that contains pieces of information like the destination port and a checksum. In actuality, the Clavis^2 adds a total of 256 bits on top of the payload due to the inclusion of optional fields. This is then encapsulated in an Internet Protocol version 4 (IPv4) [116] packet with a header that is 160 bits both at minimum and in the case of the Clavis^2. It should be noted that as the Internet Protocol version 6 (IPv6) [117] becomes more prevalent, the minimum header size will increase to 320 bits. Finally, the IPv4 packet is encapsulated in an Ethernet II [99] frame that contributes an extra 144 bits, and requires a 96-bit interframe spacing. This is summarised in figure 4.1.

As one would expect, a higher loss in the quantum channel negatively impacts $\overline{R}_{c/s}$. At 9 dB attenuation, the number of raw bits that contribute to each secret bit is greater than at 0 dB, and so more information must be exchanged per secret bit over the public channel. In addition, the Clavis^2 relies on BB84 when the loss is ≤ 3 dB and Scarani-Acín-Ribordy-Gisin 2004 (SARG04) otherwise. In the case of the latter, Alice announces two states from a choice of four instead of one basis from

a choice of two (see protocol 2.2), quadrupling the information she must transmit for each qubit received by Bob.

Finally, it can be seen that, as an overall percentage, relatively little information needs to be communicated during the initialisation period. This makes sense given it mainly consists of calibrative tasks, involving direct measurements of features like the length of the transmission line.

FIGURE 4.1: Showing the encapsulation structure for an Ethernet II frame containing an IPv4 packet, which in turn contains a TCP packet. While in principle it is possible to transmit a 11,584-bit payload, this can only happen if it is known that Bob will accept packets of such size. Otherwise, the maximum payload size is restricted to 4288 bits, calculated using the limits given in [118].

Figure 4.2 takes the values of $\overline{R}_{c/s}$ from table 4.1, and plots the minimum time ratio from equation 4.13, assuming we want to encrypt with a QKD-keyed OTP, meaning $\frac{|k_C|}{|m|_{max}} = 1$. We vary both the on-peak and off-peak data rates, as well as fixing the off-peak traffic to give a clearer picture of the limiting cases. While

$$\frac{t_1}{t_2 - t_1} \to \infty \quad \text{as} \quad \varsigma_V \to \frac{\varsigma |m|_{max}}{|m|_{max} + R_{c/s}|k_C|} \tag{4.14}$$

a network operating close to this limit can be simulated by setting

$$\varsigma_V = \left\lfloor \frac{\varsigma |m|_{max}}{|m|_{max} + R_{c/s}|k_C|} \right\rfloor_M \tag{4.15}$$

where $\lfloor \cdot \rfloor_M$ means that we round down to the nearest multiple of machine epsilon M; the difference between 1 and the next-closest number that, on a computer, is distinguishably greater than 1. In this case, $M = 2^{-52}$.

We plot figure 4.3 in similar fashion, continuing to rely on QKD as a means of distributing the symmetric key, but this time encrypting with AES-GCM, such that $\frac{|k_C|}{|m|_{max}} = \frac{256}{2^{39}-256}$ [119].

The results make clear that networks like the Washington-Moscow hotline [102], which need high security and experience low volumes of traffic for long periods, will be able to use a QKD-keyed OTP if the classical channel is the only limiting factor. However, day-to-day networks will have to continue using computationally secure encryption. Not only does AES-GCM require off-peak times per second of on-peak time that are orders of magnitude lower than for the OTP, but the off-peak data rates are limited to 99.99999(1)% of the channel capacity at worst. In contrast, the OTP restricts this to 0.50662(3)% at best, given the values of $\overline{R}_{c/s}$ measured for the Clavis[2]. Finally, we can get much closer to this limiting value for AES-GCM before $\frac{t_1}{t_2 - t_1}$ rapidly approaches infinity, as evidenced by comparing subfigures 4.2e and 4.2f with subfigures 4.3e and 4.3f, which are still .

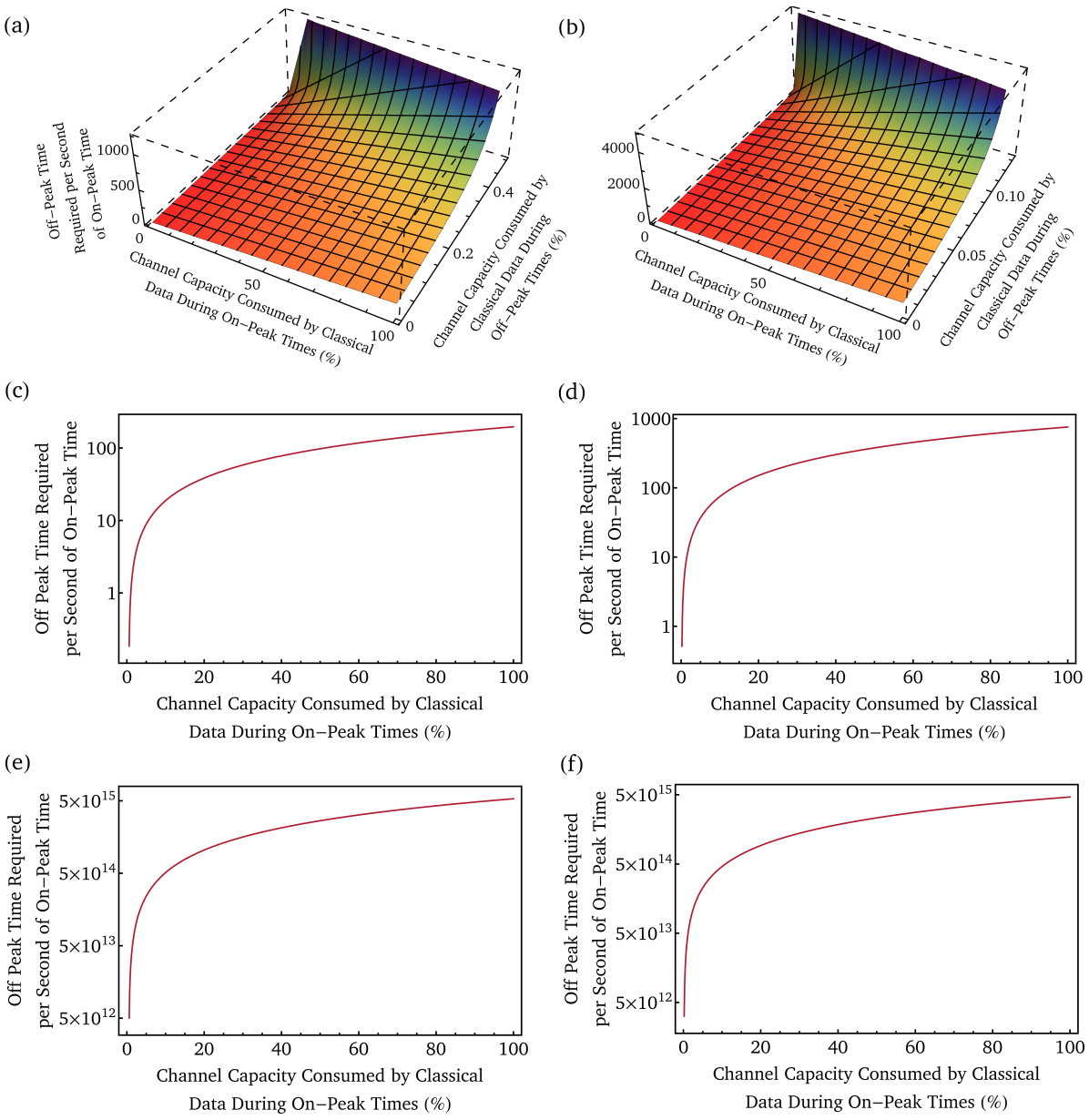

FIGURE 4.2: Showing the amount of off-peak time required per second of on-peak time in order to encrypt all data with a QKD-keyed OTP, and considering only limitations imposed by the classical QKD channel for the ID Quantique Clavis^2. We present results for (a) 0 dB loss in the quantum transmission line for varying on-peak and off-peak traffic; (b) 9 dB loss in the quantum transmission line for varying on-peak and off-peak traffic; (c) and (d) 0 dB and 9 dB losses in the quantum transmission line respectively, for varying on-peak and no off-peak traffic in both cases; (e) and (f) 0 dB and 9 dB losses in the quantum transmission line respectively, for varying on-peak and $\left\lfloor \frac{\varsigma |m|_{\max}}{|m|_{\max} + R_{c/s} |k_C|} \right\rfloor_{\mathsf{M}}$ off-peak traffic in both cases, where $\lfloor \cdot \rfloor_{\mathsf{M}}$ means that we round down to the nearest multiple of machine epsilon M.

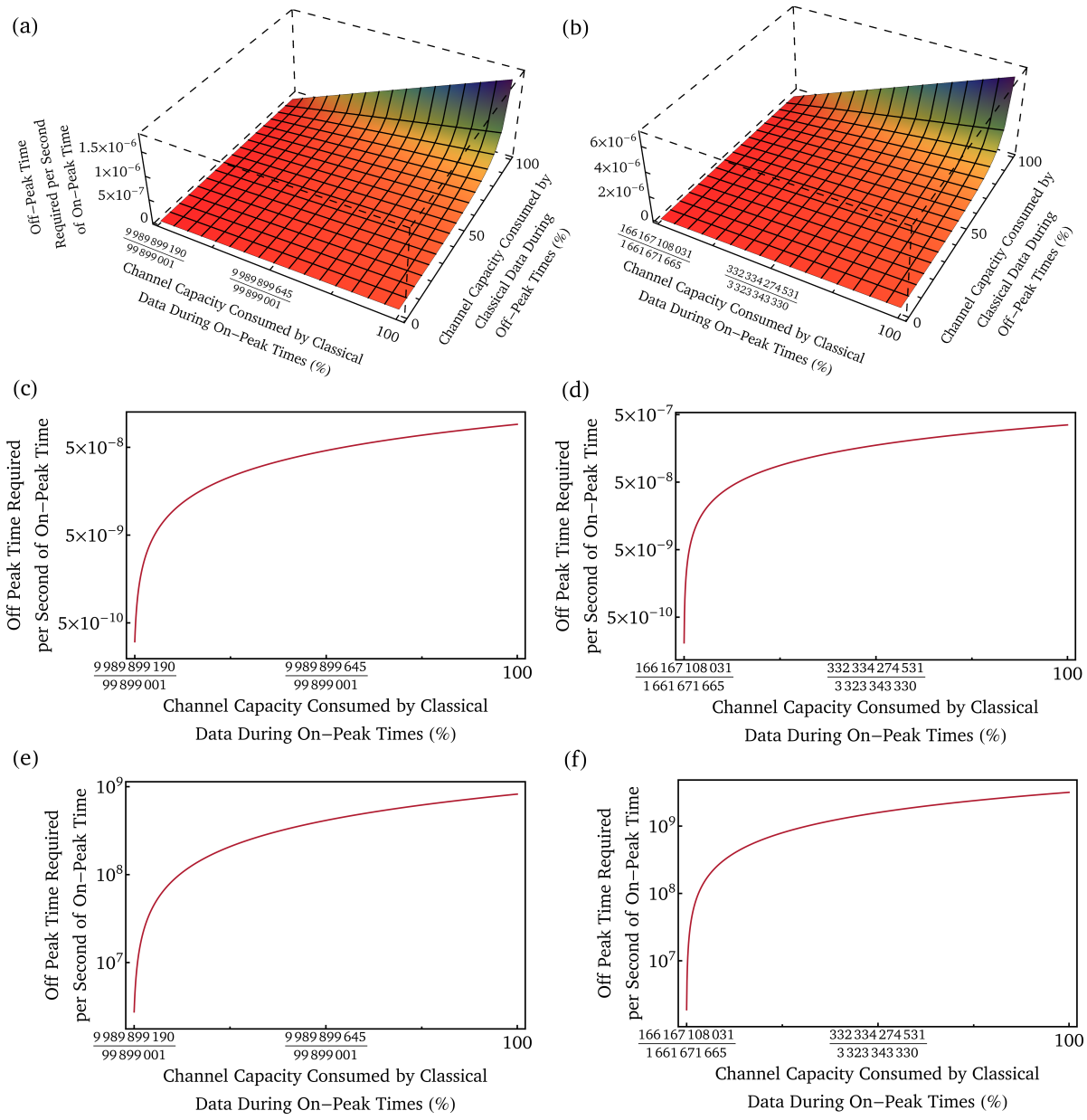

FIGURE 4.3: Showing the amount of off-peak time required per second of on-peak time in order to encrypt all data with AES-GCM, keyed using QKDand considering only limitations imposed by the classical QKD channel for the ID Quantique Clavis^2. We present results for (a) 0 dB loss in the quantum transmission line for varying on-peak and off-peak traffic; (b) 9 dB loss in the quantum transmission line for varying on-peak and off-peak traffic; (c) and (d) 0 dB and 9 dB losses in the quantum transmission line respectively, for varying on-peak and no off-peak traffic in both cases; (e) and (f) 0 dB and 9 dB losses in the quantum transmission line respectively, for varying on-peak and $\left\lfloor \frac{\varsigma |m|_{\max}}{|m|_{\max} + R_{c/s}|k_C|} \right\rfloor_M$ off-peak traffic in both cases, where $\lfloor \cdot \rfloor_M$ means that we round down to the nearest multiple of machine epsilon M.

We can now provide a more comprehensive formulation of the terms that a network must fulfil for the OTP to be used in conjuction with QKD. While we do not explicitly cover cases that can be split into three or more distinct periods of traffic, these can always be approximated by an on-peak/off-peak model, though with slightly pessimistic estimates as a result, Our model is general enough to be representative of most everyday networks, and is summarised by condition 4.2, which reduces to condition 4.1 if $|m|_{\max} = |k_C|$, $t_1 = 0$, $t_2 - t_1 = 1$ and $\varsigma_\wedge = \frac{\varsigma}{2}$.

Condition 4.2: *Assume an unsecured link of classical capacity ς experiences off-peak data rates of $\varsigma_\vee$ for time t_1, on-peak data rates of $\varsigma_\wedge$ for time $t_2 - t_1$, and quantum signals can be injected without generating any secondary artifacts that affect the above. We can encrypt all data using an arbitrary cipher, without artificially capping the classical data rates or increasing the channel capacity, so long as* $R_{c/s} \leq \frac{|m|_{\max}[\varsigma t_2 - \varsigma_\wedge(t_2 - t_1) - \varsigma_\vee t_1]}{|k_C|[\varsigma_\wedge(t_2 - t_1) + \varsigma_\vee t_1]}$.

4.2 The Effect of the Quantum Channel on Key Generation

Until now, the work in this chapter has implicitly assumed that the bit generation rate for the encryption keys is comparable with classical data rates, taking care to note that the former is distinct from the secret key rate, as it does not include the bits assigned to refreshing Alice and Bob's initial shared secret. However, as we have already indicated in chapter 3, this assumption is inaccurate, and we must examine the implications of any mismatch.

Consider the situation where

$$R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) < \varsigma_\vee \tag{4.16}$$

The left hand side corresponds to the number of bits generated per unit time that can be used for encryption, and $R_{p/t}$ is the quantum clock rate. Here, the result is trivial and well-known. Unless multiple quantum devices can be multiplexed together, the only choice is to use a computationally secure cipher. Similarly, if

$$R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) > \varsigma_\wedge \tag{4.17}$$

then so far as the quantum channel is concerned, there will be no issues with using the OTP. However, when

$$\varsigma_\vee < R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) < \varsigma_\wedge \tag{4.18}$$

the situation becomes more interesting. We define

$$\begin{aligned} \Delta_\vee &= R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) - \varsigma_\vee \\ \Delta_\wedge &= \varsigma_\wedge - R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) \end{aligned} \tag{4.19}$$

To use the OTP, it is required that

$$\Delta_{\vee} t_1 \geq \Delta_{\wedge}(t_2 - t_1) \tag{4.20}$$

Thus, by substituting equation 4.19 into 4.20 and rearranging, we find

$$\frac{t_1}{t_2 - t_1} \geq \frac{\varsigma_{\wedge} - R_{\mathrm{p/t}}\left(R_{\mathrm{s/p}} - |k_{\mathrm{init}}|/N\right)}{R_{\mathrm{p/t}}\left(R_{\mathrm{s/p}} - |k_{\mathrm{init}}|/N\right) - \varsigma_{\vee}} \tag{4.21}$$

This enables us to construct conditions 4.3 and 4.4 which, regardless of the efficiency of the public channel, must be fulfilled if we are not to continue encrypting with the Advanced Encryption Standard (AES)-based modes of operation. There is, of course, always the option to curb classical data rates. However, the end-user often prioritises minimal performance improvements over security, as evidenced by the widespread adoption of technlogies such as contactless card payments, which have a number of trivially-exploitable vulnerabilities [120–123]. Therefore it would be naïve to assume that internet users will accept slower speeds in exchange for an increase only in the theoretical security of their data.

Condition 4.3: *Assume* $R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) < \varsigma_{\vee}$. *We can encrypt all off-peak data using a QKD-keyed OTP without artificially capping the classical data rates, so long as* $D_{mux} = \left\lceil \frac{\varsigma_{\vee}}{R_{p/t}\left(R_{s/p} - |k_{init}|/N\right)} \right\rceil$ *quantum devices can be multiplexed together and* $\sum_{D_{mux}} R'_{s/t} \approx R_{s/t} D_{mux}$. *Here,* $R_{s/t}$ *is the number of secret bits generated per unit time when only a single QKD device is operational, and* $R'_{s/t}$ *is the number of secret bits generated per unit time by each of those deployed in a multiplexed configuration.*

Condition 4.4: *Assume* $\varsigma_{\vee} < R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) < \varsigma_{\wedge}$, *or condition 4.3 has been fulfilled. We can encrypt all on-peak data using a QKD-keyed OTP without artificially capping the classical data rates, so long as* $D_{mux} = \left\lceil \frac{\varsigma_{\wedge}}{R_{p/t}\left(R_{s/p} - |k_{init}|/N\right)} \right\rceil$ *quantum devices can be multiplexed together and* $\sum_{D_{mux}} R'_{s/t} \approx R_{s/t} D_{mux}$, *or equation 4.21 can be satisfied.*

The most important question that this raises is how close the speeds of the classical and quantum channels actually are to each other. In figure 4.4 we compare $R_{\mathrm{s/t}} = R_{\mathrm{p/t}} R_{\mathrm{s/p}}$ with classical data rates, noting that

$$R_{\mathrm{p/t}}\left(R_{\mathrm{s/p}} - |k_{\mathrm{init}}|/N\right) \approx R_{\mathrm{p/t}} R_{\mathrm{s/p}} \quad \text{for} \quad N >> |k_{\mathrm{init}}| \tag{4.22}$$

as is the case when taking into account the finite key limit. We split classical communications into a global average for end-user connection speeds, the data rates given by the Institute of Electrical and Electronics Engineers (IEEE) Ethernet standards, and record data rates using experimental

technology. We see that, in the worst case, the classical rates are seven orders of magnitude greater than $R_{s/t}$. While we would eventually expect to reach a saturation point for the amount of classical information transmissible across a single fibre (the Shannon limit [124]), the size of the gap indicates that this alone will not be enough to close it anytime soon.

In the best-case scenario, where only end-users take advantage of the OTP, it is not unreasonable to expect that QKD may reach the speeds required. However, a side effect of having many individual QKD devices in operation at the same time is that they must be easily multiplexable and, if the requirement of information-theoretic security extends to all parties, the situation becomes equivalent to that of protecting backbone networks rather than end-users. For the time being, we will make no further comment as to how feasible it is to implement such an architecture, however this will be the focus of chapter 7. In fact, a more important point is that in almost all cases, critical infrastructure needs to be at least as secure as the end-user, but with much higher data rates (see, for example, the data centre emulated in chapter 3). Hence, a significant step-change is still required just to get to a point where we are limited by the work in section 4.1. That is not to say progress thus far has been based entirely on incremental improvements to the basic technology. For example, the development of dedicated post-processing modules was responsible for the 11.53 Mbit/s secret key rate set by [125] (see point D in figure 4.4). Yet it seems unlikely that we will ever reach a point where, experimentally,

$$\mathrm{Max}\left(R_{s/t}\right) \geq \mathrm{Max}\left(\varsigma_{\wedge}\right) \tag{4.23}$$

This can be broken down into two reasons. Any technology that enables faster single-fibre-single-transmitter communication than contemporary classical methods will immediately supersede them, so at best quantum secret key rates can expect to equal classical data rates. However, the post-processing means $R_{p/t}$ will always be greater than $R_{s/p}$, and we would expect the rate for standard communications over a quantum channel to fall between these, as privacy amplification will not be required. **[ADD IN THEORETICAL BOUNDS FROM [126]]**

Of course, this is still not enough to rule out everyday OTP deployment on the basis of the quantum channel, as we are yet to determine how easily equation 4.21 can be satisfied. In figure 4.5, we plot $\frac{t_1}{t_2-t_1}$ using the current record for the quantum secret key rate, and

$$0 \leq \varsigma_{\vee} < R_{p/t}\left(R_{s/p} - |k_{\mathrm{init}}|/N\right) \tag{4.24}$$

For the on-peak data rates we consider both the 2018 global average for end-users, weighted by the number of unique IPv4 addresses in each country, as well as the highest experimental data rate thus far achieved (see point G in figure 4.4), where the distance for the latter was 0.4 km less than that over which the record quantum secret key rate was realised. The global end-user average was calculated to be 20.41 ± 0.58 Mbits/s, based on data from [137]. The methods of collection are summarised in [138], from which it is clear that the dataset is suitably representative of real-world speeds available to electronic devices owned by end-users. We diverged from the long-term dataset on which figure 4.4 is based, as it was discontinued after the first quarter of 2017.

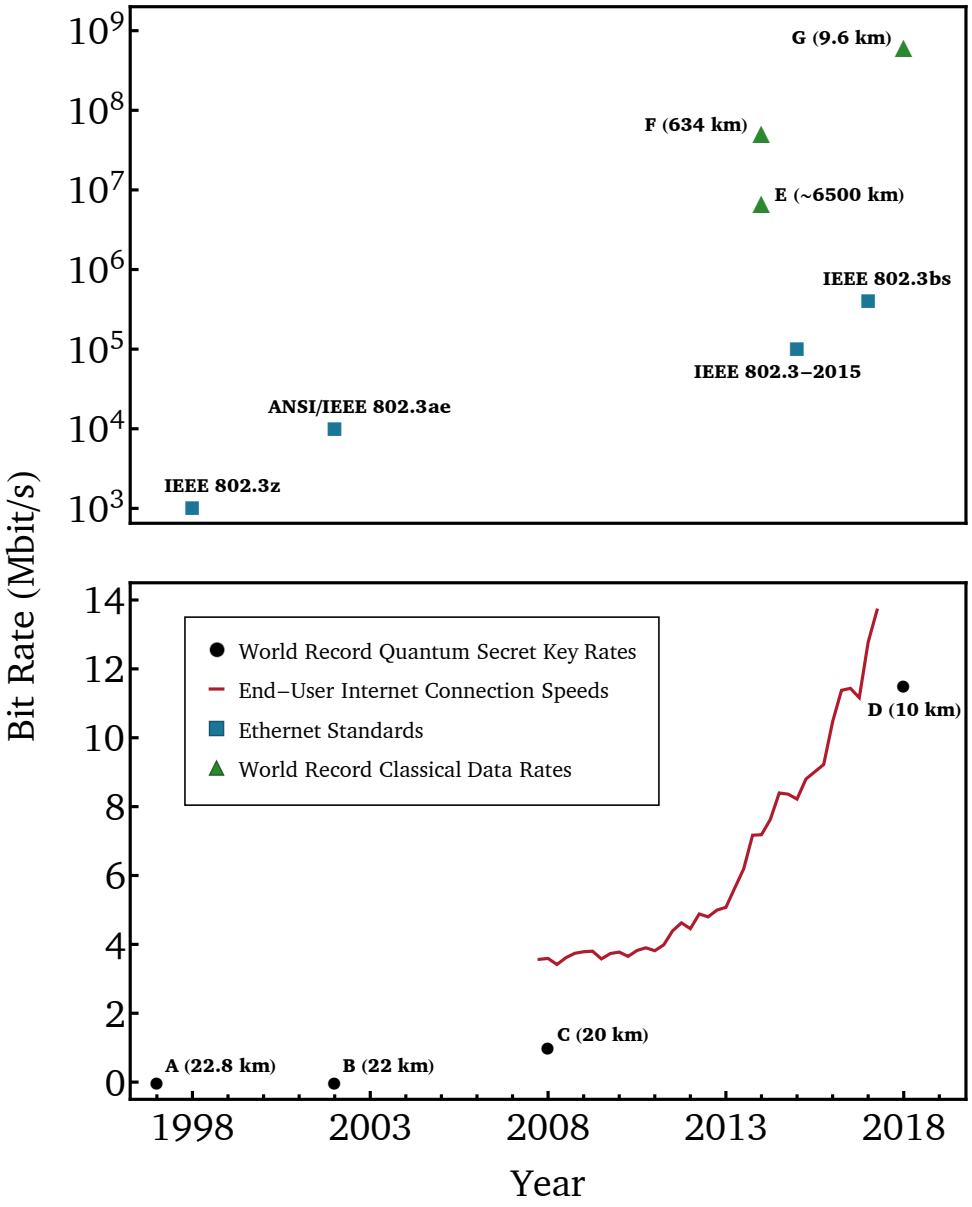

FIGURE 4.4: Comparing world-record quantum secret key rates with average end-user connection speeds, classical data rates from the IEEE Ethernet standards [82, 127–129] and world-record classical data rates using experimental technology. The protocols used for A, B, C and D were B92 [130], BB84 [131], BB84 with decoy states [132] and T12 [125] respectively. E was implemented on the Apollo South submarine cable with no customer disruption [133], F used dispersion uncompensated single-mode fibre (SMF) [134], and G used a multicore SMF [135] respectively. The end-user internet connection speeds are a global average, weighted by the number of unique IPv4 addresses in each country, and calculated from the data in [136].

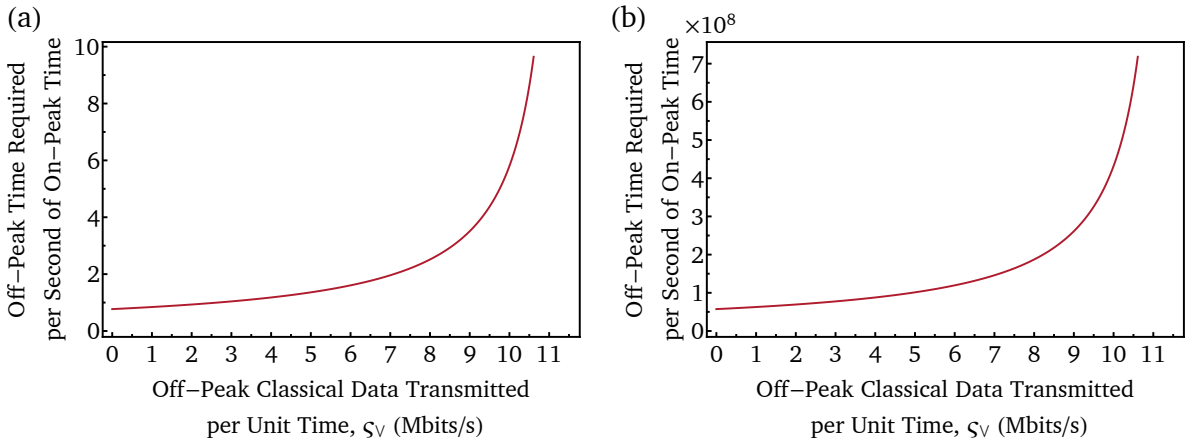

FIGURE 4.5: Showing the amount of off-peak time required per second of on-peak time in order to encrypt all data with a QKD-keyed OTP, and considering only limitations imposed by the quantum channel. We use the world-record quantum secret key rate, which was set in 2018 over a distance of 10 km (see figure 4.4). The amount of on-peak data transmitted per unit time is defined by (a) the 2018 global average for end-user data rates, weighted by the number of unique IPv4 addresses in each country and calculated from the data in [137]; (b) the world-record classical data rate, achieved in 2018 over a distance of 9.6 km (see again figure 4.4).

From figure 4.5, it can be seen that, with the exception of instances when off-peak end-user data rates are kept at no more than around 50% of their on-peak rates, using the OTP remains impractical even if ignoring the impact of the results from section 4.1. As before, bespoke networks with long periods of inactivity remain a possible application for QKD with OTP encryption. However, without the ability to multiplex several-orders-of-magnitude-worth of QKD devices, we are left us no choice other than to continue relying on computationally-secure ciphers such as AES for near-term protection of core infrastructure.

4.3 State of the One-Time Pad

Here, we summarise the hurdles that remain even when discounting the arguments put forth in sections 4.1 and 4.2. While not scientifically limiting, these are still important considerations if the OTP is to be widely deployed without introducing vulnerabilities. Overcoming them will take time, something that is lacking if QKD is to be used as a defence against quantum computers in the real world.

Furthermore, these issues are only likely to start being addressed if it can be demonstrated that a suitable method of key distribution exists, which does not introduce cumbersome overheads when paired with the OTP. Given the work presented thus far, we contend that DV-QKD does not

fulfil such a criterion in its present form, despite the promise originally shown by basic theoretical treatments, adding even more weight to the argument that AES will continue to be used for the majority of real-world encryption.

We first observe that although authenticated encryption modes exist for block ciphers, these cannot be directly applied to the OTP. Any potential solution must go through standardisation. Otherwise, there is a high risk of implementation errors as end-users, not all of whom will have a strong security background, try to combine encryption and authentication themselves, something which is fraught with insecurities [139].

In addition, the OTP itself is yet to be standardised, due to lack of widespread demand. If the reader is wondering why this is necessary for an encryption scheme that seems so straightforward, consider the following. When logging into a website, the password field is effectively unlimited in length. Without knowing any information on a particular user's password, a sensible place to start might be by trying the most common passwords in use. However, if the user then inputs their password to the website, and that is transmitted using a OTP without some kind of length padding, the attacker suddenly knows how many characters have been sent, and can restrict their attack to the most common passwords of that length. Once again, not having a standardised option means that more knowledgeable programmers will implement custom solutions, however historically this has resulted in errors of sometimes fatal consequence (see, for example, the impact on the Battle off Samar when an enciphering clerk padded a request for information with "the world wonders", leading to misinterpretation of the message [102]).

4.4 Outlook

The work of this chapter substantiates the claim that single-qubit DV-QKD is incompatible with the OTP so long as both continue to exist in their current form. We have quantified the well-known fact that, at present, secret key rates are too slow, and explored the impact QKD has on the classical part of the network, finding that the demands are untenable. On the other hand, DV-QKD with AES-GCM is expected to scale well when transitioned from research networks to the real world.

[ADD THE FOLLOWING IN HERE:]

We have said throughout that we have not ruled out the use QKD with the OTP in bespoke networks but, beyond identifying examples that of those that receive infrequent use, we have not broached the subject of whether any exist with whose capacity is not fixed. Satellite networks are a good example of this...if it's technically possibly to put the number of required classical channels in then all good.

When it comes to laying more fibre, the story is different. Obviously this is expensive, and approaches to addressing current internet capacity prefer to invest money in other methods [133]. In the United Kingdom, the aim in 2017 was still only to have fibre-to-the-premises to an extra 2 million cases by 2020, with 10 million receiving upgrades to existing copper-wire infrastructure

instead [140]. Aside from the obvious implications of there not being fibre everywhere, which will be further examined in chapter 6, this is strong evidence that the number of additional fibres required in everyday networks would not be added quickly enough to protect against quantum attacks.

[: ADD THE PRECEDING WORDS IN HERE]

While other forms of QKD are not the focus of this thesis, the question of how they behave when subject to the analysis presented herein is an important one. We will close by performing a cursory examination of the more-obvious alternatives, highlighting areas that could benefit from further work.

4.4.1 An Attempt to Circumvent the Restrictions on the Quantum and Classical Channels

When considering alternatives to BB84-style protocols, a natural place to start is with CV-QKD. In its original form, squeezed states were required [141]. While these can now be generated at telecom wavelengths [142], they are heavily affected by losses [143], and are yet to be used as the basis for a practical QKD system. Instead, the focus has largely been on implementations using Gaussian-modulated coherent states, which are capable of reaching a secret key rate of 1 Mbit/s across 25 km of fibre, which equates to 5 dB of loss [144]. This is still below the record for DV-QKD, and the types of information that must be sent over the classical channel remain the same; sifting does not take place per se, but Bob still needs to inform Alice how he measured [145]. Homodyne measurements will always return noise if the quantum bit (qubit) is lost en-route, significantly increasing the number of error correction messages that must be transmitted in comparison to DV-QKD, where single-photon detection is used [104]. It is possible to observe both quadratures simultaneously by way of heterodyne measurements [146], removing the need for Bob to make and announce a choice. In a perfect world, this would lead to double the amount of information being retained, however Bob's results will be much noiser, meaning the key rate increases by a factor that is less than this [104]. In addition, post-selection is still required whenever the channel loss is > 3 dB [147]. Thus, while other forms of CV-QKD seem to offer little in regard to sidestepping the arguments with which we are concerned, it is less clear for coherent-state heterodyne schemes, and a full analysis may reveal some benefit.

Another possibility is FL-QKD, for which a secret key rate of 1.3 Gbit/s was recently demonstrated over a channel with 10 dB loss [148]. The only caveat is this implementation did not include full post-processing, which could lead to more modest key rates if additional bottlenecks are introduced by the parts of the system which are missing (see, for example, reference [125] where custom electronics had to be developed just to reach a 13.72 Mbit/s secret key rate). Unfortunately, while there is no reason to believe that issues of this kind are anything more than engineering challenges, the classical channel in FL-QKD is simply a higher-rate version of the one in BB84 [110], meaning we are still limited by section 4.1.

For protocols based on quantum teleportation, the unitary rotation step requires two classical bits be communicated per measurement result [149]. While the payload delivered by each ethernet frame will double, the overall number of classical bits per secret bit can be expected to increase by less than this, as the amount of header information should remain constant. Nevertheless, teleportation clearly does not offer a solution to our problem, and the extra demand on the classical channel is of particular concern for future quantum repeaters.

On the other hand, superdense coding uses only a single qubit to communicate two bits of information, and can be generalised to higher-dimensional systems, transmitting r_q bits on a maximally entangled state such as [150]

$$|\psi\rangle = \frac{1}{\sqrt{r_q}} \sum_{\phi=1}^{r_q} |\phi\rangle |\phi\rangle \tag{4.25}$$

So long as we continue to encode in only two bases, the classical information that needs to be transmitted remains unchanged. Unfortunately, with the values for $\overline{R}_{c/s}$ given in table 4.1, the dimensionality required is likely to be on the order of hundreds. However, placing an exact number on this is non-trivial, as the number of secret key bits carried by each qudit will not increase linearly with dimension.

Finally, the reusable OTP [151] may in principle help circumvent the arguments in both sections 4.1 and 4.2. There are practical issues to overcome, such as how to ensure message completeness in the presence of loss. In addition, the regularity with which key needs to be refreshed is yet to be evaluated. Therefore, without further development, it is unclear as to whether or not the QKD paired with the reusable OTP could form an effective information-theoretically secure cryptosystem.