Quantum key distribution: Awesome or pointless?

Some believe the advent of quantum computing will reduce the time taken to solve cryptographic algorithms so dramatically that they will no longer provide effective security. **Sheila Cobourne** and **Dr. Carlos Cid** explain how Quantum Key Distribution could provide a solution.

Royal Holloway University of London

SearchSecurity.co.UK

INTRODUCTION

Cryptography is one of the success stories in the information security world. Properly implemented cryptography allows sensitive information (such as credit card details) to be transmitted through a potentially insecure environment like the Internet. It provides the essential security services of confidentiality, integrity and authentication for millions of day-to-day transactions.

However, some of the most popular types of cryptography rely on the difficulty of solving hard mathematical problems to provide security against attack: it is believed that the advent of quantum computing will reduce the time taken to solve these problems so dramatically, that they will no longer provide an effective security method.

All is not lost, though — a totally new technique, quantum cryptography, is waiting in the wings. This harnesses the laws of quantum mechanics, along with quantum computing power, to provide information security. Since quantum computing is still in its infancy, this is still largely a theoretical area, but one type of quantum cryptography is achievable with today's technology — Quantum Key Distribution (QKD). This uses the quantum properties of light sent along a specialised channel (quantum channel) and existing laser, fibre-optic and free-space transmission technologies can support this.

QKD's security is based on the laws of quantum physics alone, rather than hard mathematics, and is unbreakable. However, some analysts do not see the need for QKD, as existing non-quantum (classical) cryptographic systems are secure enough. (The security guru Bruce Schneier has called quantum cryptography "as awesome as it is pointless," so no prizes for guessing where he stands on the issue!)

This article describes quantum key distribution, its strengths and weaknesses, its place within cryptography, and whether it is actually needed at all. It will also identify potential applications and commercial prospects of QKD. But, fear not, no quantum physics or mind-boggling mathematics will be used! Of necessity, technical terms are needed throughout the report, so some basic cryptography will be explained in the next section, before proceeding on to a discussion of QKD itself.

CRYPTOGRAPHY BASICS

Cryptography is generally used when communicating parties wish to exchange information over

an insecure channel. Within the cryptographic community, these communicating parties are conventionally called Alice and Bob: it is assumed that messages and information sent between them could be subject to eavesdropping by an adversary called Eve. (Alice, Bob and Eve aren't necessarily human, by the way — they could also be PCs or software.)

Keys are a fundamental element of cryptography. They are special pieces of data that are carefully generated for use in the encryption and decryption of sensitive information. It is essential that the keys are kept secret. This is related to the well-known Kerckhoff's principle, which states that the security of a cryptographic system should not rely on the secrecy of the algorithm used for encryption and decryption, but rather on the secrecy of the key.

Cryptography could not function without keys, but it is a major challenge to ensure that the correct key is available to Alice and Bob at the right time. There are several approaches to overcome this problem: a key can be generated centrally and sent to Alice and Bob when needed (key distribution) or Alice and Bob could generate a key between themselves (key establishment or key agreement). However, no existing method is 100% secure. For example, a very secure way of distributing keys uses a trusted courier to physically transport a key in a tamper-proof medium (such as a smart card). However, if the courier is actually untrustworthy he or she can change or damage the key in transit, and the procedure fails.

Cryptography could not function without keys, but it is a major challenge to ensure that the correct key is available to Alice and Bob at the right time.

Different security levels can be achieved by classical cryptography. Computational security exists where a system is theoretically breakable by trying every possible key — the brute-force attack — but the computational effort required to do so is so time-consuming and expensive that it is not economically viable for an attacker to perform the attack. Unconditional or perfect security exists in cases when, even if an attacker has infinite resources at their disposal, the system still cannot be broken.

The One-Time Pad (OTP) is a method for achieving perfect security of encryption, provided that it uses a key that is randomly generated, as long as the message and is used only once. However, OTPs have immense practical difficulties: generating long, truly random keys is problematic; distributing the keys to recipients is a logistical nightmare; sender and receiver have to be totally synchronized to make sure that the same keys are used for the same message; and ensuring keys are never re-used is a challenging task. For this reason, OTPs are currently seldom used in practice, but as will be seen in this report, when combined with quantum key distribution they become a much more realistic option.

Now the terminology is clearer, a brief description of quantum key distribution follows - where the cryptographic and quantum world meet.

HOW DOES QKD WORK?

Despite its name, quantum key distribution is a key establishment method which creates key material by using the quantum properties of light to transfer information from Alice to Bob.

Alice sends some quantum information to Bob along a specialised quantum channel, such as a fibre optic link. Depending on how he sets his detection equipment for each piece of quantum information sent, Bob's measurements will either be perfectly correct, or a completely random value. This is a direct consequence of quantum physics. The sending and receiving of quantum information is the only quantum part of QKD: everything that follows is done using conventional technology, and is called classical post-processing.

Alice and Bob then use a secure classical communications channel to compare Alice's information sent with Bob's information received, and they decide which measurements will be used to generate the secret key. This potential key material is subjected to standard error-correcting routines, and then compressed in a process known as privacy amplification. The next phase, however, is the most important: authentication. Quantum key distribution is vulnerable to Man-in-the-Middle attacks, where an attacker not only controls communications between Alice and Bob but impersonates Alice to Bob and vice versa. Authentication is essential to ensure information is being transferred between the correct parties.

Once all the classical post-processing has been successfully completed, the key that has been established can be used by Alice and Bob in classical encryption.

If Eve attempts to intercept the initial quantum

communication, she will always be detected thanks to the effects of quantum mechanics: a higher than expected number of errors will occur in Bob's measurements. Alice and Bob can then abandon the key and try again at a different time when Eve has retreated, cursing the laws of physics. A key established via quantum key distribution simply cannot be compromised by Evil Eve.

Alice and Bob can then abandon the key and try again at a different time when Eve has retreated, cursing the laws of physics.

A point to remember is that all key material produced by quantum key distribution is stored on conventional equipment, and used in classical encryptions: quantum computers are needed to store information in quantum form, and they are not available using current technology.

WHAT ARE QKD'S STRENGTHS?

Quantum key distribution is a particularly good method for producing long random keys. A property of quantum key distribution is that a relatively short input can be used to generate perfectly secure random key material ever after, as follows. A secret key is shared between Alice and Bob to authenticate the very first quantum exchange: it has been shown that using part of the output of this QKD session to authenticate the next QKD session means that this second round is also perfectly secure. QKD can therefore be run almost continuously without loss of security, and the short initial key can be expanded: each new QKD session key is independent of all previously used keys, so this reduces the number of ways a malefactor can attack the system.

Additionally, security provided by QKD is future proofed: it means that even if a cryptographic system is broken at some unspecified future time, previous messages sent through it remain secure. The unconditional security of QKD systems has been mathematically proven: even in the face of an adversary with infinite supplies of time and processing power, the security simply cannot be broken.

And, of course, Eve is forced to pack up her eavesdropping kitbag and head for the hills, howling in frustration because she will always be found out.

WHAT ARE QKD'S WEAKNESSES?

Quantum key distribution sounds almost too good to be true, and yet there has been no mass stampede to implement it on a large scale. There are a number of technical weaknesses, but the crux of the matter is — do we really need it?

Technical weaknesses appear when the practicalities of QKD implementation are assessed: quantum channels can only work over a limited distance; information currently can't be transferred fast enough to provide adequate service levels; quantum optic equipment is vulnerable to attack; and an expensive new infrastructure will be needed to support quantum processing.

But the real issue — the $64,000 question — is whether QKD is actually necessary. There are classical equivalents to all the functions it provides, and introducing quantum key distribution, with its associated perfect security, does not necessarily increase the overall protection of a system. As Bruce Schneier states "[s]ecurity is a chain: it's as strong as its weakest link". It is possible to build an insecure system using strong cryptography, whilst believing that the overall security level is as strong as the cryptographic mechanism used. Classical cryptography is an extremely strong defence mechanism. If a security system fails, it is much more likely to be through human deficiencies — a password written on a Post-it note stuck to a screen, for example — than by cryptographic attack.

Also, despite rumours of its imminent demise, it's not all doom and gloom in the classical arena. Admittedly, cryptography-killing mathematical advances could happen at any time, regardless of quantum computing developments. But when quantum computers' spectacular processing capabilities render some schemes unusable, other types of algorithm will remain secure by simply increasing the length of the key. There are also new cryptographic methods under development, which are immune to quantum processing advances.

Is the promise of perfect security a big enough business imperative to warrant the expense of specialised equipment and infrastructure? Classical cryptography provides more than adequate security, so the benefits of QKD are really unclear: should pragmatism win over theory? Examining some of the proposed practical applications may shed some light on this dilemma.

QKD NETWORK APPLICATIONS

A networked solution suggests itself because of the technical restrictions on quantum channels.

Quantum channels only function over a limited distance, and amplification of the quantum information signal won't be possible until quantum computers are available. Joining many "Alice-Bob" QKD paths into a quantum network extends the range of the quantum information transfer, and this has been tested practically: the EU-funded SECOQC project operated one such network as a field trial in Vienna in 2008. A classical key management infrastructure was designed to support this network's quantum capability, including unconditionally secure classical authentication of each quantum link to prevent man-in-the-middle attacks.

Several manufacturers took part in the SECOQC project, including idQuantique and Toshiba, testing a range of commercially available equipment and quantum transfer techniques. Most exceeded the SECOQC performance objectives for both key generation rates and the distance the quantum signal could travel — a very encouraging start for a new technology.

Along with specialised quantum generation and measurement equipment, a quantum channel and a conventional communications channel, Alice and Bob need to pre-share an authentication key before they can attempt quantum key distribution. This means QKD networks are "closed" because only authorised parties with appropriate equipment can overcome the barriers to joining. This is in marked contrast to the freely available, "open" network that is the Internet, where anyone with a PC and a phone connection can join in the online fun.

The closed nature of QKD networks suggest that they are best suited to high security, controlled environments, where only users who are known and trusted can use them.

The closed nature of QKD networks suggest that they are best suited to high security, controlled environments, where only users who are known and trusted can use them. But QKD, when combined with OTPs or other existing cryptography can result in very long-term security. This may be useful in organisations such as Government and Intelligence agencies or businesses with long-term strategic trade secrets which need

to be kept confidential.

Another application arena for QKD may be in Closed Electronic Data Interchange systems (EDI), such as the SWIFT and CHAPS systems, which are used for high value banking transactions. Quantum key distribution has already been used to safeguard financial transactions; in 2004, money was transferred between Vienna City Hall and Bank Austria Creditanstalt — a donation of €3,000 from the Mayor of Vienna to the University of Vienna.

SHORT RANGE QUANTUM KEY DISTRIBUTION APPLICATIONS

Another implementation approach concentrates on very short range QKD, where a quantum "Alice module" is held on a portable token/smart card (a "quantum token") and a quantum "Bob module" is fixed into a permanent structure such as a bank ATM ("quantum ATM"). They communicate via free-space quantum optic technology (i.e. there is no fixed fibre optic link between them), and use classical authentication methods to keep the man-in-the-middle at bay.

A "quantum top-up" procedure uses this equipment to generate keys via QKD: these keys (sometimes called "quantum secrets") can be used immediately at the quantum ATM or stored securely on the quantum token for later use. Once a key has been used in a transaction, it is deleted from the quantum token, so the quantum top-up procedure needs to be repeated at intervals: i.e. the key is a consumable.

This method could potentially be used in both anti-skimming procedures and online banking applications.

Skimming attacks are used to steal card and PIN data at bank ATMs. If a key generated in a quantum top-up process is used immediately at the quantum ATM to encrypt a PIN via a one-time pad, perfect security can be achieved. Eavesdropping of the quantum top-up will always be detected, and perfect security cannot be broken, so skimming will become impossible.

Online banking fraud is increasing, not because bank systems are easy to break into — they are not. Instead, online banking users are targeted to get them to reveal security information. Examples include "phishing" emails which trick the user into revealing secret password details or active attacks which redirect unsuspecting users to malicious websites which harvest their data.

Some banks have implemented authentication schemes using "something you know" (a PIN) and "something you have" (a dedicated card

reader for a Chip and PIN bank card). Using a suitable reader, this approach could be adapted to use keys stored on a quantum token. As keys are deleted from the token once they have been used, this limits the number of times the token could be used before a visit to a bricks-and-mortar bank facility is necessary to perform a quantum top-up procedure.

Another method of authentication (used widely in Germany) is the Transaction Authorisation Number (TAN) scheme. TANs are 6 digit numbers issued to bank customers, to be used to authenticate transactions online in conjunction with a PIN. TANs can be supplied on printed lists, or sent to the customer's mobile phone (Mobile TAN or mTAN). However, there are security weaknesses: for example, criminals are paying high prices for old Nokia 1100 mobile phones which can be re-programmed to use someone else's phone number, and hence receive their mTANs.

Using a suitable reader, the keys stored on a quantum token could be used in authentication via a TAN system. The quantum top-up procedure is very similar to other methods of obtaining TAN lists from banks — i.e. in a separate stage, independent of the online transaction.

COMMERCIAL PROSPECTS

For a technology to become successful commercially, it must solve a business problem, save money or make an existing procedure more streamlined. There will be applications where QKD could be ideal — replacing trusted couriers or in high security environments for example — and others where the benefits are not so clear — e.g. anti-skimming and online banking. In all cases, extensive (and expensive) infrastructure is needed to allow the technology to work.

Research and development continues to increase the efficiency and reduce the cost of the equipment needed for quantum key distribution.

Research and development continues to increase the efficiency and reduce the cost of the equipment needed for quantum key distribution. For example, in 2009, Toshiba Research Labs developed a new photon detector: this allows faster transfer rates along longer quantum channels to be achieved. Andrew Shields of Toshiba

commented that it "means we could have 8,000 users and the technology starts to become very useful". Commercially available products such as idQuantique's Cerberis have been designed to fit into existing fibre-optic networks, to provide both QKD and classical encryption which achieve the highest security levels. MagiQ's QPN Security Gateway is advertised as being suitable for use in the military, intelligence, financial and disaster recovery arenas. There is clearly a confidence in the QKD equipment supplier world that there is a market for their goods.

Compliance regulations, such as BASEL and Sarbanes-Oxley, require companies to protect their data from threat.

Compliance regulations, such as BASEL and Sarbanes-Oxley, require companies to protect their data from threat. This may lead to increased pressure on organisations to use the most up-to-date security technologies such as QKD. Building systems that are future-proofed is highly desirable: QKD can play its part here, too.

With regard to portable applications aimed at the general public, ease of use will be paramount. QKD anti-skimming benefits will be gained without any extra effort on the part of the user; however, the use of keys from a quantum token in online banking is less convenient than present systems, and would require a culture shift in usage for the U.K market. Unlike a Chip and PIN card, which can be used whenever it is needed (funds allowing!), a quantum token uses up its keys every time a transaction is done, and requires regular replenishing via a quantum top-up procedure. There may be times when the quantum token is unusable if there are no keys left on it.

However, in other countries (e.g. Germany) where the TAN system of authentication is in use, the consumer experience is different. As procedures already exist for TANs, introducing a quantum top-up stage (assuming equipment and infrastructure is in place) would be a replacement process rather than an addition, and hence may be more acceptable to users.

Ultimately the business decision whether to adopt this new technology will boil down to a cost/benefit analysis. Costs are measured in hard cash and working hours for personnel: benefits however can be intangible as well as squarely aimed at the balance sheet. There may be reputa-

tional advantages for an organisation if they adopt QKD technology: implementing the newest, coolest technology makes a business seem cutting-edge. On the other hand, introducing an immature new security technology could be detrimental to corporate image if it does not work as well as expected and leaves the organisation open to attack.

Does new technology necessarily equate to better technology? The benefits of quantum key distribution may only be marginal for some applications: it may be that the large corporate investment required for QKD infrastructure, equipment and education could be better spent developing less radical technologies to solve the same business issues.

Business decisions are never easy!

CONCLUSION

The overall conclusions that can be drawn from this study are somewhat mixed.

Commercial success for a technology occurs when its benefits to an organisation outweigh its costs. Benefits can be tangible (e.g. money saved) or intangible (e.g. reputational benefits). For example, an intangible benefit could be gained if an organisation thinks that by using the most up-to-date techniques, they will gain a degree of kudos as an early adopter — this intangible benefit may be seen as a means to competitive advantage. Deploying quantum tokens and ATMs requires a huge investment in infrastructure: it is debatable whether this could be justified financially. QKD networks are, therefore, most suited to high security environments where costs may not be a stumbling block.

Deploying quantum tokens and ATMs requires a huge investment in infrastructure: it is debatable whether this could be justified financially.

There are applications that need the perfect security a one-time pad encryption can offer: since quantum key distribution is good at creating the required long random keys from a short input, OTPs could therefore become a more practical option.

Had QKD been a mature technology when Chip and PIN systems were introduced in 2006, it would have been a relatively easy (although more

costly) task to include quantum processing modules in the Chip and PIN readers to provide quantum top-up capability. Or, if quantum computers were currently sophisticated enough both to endanger the security levels provided by mathematically intractable cryptography and to provide fully-functioning quantum networks, then QKD could provide an excellent method of key establishment in a quantum computing environment. Unfortunately, neither of these scenarios is true, so quantum key distribution has arrived in the commercial sphere both too early and too late — the right technology, at the wrong time.

Research efforts continue to make quantum equipment faster, more effective and cheaper. Eventually there will come a time when the performance and cost differences between conventional and quantum networks will be negligible and the implementation decisions can be based on security issues alone.

The main problem QKD faces is that all potential application areas identified for it have existing classical methods of achieving very good security levels. It would be a brave executive indeed who attempts to justify the costs of installing expensive new equipment and changing existing systems so that extremely good security can be upgraded to (claimed) perfect security. The cost and consequences of adopting a "good enough" route rather than a "perfect" one have to be managed as part of an organisation's overall risk portfolio.

Eventually there will come a time when the performance and cost differences between conventional and quantum networks will be negligible and the implementation decisions can be based on security issues alone.

Although absolute confidence in quantum key distribution may be slightly misplaced at the moment, it is most certainly an area that merits further research. Bruce Schneier's description — "awesome [but] pointless" — is not 100% true. *"Awesome"*? Definitely. Using quantum mechanics to provide unconditional, eavesdropper-proof security is awesome by any standard. *"Pointless"*? Not totally. QKD can co-exist peacefully alongside classical cryptographic methods, not replacing but

enhancing them. Used in carefully selected applications in this way, quantum key distribution could have a viable commercial future awaiting it. ■

ABOUT THE AUTHORS

Sheila Cobourne has a background in systems analysis and worked in multi-national oil companies and financial organisations before taking an extended career break to raise a family. During this time she also studied part-time for an MBA and MSc in Mathematics.

Introduced to cryptography though mathematics, she became interested in the wider area of information security, which led to her taking the MSc at Royal Holloway.

Sheila is currently applying to do a doctorate at Royal Holloway. Her research interests include smart cards, cryptography and the human aspects of information security.

Dr Carlos Cid received his PhD in Mathematics from the University of Brasilia, Brazil in 1999. He joined the Information Security Group at Royal Holloway in October 2003 and has a broad interest in the area of information security, in particular cryptography.