DIY-QKD – the results of an Innovate UK Quantum Technologies Germinator project investigating a passive, chip-based approach to Quantum Key Distribution

Friederike Jöhlinger, Andriy Boubriak & James Lee

It's well known that during the second world war, codebreakers at Bletchley Park cracked the Enigma code with help from Polish mathematicians, rendering the Enigma machine insecure. What happened afterwards is less well known – the Allies did not reveal the ability to crack the code and sold captured enigma machines to developing countries. Wave Photonics, a UK start-up (with our own Polish mathematician!) has explored a scheme to securely encrypt information, the question is - should you trust us?

Introduction

Cryptography is vital for the functioning of modern society – it is needed for everything from protecting financial transactions and securing confidential medical data to protecting critical infrastructure.

Current encoding schemes rely on algorithms such as RSA or elliptic curve cryptography. The basis of this security is that cracking these problems is hard for classical computers. This is not the case for quantum computers – the creation of a quantum computer would render current approaches to cryptography insecure. Furthermore, it's possible to simply store an encrypted message or file sent today, then to decrypt it later when quantum computers become available, meaning that information sent now is not safe from future quantum attacks.

There are two approaches to dealing with this threat: The first relies on new types of mathematical schemes, which are assumed to be resistant to the special abilities of quantum computers and is called post-quantum cryptography. A second option is given by Quantum Key Distribution (QKD), where instead of relying on mathematical problems, quantum effects are used to establish a secure key between two parties.

The advantage of the latter approach is that the security of QKD can be proven, based on current understanding of quantum theory, and does not depend on the abilities of a computer, now or in the future.

However, this security is dependent on the implementation of the system – even for schemes designed to be independent of the equipment used (called Device-Independent or DI-QKD), QKD systems can't guarantee security against malicious devices inserted at the manufacturer's site or in transit before they reach the users. Given this, a clear risk to the security of a QKD system is interference by malicious actors in the system assembly or development.

It was this issue that led us to wonder: Is it possible for us to develop an approach to QKD that would be secure, even if one of us were a spy?

Funded by an Innovate UK Commercialising Quantum Technologies Germinator Project, Wave Photonics has been investigating an approach where users can easily assemble their own QKD systems using components and supply chains that they trust; an approach we call DIY-QKD.

Approaches to securing data against quantum attacks.

Current approaches to cryptography are largely insecure against attacks from a sufficiently powerful quantum computer. Post Quantum Cryptography (PQC) represents that fastest and most cost-effective way to ameliorate this - new encryption algorithms designed to be secure against quantum attacks can be implemented in software with no need for expensive new infrastructure. PQC is still in development with NIST running an ongoing process to determine the most suitable candidate. PQC is likely a valuable tool and has a role to play in defending our communications against future quantum threats. However, there is no guarantee that these approaches will be secure against future advances in computing (in fact, one of the leading candidates in the NIST PQC competition was recently found to be insecure, even to attacks from a laptop!)

For critical applications, or for information which must be kept confidential for long timescales, there is more justification for the additional costs and infrastructure required for QKD. There are multiple companies around the world selling QKD systems with several more companies in the development process. The commercial systems available today come as complete systems from a single supplier, typically with costs of hundreds of thousands of pounds per system. Although there are efforts to reduce costs, space and energy consumption via the use of integrated photonics for QKD, these systems are not yet commercially available (to the best of the authors' knowledge).

There have been field demonstrations of QKD systems and telecoms service providers are demonstrating QKD networks using trusted nodes, with the view to eventually creating large scale QKD networks to serve as a layer securing the existing networks. For example, the EuroQCI Initiative aims to build a secure quantum communication infrastructure that will span the whole EU.

DIY-QKD

To create an alternative to having to buy a complete QKD system from a single vendor, Wave Photonics has been developing a new approach to QKD: DIY QKD. Over the past 6 months, we have investigated an approach based on an easily characterizable, passive chip, which can be combined with lasers, detectors and simplified control electronics by an end user, telecoms service provider or systems integrator to create a full QKD system. At the time of writing, we are in the process of patenting this approach and have designed the first version of the chip. Key rates have been calculated and are feasible, being only slightly lower than ones from conventional QKD approaches.

The approach we are developing is based on the idea of disaggregation, with transparent, open-source control and processing software and generic components from supply lines trusted by the user. The only specialised component would be a passive optical chip, for which there are many fabrication options.

In addition, the security of many QKD systems depend on random number generation, for which Quantum Random Number Generators (QRNG) are frequently used – the reliability and control/readout electronics of a QRNG are another potential weakness in a QKD system, i.e. if the

QRNG is compromised, the QKD system can be compromised. Our approach does not depend on a dedicated QRNG.

All of this means that, as a vendor, our ability to compromise the system is greatly reduced compared to selling a full system or active chip/co-packaged chips with complex control electronics; the passive optical chip could be well characterised optically by the end user and the open-source approach would make the control and processing software open to public scrutiny.

As well as developing this scheme, we have explored the benefits and disadvantages of our approach for a commercial and technical perspective – the following sections provide an overview of what we found.

Integrated photonics

Perhaps unsurprisingly for an integrated photonics company, we found that there were many advantages to taking a chip-based approach to implementing our scheme (although in principle it could be implemented using bulk optics). Our scheme relies on multiple, phase-stabilised interferometers – this is much simpler to do using quantum photonic integrated circuits (QPICs) which generally have much greater phase/temperature stability relative to bulk optical setups and do not require extensive alignment.

As well as reduced active stabilisation requirements, QPICs can be cost-effectively manufactured in volume and are lighter and more compact than bulk optics-based alternatives, giving a Size, Weight, Power and Cost (SWaP-C) advantage.

Lastly, at the expense of some of the benefits of the DIY approach, there is scope for full integration of the photonic part of our scheme with lasers and detectors being included on or co-packaged with the chip. This would further reduce the size and cost of the system and the simplified photonic and electronic requirements of our scheme may make it more cost-effective than competing chip-based QKD technologies. That said, as the cost of packaging is typically 70%-90% of the cost of manufacture for integrated photonic products, this approach may not be significantly cheaper than competing chip-based approaches at scale.

Passive scheme

To avoid ambiguity, by passive, we mean that the chip does not contain any electronically-controlled components to determine the sent key or decoy states. The scheme of course requires the use of lasers and detectors, which are active components, but the sent key and decoy states are not actively encoded via modulators or laser seeding.

When considering integrated photonic approaches, the passive scheme has the benefit of not requiring active on-chip components which means that it is suitable for multiple platforms including Silicon Nitride (SiN) (a platform which does not typically allow for active components). Active chips are typically more difficult and expensive to produce, so this simplifies the fabrication process and requirements and so reduces the cost per chip.

The ability to use multiple platforms also means that it is possible to use a wider range of wavelengths for the scheme – for example, Silicon on Insulator (SOI) is typically used for telecoms wavelengths (most frequently ~1310 nm and ~1550 nm) where optical fibres have minimal

dispersion and low loss respectively. However, for some applications, shorter wavelengths offer better performance, for example free space/satellite QKD is frequently done using wavelengths of ~850 nm, but SOI has very high loss for wavelengths below 1 um. The ability to use SiN for our scheme means that it is suitable for satellite and free-space operation.

Furthermore, the use of telecoms wavelengths is generally required by the properties of conventional optical fibre, but the development and commercialisation of hollow core fibres suitable for other wavelengths can change this – for example, it could enable fibre-based QKD at short wavelengths, where single photon detectors and cheaper and more efficient. SiN chips designed to implement our scheme would support the development of systems which use this approach.

Finally, the passive approach removes the need for a modulator, which reduces the cost and the complexity of the control electronics, as well as reducing the vulnerability to Trojan Horse attacks (where an eavesdropper uses an external laser to observe the operation of the modulator to determine the sent key).

Disaggregation

For QKD, the trustworthiness of the supply chain is of great importance as malicious components can compromise the integrity of the system. For the creation of QKD networks across or between nations, these nations can best ensure the integrity of the supply chain by ensuring that it is contained within their borders. As, there are presently relatively few QKD system vendors, national telecoms service providers may not have the option to buy QKD systems from organisations headquartered in their own country, which would result in a reliance on foreign nations and companies for critical infrastructure. The national telecoms providers that we spoke to in this project expressed a reluctance to be dependent on foreign suppliers in this way.

Additionally, as not all nations will have a complete sovereign supply chain, their ability to ensure the integrity of each of the components is reduced. This can be countered using approaches to QKD that are more robust to the inclusion of malicious devices – the idea behind this approach is that it is more challenging for an eavesdropper to compromise devices from multiple suppliers in a coordinated way than to compromise the system at a single location. Our early analysis shows that our passive scheme could be adapted to be suitable for this approach and the DIY nature lends itself to compatibility with multiple suppliers.

However, while the initial motivation for the disaggregated approach was to improve the system security, we found that perhaps the biggest advantage is in improving supply chain robustness.

For datacoms and telecoms, disaggregation can be used to reduce cost and remove the dependence on a single supplier. Even so, over reliance on a single supplier and international supply chains were all issues were highlighted as areas of high concern by the guidance on the telecoms sector, released in January 2020 by the National Cyber Security Centre (NCSC).

For example, BT has been forced to remove all of Huawei equipment from the network – this is expected to take until 2027, delay the 5G rollout by up to 3 years and cost £500 million.

Sanctioned suppliers are not the only risk, the COVID-19 pandemic has shown that supply chains can be fragile and unexpectedly disrupted.

Consequently, we believe that to ensure continuity of service, QKD infrastructure providers should endeavour to have flexible supply chains and use disaggregation to reduce the reliance on individual suppliers – QIY-QKD would enable this.

Certification and standards

Standards are still in development for QKD and are vital for ensuring future interoperability between QKD systems. Additionally, there is ongoing work by ETSI and BSI to enable security accreditation and certification of QKD systems.

Interoperability will reduce the vendor lock in and supply chain fragility for the creation and maintenance of QKD networks.

In the project proposal, we expressed doubts as to the usefulness of relying on certifications for security in QKD, especially when there have been examples of certifications failing to ensure the intended quality and performance in other industries. However, our market research highlighted the importance of certification for both the purchasers (e.g. telecoms service providers) and end users (e.g. governments) of QKD systems. It is not practical for end users to perform their own security analysis for each system given the range of skills required, so certification is a requirement for many end users to be confident that the system is in fact secure. From the perspective of service providers and the purchasers of QKD systems, certification serves as a form of passing the blame in the event that a system is insecure.

An ETSI white paper on Implementation Security of Quantum Cryptography discussed sophisticated example attacks such as Trojan-horse attacks, photon number splitting attacks and detector spoofing attacks. Surprisingly however, it did not include guidance on ensuring that the system is not compromised at the site of manufacture.

It remains to be seen if this will be sufficient for end users sending highly sensitive information where security against systems compromised at the manufacturer's site is required.

We conclude that in order to be relevant to the widest possible user base, our DIY-QKD scheme implementation would have to be certified and conform to the necessary standards. Our market research revealed that the additional security possible via DIY-QKD was not seen a key benefit for many potential customers as certified systems would enable them to offer QKD services while affording them protection in the event that the systems were compromised.

Conclusions

We believe that it is advisable to make efforts to secure communications against quantum attacks given the continuing advance of quantum computing technology. Post Quantum Cryptography, although much faster and cheaper to implement, does not necessarily provide protection against future quantum attacks, meaning that Quantum Key Distribution has an important role to play in securing sensitive information or critical infrastructure.

Although the weakness of current QKD approaches to compromisation at the site of the manufacturer was accepted by the organisations that we spoke to, the use of certified and ready-assembled systems was more important to their business case than the extra security that they may

gain in principle by using DIY-QKD. We have yet to determine if this is also the case in applications where very high levels of security are required.

Sacrificing the DIY approach and fully integrating our scheme would likely provide a cost-effective way to produce QKD systems suitable for developing standards and certification, but this may not be significantly cheaper than other QPIC-based approaches at volume.

However, the supply chain aspects afforded by the disaggregated nature of our approach appear to be highly relevant as the importance of trustworthy and robust supply chains for critical infrastructure becomes a topic of increasing focus for national governments.

Additionally, the ability of our scheme to remain chip-based over a wide wavelength range makes it suitable for fibre and free-space implementations of QKD, as well as novel approaches using non-standard wavelengths to benefit from improved source, fibre or detector characteristics.

A route to commercialising the progress made in this project would be the development of a company which interfaces with multiple fabs, manufacturers and packagers to produce QKD systems suitable for certification. This would enable organisations, countries or collections of countries to purchase QKD systems assembled using domestic suppliers or specified and controlled supply chains, reducing the fragility of supply and risk of insertion of malicious components for QKD systems relative to buying complete systems from a single supplier.

If you find this topic interesting, have any questions, or would like to tell us that we are wrong about something, please get in touch via our website: https://www.wavephotonics.com or via email: info@wavephotonics.com.