Building the quantum network†

Chip Elliott
BBN Technologies, 10 Moulton Street, Cambridge, MA 02138, USA
E-mail: celliott@bbn.com

Abstract. We show how quantum key distribution (QKD) techniques can be employed within realistic, highly secure communications systems, using the internet architecture for a specific example. We also discuss how certain drawbacks in existing QKD point-to-point links can be mitigated by building QKD networks, where such networks can be composed of trusted relays or untrusted photonic switches.

1. Introduction

After nearly two decades as a laboratory curiosity, quantum key distribution (QKD) techniques are just now emerging as useful building blocks in highly secure networks. Under DARPA sponsorship, a team from BBN Technologies, Boston University and Harvard University has recently begun a five-year research program to design and build the world’s first such highly secure quantum network, one that delivers end-to-end network security via high-speed QKD, and to test that network against sophisticated eavesdropping attacks.

This paper briefly describes the system architecture of our quantum network as it evolves through three major stages, from a single, stand-alone QKD link supporting highly secure internet communications, through both trusted and untrusted QKD networks. This paper provides a network engineer’s view of quantum cryptography. Although the contrast with neighbouring physics articles may be disorienting, we hope to provide some hint of the larger engineering context into which quantum cryptography now fits and to stimulate thinking and dialogue on these broader issues.

The quantum network marries a variety of QKD techniques to well established internet technology in order to build a secure key distribution system employed in conjunction with the public internet or, more likely, with private networks that employ the internet protocol suite. We note that such private networks are currently in widespread use around the world.

† The opinions expressed in this article are those of the author alone, and do not necessarily reflect the views of the United States Department of Defense, DARPA or the United States Air Force.
with customers who desire secure and private communications, e.g. financial institutions, governmental organizations, militaries and so forth, and that a marriage of QKD technologies to these types of private network may prove both feasible and immediately appealing in certain contexts. Rollout into the worldwide, consumer internet is of course much more problematic as it would require substantial physical changes to very large numbers of computers and routers, and widespread alterations to the world’s existing fibre infrastructure.

In its simplest form, the quantum network distributes keys for a virtual private network (VPN) overlay running atop an underlying public or private internet; unfortunately today’s QKD techniques are distance limited and so the geographic extent of the resultant VPN would have to be fairly circumscribed, e.g. a single metropolitan area for fibre-based QKD. With our trusted network approach, this geographic span can be extended, though at a cost of QKD relays or repeaters at intervals of 50 km or so along a fibre network. These relays need to be trusted with all key material, so they would likely have to be locked, tamper resistant and perhaps guarded in order to form a wide-scale network. Finally, we also sketch an untrusted variant of our QKD network in which optical switches are employed instead of trusted relay nodes; this variant has some advantages but again is constrained to relatively small geographic spans. Thus as we shall see, there are differing strengths and weaknesses to each of these approaches, and none can be considered a perfect solution to the problem of key distribution. We do claim, however, that these approaches may be highly practical for certain constrained problems, e.g. those in which key distribution does not need to be performed over a large geographic area or those in which trusted relay points may be practical.

For background reading, please see [1] for an excellent survey and bibliography of quantum cryptography techniques, [2, 3] for general information about classic cryptography and secure communications, [4] for an introduction to internet protocols and architecture and [5, 6] for standards documents on the internet security architecture IPsec and its key exchange protocol IKE.

2. Some desirable attributes in a QKD network

In abstract terms, QKD offers a technique for coming to agreement upon a shared random sequence of bits within two distinct devices, with a very low probability that other devices (eavesdroppers) will be able to make successful inferences as to those bits’ values. In specific practice, such sequences are then used as secret keys for encoding and decoding messages between the two devices. Viewed in this light, QKD is quite clearly a key distribution technique, and may profitably be compared against other techniques for key distribution such as trusted couriers, algorithmic methods such as Diffie–Hellman and so forth. More broadly, one can rate QKD’s success against a number of important goals for key distribution, as marshalled in the following paragraphs.

Protection of keys

QKD offers significant advantages in this regard and indeed this is the main reason for interest in QKD. Public key systems have suffered from an ongoing uncertainty that decryption is mathematically or algorithmically intractable. Thus the methods of key agreement that are widely employed in today’s internet security architecture, e.g. Diffie–Hellman, may perhaps be broken at some point in the future, leading to loss of ability to communicate securely. Classic
secret key systems have suffered from rather different problems, namely, insider threats and the logistical burden of distributing keying material. Assuming that QKD techniques are properly embedded into an overall secure system, they can provide automatic distribution of keys that may offer security superior to that of its competitors.

**Authentication**

When delivering secret keys to someone, it is very important not to give them to the wrong person! QKD is a key agreement primitive that does not in itself provide authentication. Current strategies for authentication in QKD systems include prepositioning of secret keys at the distant device, to be used in hash-based authentication schemes, or hybrid QKD–public key techniques. Neither approach is entirely appealing. Prepositioned secret keys require some means of distributing these keys before QKD itself begins, e.g. by human courier, which of course may be costly and logistically challenging. In addition, this scheme appears open to denial of service attacks in which an adversary forces a QKD system to exhaust its stockpile of key material, at which point it can no longer perform authentication. Hybrid QKD–public key schemes, on the other hand, inherit the possible vulnerabilities of public key systems to cracking via quantum computers or unexpected advances in mathematics.

**Sufficiently rapid delivery of keys**

Key distribution systems must deliver keys fast enough so that the encryption devices that employ these keys do not run out of keying matter. This is obviously a race between the rate at which keying material is generated and the rate at which it is consumed for encryption or decryption activities. Today’s QKD systems achieve on the order of 1000 bits s$^{-1}$ throughput for keying material, at best, and often run at much lower rates. This is unacceptably low if one uses these keys in certain ways, e.g. as one-time pads for high-speed traffic flows. However it may be acceptable if the keying material is used as input for less secure (but often secure enough) algorithms such as the advanced encryption standard (AES). On the whole, however, it would be beneficial if QKD delivery rates could be increased by at least several orders of magnitude.

**Robustness**

This is a critical property for all non-stop systems but has not traditionally been taken into account by the QKD community. Since keying material is essential for secure communications, it is extremely important that the flow of keying material not be disrupted, whether by accident or by the deliberate acts of an adversary (i.e. by denial of service). Here QKD has provided a highly fragile service to date since QKD techniques have implicitly been employed along a single point-to-point link. Thus if that single link were disrupted, whether by active eavesdropping or indeed by fibre cut, all flow of keying material would cease. We argue that a meshed QKD network is inherently far more robust than any single point-to-point link since it offers multiple paths for key distribution. If one link is disrupted or eavesdropped, the network can automatically route around the disruption. While this is a useful technique for any form of communication network, it is particularly *a propos* for QKD, where quantum information has traditionally flowed along a single path without any form of backup or fail-over.
Distance and location independence

Ideally, any entity would be able to exchange keying material with any other entity in the world. Rather remarkably, the internet’s security architecture does offer this feature—any computer on the internet can form a security association with any other, exchanging keys through the internet IPsec protocols. This feature is notably lacking in QKD, which requires the two entities to have a direct and unencumbered path for photons between them, and which can only operate for a few tens of kilometres through fibre.

Resistance to traffic analysis

Adversaries may be able to perform traffic analysis on a key distribution system in order to understand the relationship between communicating entities. For instance, a heavy flow of keying material between two points might indicate that a large volume of confidential information flows, or will flow, between them. It may be desirable to make such analysis as difficult as possible. Here QKD in general has had a rather weak approach since most setups have assumed dedicated, point-to-point QKD links between communicating entities which has thus clearly laid out a map of the underlying key distribution relationships.

As important guidelines of our overall research agenda, we are working to strengthen QKD’s performance in these weaker areas. In some instances, this involves the introduction of newer QKD technologies; for example, we hope to achieve rapid delivery of keys by introducing a new, high-speed source of entangled photons. In other instances, we rely on an improved system architecture to achieve these goals; thus, we tackle distance and location independence by introducing a network of trusted relays.

3. System architecture of a point-to-point QKD link

Figure 1 presents a simplified, block diagram of a point-to-point QKD link as it would likely be employed in practice. Here the QKD link supports secure communications between two private enclaves so that they may exchange confidential information through a public communications network such as the internet or the global telephone system. Each enclave is typically a collection of one or more local ethernets; the whole diagram thus represents a widely deployed type of secure networking, e.g. one that securely links a branch office to a corporate headquarters.

Such secured communications are often implemented via specialized devices such as VPN gateways so that one need administer only a single device in order to establish or monitor external security for a given private enclave. These gateways are responsible for setting up security associations (and thus encrypted tunnels) with authorized distant gateway(s), for encrypting all local traffic before it is injected into the public network and for decrypting and authenticating traffic received from the public network before sending it onwards, in the clear, within the destination enclave.

In general, such systems require two distinct communications paths: one for the cryptographic keys themselves, the other for the encrypted message traffic. In conventional technology, keys may be distributed via an out-of-band channel such as couriers, or via an in-band channel using techniques such as Diffie–Hellman key exchange [2, 3]. In the quantum
network, keys are distributed via a smorgasbord of out-of-band QKD techniques (e.g. weak-coherent and entangled), and these cryptographic gateways thus act as QKD endpoints because they contain one or more QKD devices apiece.

Today’s internet offers a well defined security architecture, IPsec, that specifies the protocols, algorithms, databases and policies required for secure communication [5, 6]. IPsec provides all the tools needed for secure communication between cryptographic gateways or indeed between individual computers on the internet. Among other things, IPsec defines how two endpoints authenticate each other, exchange keys and encrypt and decrypt messages flowing between these endpoints. Thus in order to secure internet traffic via quantum cryptography, one must marry QKD technology into the overarching, and already well established, internet security architecture.

Figure 2 resolves this basic setup into considerably more detail and represents the first stage in our quantum network research program. A full description of the internet protocol suite is obviously beyond the scope of this paper; see [4] for a good tutorial. The basic concepts, however, are not difficult:

(a) two QKD endpoints establish communications via a dedicated fibre or wavelength for the quantum path, and via the internet for messaging;
(b) the transmit side prepares and transmits raw keys, from which both sides come to agreement on a shared, secret key;
(c) this secret key is then employed in the cryptographic gateway for protecting message traffic that will transit the internet within secured IPsec tunnels.

As in the simpler schematic, this diagram depicts two private enclaves—at the left and right edges of the drawing—connected via two distinct communications networks, namely, the internet for message traffic and a fibre optic QKD channel for key distribution. Each cryptographic gateway is implemented via a pair of specialized computers. The VPN computer implements the non-real-time portions of the gateway, and in particular both the QKD protocols and the internet protocol suite. It also contains the encryption device for message traffic. The optical process control (OPC) computer runs instrument-control programs that perform management of the optical and electronic devices that comprise the QKD laser source suite and avalanche photo-diode (APD) detector suite. These two computers are linked via a private ethernet that carries control traffic between them, including the raw key symbols as transmitted or received via the QKD link.

*New Journal of Physics* 4 (2002) 46.1–46.12 (http://www.njp.org/)
In our first link, the QKD physical layer employs BB84 [7] with a weak-coherent source and phase modulation. Current designs call for use of commercial telecommunications devices throughout the physical layer, in particular for an attenuated Mitsubishi FU-68PDF-V520M61B source at 1550 nm, cooled JDS Uniphase-Epitaxx low noise APDs, EPM 239 AA SS, as gated detectors, JDS Uniphase phase modulators at 1550 nm and polarization-maintaining fibre within the source suite and detector suite. The physical channel between source and detector suites is standard telecommunications fibre, i.e. it does not maintain polarization. An auxiliary bright source at 1300 nm is multiplexed onto the link to provide timing and framing signals for the detector suite. Our second link will employ an entangled source currently being developed by Sergienko’s research team at Boston University [8]. From an architectural standpoint, this new entangled source will fit neatly into the same general structure as the first weak-coherent link, and provide similar security guarantees. However the Boston University source should provide greatly improved throughput over the weak-coherent link.

At higher levels of the protocol stack, we have extended the KAME version of NetBSD [9], with a modified version of the ‘raccoon’ internet key exchange (IKE) protocol engine [9], to accept and employ keys produced by our QKD links. These keys are currently used as seed values for an AES encryption algorithm for traffic protection. We supply a new seed value for the AES key, derived from the QKD link, every few seconds; contrast this with the daily or monthly key update typical of many secure networks. (Although this practice is not as secure as a one-time pad, rapid rekeying is useful in practice since key bit entropy is spread over a relatively small amount of traffic.) We have developed a C language suite of QKD protocols, as described below, that refine the raw key material provided by the QKD physical layer and that convey refined key material to IKE. These higher layers of the system are currently integrated and operational.
This system can be most easily understood by following its operation during routine practice. At such time, the VPN and OPC computers operate in only loose synchrony. In essence, the OPC source and detectors suites provide a continuous stream of raw key symbols to their corresponding VPN computers. These symbols include both the basis used for a given bit (as transmitted or received) and the bit’s value, along with QKD framing information. As the VPN computers receive these frames of raw key symbols, they perform a suite of well known QKD protocols (sifting, error correction, privacy amplification etc) transported through the internet as public channel in order to derive the actual ‘good’ key bits. These good bits continuously accumulate in a reservoir of shared keying material within each QKD endpoint. Referring back to figure 2, this keying material is then available for use via the IPsec protocol suite where it can be used to encrypt one or more secure tunnels through the internet. In particular, the keying material is fed to an encryption device (crypto) for use in encrypting or decrypting IP datagrams as they pass through the VPN computer. For traffic flows that must be very highly secured, a one-time pad (Vernam cipher) approach may be employed. For less critical traffic flows, the key may be used as input to an encryption algorithm such as the AES, triple data encryption standard (3DES) etc. As has been discussed above and by others [10], the QKD mechanisms may thus be employed to rekey such algorithms at fairly high rates, e.g. multiple times per second, which may improve the overall system security.

In short, the QKD keying material is employed in both VPN computers as keys for the local crypto device. Then as traffic flows enter the VPN computer in the clear from the private enclave (conventionally known as the ‘red’ side of the gateway), they pass through this crypto and become encrypted. These encrypted datagrams are then carried through the ‘black’ public internet, or any other suitable communications network, until they are received at the distant VPN gateway, where they are passed through another crypto and thus decrypted, and then sent once again in the clear onto the ‘red’ private enclave at the distant location.

Figure 3 provides a finer-grained schematic of the multiple layers of protocols and algorithms in a useful QKD protocol suite. This figure is drawn in accordance with the conventions of network engineering, in which the physical layer is depicted at the bottom of the diagram and
higher layers rely on the products of those beneath them. The reader should thus read from the bottom of the diagram up to follow the refinement process.

Most sublayers present a number of options. For example, encoding options include BB84 versus B92 [11], polarized versus interferometric encodings [8], weak-coherent versus entangled [1], round-trip versus one-way [1] etc; error detection and correction options include Cascade [12], simple parity as in Los Alamos [10] etc. Most of these options have been previously implemented, either in functioning QKD systems or in simulations, with the apparent exception of authentication, which must include continuous authentication via an initial seed of key material at the endpoints, periodically refreshed by drawing off unused keying material that has been disseminated via QKD links in operation. At the time of writing, we have implemented encoding, sifting and error correction layers embedded into an overall framework for public QKD protocols. This framework is extensible so that we may experiment with alternative options for one or more layers. All protocol engines are implemented in ANSI C; it is planned to make them freely available for other researchers.

4. System architecture of a trusted network

As useful as a QKD point-to-point link may be, it still suffers from striking drawbacks. First, it is geographically constrained by the distance over which a single link may be operated. Fibre attenuation limits terrestrial links to 50 km or less in practical applications. Free-space links, e.g. to airborne relays or satellites, may allow wide-area or even transcontinental links but still do not permit truly global coverage. Second, isolated point-to-point links are subject to simple denial-of-service attacks such as active eavesdropping or cutting the fibre. Third, in practice it may be prohibitively expensive to establish pairwise, dedicated point-to-point links between all private enclaves that wish to communicate with each other.

To a surprisingly large extent, these drawbacks can be mitigated by organizing a number of QKD links into a QKD network, which is the second major step in our research program. Figure 4 depicts a QKD network in highly schematic form. As in previous diagrams, QKD endpoints
can be seen to the left and right edges of the diagram. Behind these cryptographic endpoints lie private enclaves. In contrast with the point-to-point links described before, however, the QKD endpoints are now linked via a mesh of QKD relays or routers.

As depicted, this form of a QKD network is composed from a collection of point-to-point QKD links. Thus the leftmost QKD endpoint exchanges keying material with relay A, which in turn exchanges keys with some or all of its neighbours, i.e. relays B and/or C, etc. When a given point-to-point QKD link within the relay mesh fails—e.g. via a fibre cut or too high a level of eavesdropping or noise—that link is abandoned and another used instead. Thus the overall QKD network can be engineered to be resilient even in the face of active eavesdropping or other forms of denial-of-service attacks.

Such QKD networks can be built in several ways. In one variant, the QKD relays may transport only keying material but never message traffic. Thus after the various relays have established pairwise agreed-to keys along an end-to-end point, e.g. between the two QKD endpoints, they may employ these key pairs to securely transport a key ‘hop by hop’ from one endpoint to the other, being one-time-pad encrypted and decrypted with each pairwise key as it proceeds from one relay to the next. In this approach, the end-to-end key will appear in the clear within the relays’ memories proper, but will always be encrypted when passing across a link. Such a design may be termed a ‘key transport network’.

In another variant, the QKD relays may transport both keying material and message traffic. Figure 5 illustrates this second variant, in which the relays are acting as internet-like routers with pairwise QKD mechanisms providing link encryption between the routers. In essence, each IP datagram of message traffic is encrypted once as it transits from the QKD endpoint to its first relay. Then it is decrypted, held in the clear in the relay’s memory, and then re-encrypted with a second set of keys and sent onwards to the next relay. This operation proceeds, hop by hop, until the datagram is finally received at the destination endpoint and sent onwards to the attached private enclave. We note that this network differs from the standard definition of the internet by interposing a set of encrypted tunnels (‘virtual links’) between cooperating routers.

Such QKD networks bring important benefits that greatly mitigate the drawbacks of point-to-point links enumerated at the start of this section. First, they can greatly extend the geographic

**Figure 5.** QKD network with trusted relays and link encryption.
reach of a communications network secured by quantum cryptography, since wide-area networks can be created by a series of point-to-point links bridged by active relays. These links can further be heterogeneous transmission media, i.e. some may be through fibre while others are freespace. Thus in theory such a network could provide fully global coverage. Second, they lessen the chance that an adversary could disable the key distribution process, whether by active eavesdropping or simply by cutting a fibre. A QKD network can be engineered with as much redundancy as desired simply by adding more links and relays to the mesh. Third, QKD networks can greatly reduce the cost of large-scale interconnectivity of private enclaves by reducing the required \((N \times N - 1)/2\) point-to-point links to as few as \(N\) links in the case of a simple star topology for the key distribution network.

Such QKD networks are by no means panaceas, however. Their prime weakness is that the relays must be trusted. That is, since keying material and—directly or indirectly—message traffic are available in the clear in the relays’ memories, these relays must be prevented from falling into an adversary’s hands. In practice, they would need to be in physically secured locations and perhaps guarded if the traffic were truly important. Although this is a fairly onerous condition, we note that only the relay devices themselves must be secured; fibres or freespace links between them do not need such protection. Hence only a finite number of small areas would require high levels of physical security. A related, but perhaps more subtle, drawback is that all users in the system must trust the network (and the network’s operators) with all keys to their message traffic. Thus even if a pair of users have unusually sensitive traffic, they must expand the circle of those who can be privy to it to include all machines, and probably all operators, of this QKD network that is used to transport this sensitive traffic. This is obviously undesirable for truly sensitive traffic, where the circle of trust (the trusted computing base [3]) should be kept as small as possible.

One further caveat bears emphasis. Single-link security has been thoroughly investigated to date but we are not aware of any similar proofs for QKD networks. Detailed and explicit proofs will be required before these networks can be declared ‘secure’.

5. System architecture of an untrusted network

As in classical cryptography, an end-to-end approach is likely to provide the most satisfactory architecture for disentangling the users’ keying material for secured traffic flows from the network that transports such flows. We propose an approach that introduces unamplified photonic switches into the QKD network architecture in order to provide end-to-end key distribution via a novel mesh of untrusted switches.

Figure 6 depicts this architecture in schematic form. By contrast with the trusted network architecture, the untrusted QKD switches do not participate in the QKD protocols at all. Instead they are merely used to set up all-optical paths through the network mesh of fibres, switches and endpoints. Thus in essence a photon from the leftmost QKD endpoint proceeds, without measurement, from switch to switch across the optical QKD network until it reaches the rightmost QKD endpoint at which point it is detected. We currently anticipate that the QKD switches will be built from MEMS mirror arrays, or equivalents, together with novel distributed protocols and algorithms that allow end-to-end path setup across the network, and that (as in untrusted networks) provide a robust means for routing around eavesdropping or failed links.

New Journal of Physics 4 (2002) 46.1–46.12 (http://www.njp.org/)
Untrusted QKD networks have different strengths and weaknesses than trusted QKD networks. Their main strength is that they provide truly end-to-end key distribution; QKD endpoints need not share any secrets with the key distribution network or its operators. This feature may be extremely important for highly secure networks. Their weaknesses appear significant, however. Unlike trusted relays, the untrusted switches cannot extend the geographic reach of a QKD network. In fact, they may significantly reduce the network’s reach since each switch adds at least several dB loss to the photonic path. In addition, it will likely prove difficult in practice to employ a variety of transmission media within an untrusted network, since a single frequency may not work well along a composite path that includes both fibre and freespace links. Untrusted networks may also introduce new vulnerabilities to traffic analysis.

On a cheerier note, the principal weakness in untrusted QKD networks—limited geographic reach—may potentially be countered by quantum repeaters [13]. There is currently a great deal of active research aiming towards such repeaters, and if practical devices are ever achieved, they should slide neatly into the overall architecture of untrusted QKD networks to enable seamless QKD operations over much greater distances than are currently feasible.

6. Conclusion

QKD techniques can be married to standard internet technology in order to provide highly secure communications for practical use. A research program is outlined that will integrate both weak-coherent and entangled QKD links with internet technology, and demonstrate QKD networks of both trusted (opto-electronic) and untrusted (passive photonic) switches. Such networks should be able to route around eavesdropping, noise and denial-of-service attacks on the QKD links.

Acknowledgments

We are deeply indebted to Dr Mike Foster (DARPA ITO) and Dr Don Nicholson (Air Force Research Laboratory) who are the sponsor and agent, respectively, for this research project. We also thank Professor Paul Kwiat and the anonymous referees for New Journal of Physics. This
paper reflects highly collaborative work between the project members. Of these, particular credit is due to Alexander Sergienko and Gregg Jaeger (Boston University), John Myers (Harvard) and Alex Colvin, William Nelson, David Pearson, Oleksiy Pikalo, Greg Troxel and John Schlafer (BBN). Our interest in QKD networks was sparked by the prior work of, and discussions with, the quantum cryptography groups at IBM Almaden and Los Alamos, and by the kind hospitality of Dr David Murley several years ago.

References

[1] Gisin N et al 2001 Preprint quant-ph/0101098
[2] Schneier B 1996 Applied Cryptography (New York: Wiley)
[3] Menezes A et al 1996 Handbook of Applied Cryptography (Boca Raton, FL: Chemical Rubber Company Press)
[4] Comer D 2000 Internetworking with TCP/IP (Englewood Cliffs, NJ: Prentice-Hall)
[5] Kent S and Atkinson R 1998 Security architecture for the internet protocol Preprint RFC 2401
[6] Harkins D and Carrel D 1998 The Internet Key Exchange (IKE) Preprint RFC 2409
[7] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore) (New York: IEEE)
[8] Walton et al 2001 Performance of photon-pair quantum key distribution systems J. Mod. Opt. 48 2055–63
[9] http://www.kame.net/
[10] Hughes R J et al 1996 Quantum cryptography over underground optical fibres Advances in Cryptology—CRYPTO ’96 (Springer Lecture Notes in Computer Science vol 1109) ed N Koblitz (Berlin: Springer) pp 329–42
[11] Bennett C H 1992 Quantum cryptography using any two non-orthogonal states Phys. Rev. Lett. 68 3121
[12] Brassard G and Salvail L 1994 Secret key reconciliation by public discussion Lecture Notes in Computer Science vol 765 (Berlin: Springer) p 410
[13] Duan L-M et al 2001 Long-distance quantum communication with atomic ensembles and linear optics Nature 414 413