Quantum Encryption in Military Communications

Lt M.J.L. Colbeck RN MSci

November 6, 2023

Abstract

The development of Quantum Computers poses an existential threat to modern secure communications due to their ability to process data exponentially quicker than a conventional computer. This new threat is the largest threat posed to modern communications since the invention of the first computers during the Second World War. This paper explores the requirement to adopt quantum resiliant, “post-quantum”, encryption into the military environment to avert information leakage and disaster on the battlefield.

Biographical Notes

Morgan Colbeck was born in Bedfordshire and quickly developed a keen interest in science and technology. After attending Bedford School he moved on to the University of Durham, choosing Collingwood College due to his love of rugby.

He graduated in 2018 in Natural Sciences, specialising in Maths & Physics. Despite choosing Black Hole Thermodynamics as the topic of his dissertation, he was exposed to Quantum Computing and Quantum Optics, which quickly became a key interest as his understanding of cybersecurity developed.

After graduating, he briefly worked as a computer programmer for BAE Systems Applied Intelligence (now Digital Intelligence) before joining the Royal Navy in September 2019 as an Officer Cadet, training to become a Weapons Engineer Officer.

Following short assignments on HMS Prince of Wales and HMS Defender as well as further training at HMS Collingwood, he joined HMS Duncan as the Weapons Section Officer (WSO) in May 2022. He then moved on to become the Communications and Information Systems Engineer (CISE) in January 2023, gaining a good understanding of how military communications are currently configured.

Now Lt. Colbeck, he is serving as the Deputy Weapons Engineer Officer (DWEO) on board HMS Duncan and, at time of writing, is deployed with the Standing NATO Maritime Group 2 (SNMG2) in the Mediterranean.

Outside of work, he continues to engage with his interest in computer programming, teaching people in his spare time, as well as his constant interest in rugby. He now lives in Guildford, Surrey with his wife Annabel whom he recently married in December 2022.

1 Introduction

The decisive factor in the Allied victory in the Second World War was attributed to Project Ultra by Eisenhower. The benefits of which were especially gained in naval warfare where the long time scales naturally benefit from early warning. This was especially notable in the Battle of the Atlantic (Padfield, 1995) where the interventions by Bletchley Park allowed crucial allied supply convoys to evade their hunters. This kept the United Kingdom in the war, allowing eventual allied victory.

The gargantuan was achieved by espionage, technology, and good luck in equal measure. Since the Second World War, the rate of technological progression has accelerated. Combining this with the potential advent of Quantum Computing, what is the threat to modern military communications and does the very quantum technology itself offer a solution?

This article is a brief exploration of the threat posed to military communications as well as an application of the current preventative measures being undertaken in the civilian world to the military scenario.

2 Threat Analysis

Though deception, and intelligence of the enemy's deception, has been an integral part of warfare since Sun Tzu "where you are strong appear weak and weak appear strong" (Tzu, 2021). The mass mobilisation of armies in the late 19th Century brought a new requirement for secure long range communications. As the benefits reaped from keeping your communications and intended movements secret grew more and more, so too did the importance of cryptanalysis (the method of breaking codes).

The 20th Century brought increased opportunities for this new information based warfare with the advent of improved long range communications. Benefits were obtained by the British in the First World War by the Admiralty's Room 40 breaking the German naval codes (Beesly, 1982). This allowed the Royal Navy to detect and outmanoeuvre the German fleet in the North Sea, directly leading to the endurance of the naval blockade throughout the war. Knowledge of the enemy's movements, especially when naval timescales are considered, allows one's own units to be moved into position such that these plans can be defeated.

When the Second World War broke out, the kinetic effects of code breakers were again demonstrated at the Battle of Matapan. Due to the intelligence provided by Bletchley Park (Ferris, 2020), Admiral Cunningham understood the makeup of the Italian fleet, which aimed to intercept a convoy, and was therefore able to prepare and execute a counter. This victory crippled the Italian Regia Marina, allowed Malta to endure, and directly lead to the allied success in the turning point victory at El Alamein, the aftermath of which allowed the allied success of the North Africa campaign.

The outcome of military communications being broken, as shown at Matapan, is defeat, death, and loss of assets. This means that the cost of a data breach can be considered to be catastrophic, warranting enormous precautions to avoid it.

This example shows the catastrophic kinetic effects of broken military communications. Exceptional measures are therefore warranted in order to prevent such an event taking place. By contrast, in the civilian sector, the cost of a data breach could vary depending on which data was breached. Therefore the approach taken by companies such as AWS, Amazon Web Services, must be considered to be the absolute minimum standard adopted by the military for securing communications.

Military communications are a sufficiently large target, in comparison to a small business, that all conventional TESSOC (Terrorist, Espionage, Sabotage, Subversion, and Organised Crime) threat actors are credible players. Any communication system must therefore be able to resist each of these. These can be considered to have different levels of resources and interest in cracking military communications. State level espionage can be broadly considered to be the most dangerous and threat actors in this category can be assumed to have state of the art methods and equipment.

In addition, when military communications are monitored it would be very difficult to prove when another actor has cracked the codes in question. Indeed a key requirement of the Ultra programme during the Second World War was that its intervention was not revealed so that the enemy was not afforded an opportunity to change its encryption system (Winterbotham, 1974). This means that if a breach takes place, the military would probably not be aware until after kinetic effects have begun to be experienced.

As early detection and treatment is a key factor in compensating for weaknesses in most security systems, the difficulty in detecting a breach means that security measures must be more restrictive to further reduce the probability that a breach would take place. This further necessitates more restrictive and secure methods of communication than would be used in the civilian sector.

Most cryptographic systems attempt to meet the ideal standard given by the One Time Pad, detailed in Annex A, and the military is no exception. However, due to various real world requirements, this standard cannot be obtained and one of the key requirements is usually sacrificed to obtain a greater level of practicality.

Military cryptography uses a similar encryption system to that used in GSM mobile phone networks and Bluetooth. Both of these have been broken, as shown in (Lu et al., 2005) & (Barkan et al., 2008), with classical methods using a long period of data gathering and cryptanalysis, both of which it can be assumed that TESSOC and state level espionage threats in particular have had.

It is worth noting at this point that this encryption method overcomes the One Time Pad's difficulties with key distribution (Annex A for details) by sacrificing the requirement for true randomness. This means that military cryptography is *not* uncrackable. However, it is currently considered sufficiently difficult to crack that the information will no longer be useful by the time that it is cracked. This assessment is due to the fact that no breach has been discovered, a flawed assessment due to the earlier mentioned strategic imperative to not reveal when an opponent's communications have been broken.

The emerging quantum threat allows new algorithms to be used which were impractical when modern encryption was designed. In particular, Simon's algorithm (Simon, 1997) allows the period of the pseudo random sequence to be found with substantially less computing power than a conventional computer. From this the number of Linear Frequency Shift Registers themselves can be identified and the number of required entangled Qubits (quantum bits) known. This result can then be combined with Grover's algorithm (Grover, 1998) to find the initial seed exponentially faster than will a conventional computer.

The overall result of these factors is that a state level actor, who must be assumed to be developing state of the art quantum computers by modern risk analysis, presents a potentially catastrophic threat to modern encryption. In the financial sector, following the release of (bof, 2022), when analysing a risk the potential outcome must be considered as something which *will* happen, as opposed to something which *might* happen. The military must take this new risk definition into account when performing a risk assessment. Therefore, since there is a potential outcome in which military communications could be broken, it must be considered that this will occur making expensive and exceptional actions warranted to be undertaken in order to avert disaster.

3 Industry's Example

With the rise of cloud computing services and their increasing role in the economy, the threat posed to the RSA algorithm (block diagram in Figure 1, from (noa)), and its implementation in the SSL/TLS protocol, by quantum computers becomes ever more important to counteract. This threat is very well understood due to numerous internet security audits. It is thought that the RSA algorithm will become obsolete once the quantum breakthrough takes place due to the speed of Shor's algorithm (Shor, 1994) on a quantum computer. This timeframe is subject to debate but some estimates have a 50% likelihood of this occurring within 10 years (Grobman, 2020).

Precedent with the SHA2 vulnerabilities (Schneier, 2015) shows that immediate action needs to be taken to avoid catastrophe. Consequently, the US National Institute of Security Technology (NIST) has been researching

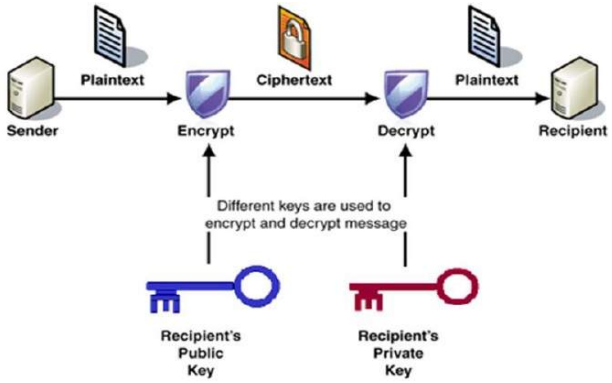

Figure 1: RSA Algorithm and Public Key Cryptography

post quantum cryptography over the last 10 years, with parallel accreditation boards elsewhere, notably the EU's PQCRYPTO project.

Amazon Web Services, AWS, presents an industry target large enough to be roughly comparable to the military target. They have made it policy to adopt post quantum encryption algorithms and are currently implementing a hybrid approach, encrypting both with SSL/TLS as well as quantum resistant (Peikert, 2014), lattice based encryption algorithms, called "post-quantum" encryption.

This approach means that the data cannot be compromised without **both** the lattice encryption and the SSL/TLS encryption being compromised. The benefit of this is that it allows the organisation to hedge against potential vulnerabilities not yet found in the new encryption system.

Lattice based encryption offers other advantages, with both public and private components. This allows one of the key drawbacks of the one-time pad to be overcome: authentication. Lattice based encryption therefore facilitates identity verification (Güneysu et al., 2012), a key advantage in a world where phishing attacks are becoming more prevalent and useful for digital signing in line with the MOD policy of "Digital by Default".

Another key advantage of adopting this is the option to add verification to messages ensuring that they actually do come from where they claim to have come from. As the Navy moves increasingly towards web based applications and sailors using MOD provided devices for working remotely, this reduces the risk posed by a spoof website or by phishing emails.

This encryption method is entirely open source (Yuan et al., 2018) and is grounded in modern technology (Güneysu et al., 2012). There is no requirement for a hardware update and therefore overhead cost is minimised. The only initial cost is in adding the required code to the existing code base. In addition, as only the encryption algorithm has changed, there is little noticeable difference to the end-user, therefore requiring no retraining to utilise this new system.

It should be noted at this point that a critical difference between AWS and the MOD is that AWS operates an open system, with no real restrictions on what devices can be used to connect to their systems. The cryptographic system therefore must be able to be distributed over the internet, or generated locally by a standard Commercial off the Shelf (COTS) device.

However, since the MOD can control all devices used to access the cloud services, unlike AWS, there may be stronger, symmetric systems that are not as generic in their application as lattice encryption. There is also the drawback that since these methods were only developed recently, there are no personnel currently employed in the MOD who are experienced with these methods. Building this level of capability takes time and investment.

The key benefit of this comparison is that AWS is a commercial entity. It therefore has a commercial interest in publicising their measures to secure clients' data. Clients naturally being drawn to cloud providers who are more proactive in securing their clients' data. By contrast, military organisations are naturally secretive about their ideas of future encryption.

4 Quantum Communications

Since the threat actors are larger than those posed to industry as well as the consequences of broken encryption being higher, a better standard of cryptography is warranted. This solution could come in the form of quantum key distribution (QKD). A simple block diagram is in Figure 2, from (Nurhadi and Syambas, 2018).

However, QKD is dependent on components that are manufactured on the quantum scale, making them extremely difficult and expensive to produce. As military applications require a large amount of assets, as well as

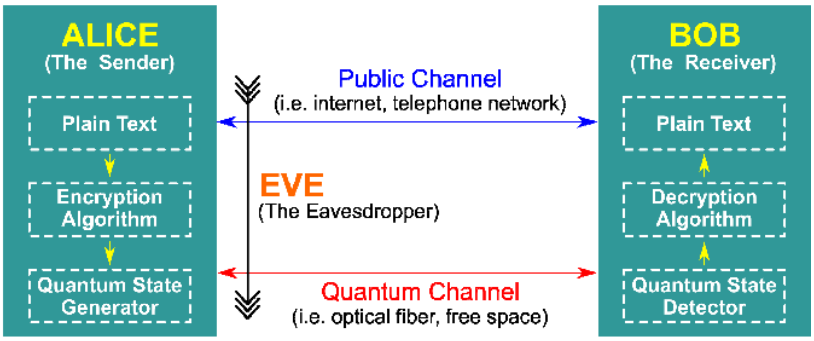

Figure 2: Quantum Key Distribution Block Diagram

spares for endurance, this cost factor could be prohibitive for an already budget restricted Navy. In addition, there is no guarantee that this investment will provide any appreciable increase in secrecy than the lattice algorithms, or other post quantum algorithms, discussed earlier.

This quantum equipment relies on highly qualified personnel to diagnose and repair any issues with the equipment, requiring a large amount of time and resources and would have to be done concurrently with any design and issuing of equipment to ensure that there were people capable of maintaining it as the equipment is rolled out.

These drawbacks aside, the magnitude of the threat warrants exceptional effort to be expending in securing communications and the cost factor will be broadly disregarded in the following analysis.

Broadly, naval applications can be broken down into: shore to shore, communication between bases where hard line links are required; shore to sea, communication between a shore base and a vessel operating at sea anywhere in the world where hard line links cannot exist; and sea to sea, communication between units in a task group, normally on a tactical level, where hard line links are not required.

For all discussed quantum encryption protocols, it is assumed that there is a parallel classical communications channel as well as the quantum channel. In most applications, the encrypted data is then transmitted through the classical channel.

The most common implementation of QKD is known as the BB84 protocol as developed in 1984 by Bennett and Brassard. It should be noted at this point that this is not the only QKD protocol and there are other options. See (Bennett and Brassard, 2014) for an explanation of BB84. BB84 was notably proved to be secure in (Shor and Preskill, 2000). A huge benefit of BB84 is that it is evident when the communications have been intercepted by a third party, making it clear when someone is eavesdropping communications and aiding the detection criterion for an encryption system.

Quantum cryptography was, when originally proposed in 1984, merely a theoretical idea. This is no longer the case. From 2004 to 2007, the DARPA quantum network ran constantly as a 10 node quantum network (Elliott et al., 2005), executing quantum cryptography on a macro scale in a practical system. This concept has since been developed and achieved through commercial fibre optics in Guangzhou up to 50km (Zhang et al., 2019).

Specialist quantum networks have been built in the EU as well as in China with a 2,000 km line between Beijing, Jinan, and Shanghai, combined with a 2,600 km satellite link to reach Haifei as shown in Figure 3 from (Chen et al., 2021). This is the first fully integrated ground and space quantum network.

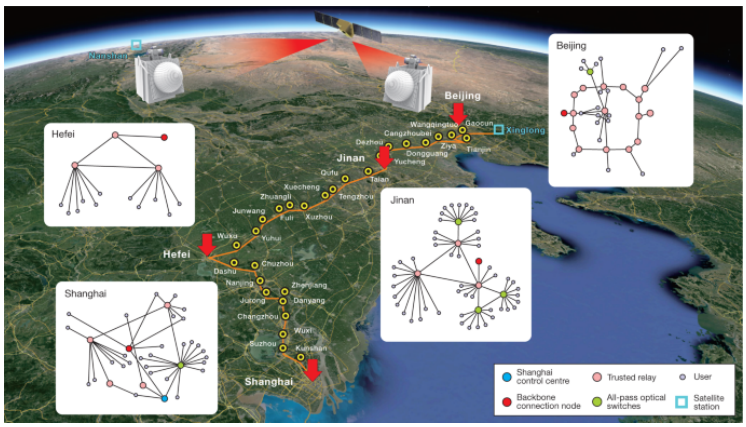

Figure 3: Chinese Specialist Quantum Network

Quantum networks are not only possible, they are a practical reality offering secure, uncrackable communications with specialist networks proven to span up to 2,000 km with current technology. This offers a unique opportunity to improve existing links between shore military establishments and upgrade their networks.

There are however considerable drawbacks to laying specialist networks, even if cost itself were not a factor. The main issue being that it removes the reliability advantages offered by the conventional internet system. Through packeting and checksums, the internet can send information from A to B which will find a route even if certain communications lines are damaged, shown in Figure 4, from (Keary, 2020). This factor was a key design requirement of the original ARPA net in preparation for conflict with a peer adversary and should not be discarded lightly.

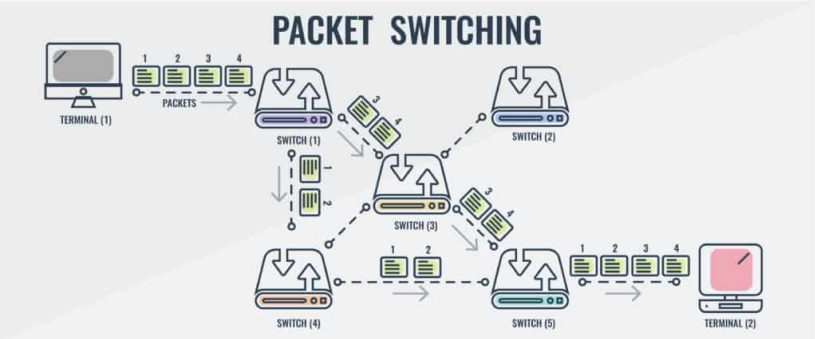

Figure 4: Internet Packet Switching

By laying specialist networks, this advantage of the internet is removed and everything becomes intrinsically tied to the specialist networks, which are subject to the same damage as the civilian network but have fewer cables, and therefore less redundancy, available. This limits the robustness of the network and renders it unacceptable for military use, where reliability is essential.

The approach of using the same civilian fibre optic networks must therefore be used due to the reliability these networks offer. This also offers the benefit of partially hiding the network traffic within public communications as well as reduced cost.

5 Shore Based Communications

In the Information Age, the requirement for the easy and timely distribution of intelligence and general information is directly linked to the success of a nation's military. Due to the nature of this information and the need for secrecy, the measures taken to prevent others from accessing this information can be prohibitive to the ease of its use.

As more and more separate bases are responsible for collecting and sorting information and the importance of access to it grows, it becomes crucial to be able to pass this information without it being couriered. Laying a specific network for this communication would be expensive. Additionally it is unlikely to remain classified where the network is to be laid due to the magnitude of the work required. This renders it vulnerable to sabotage or eavesdropping, as well as carrying a large cost requirement.

Quantum Cryptography offers a unique opportunity in this field. The advances made and exhibited by the Chinese teams above have shown that it is possible to achieve an uncrackable, quantum encrypted network through the conventional internet at ranges up to 144km, within current limitations. This would permit secure, uncrackable communications between NCHQ and Northwood (separated by under 130km).

It is possible that this distance could grow with technological advances however with these current limitations it is possible to establish communications nodes spanning the whole country and connecting all major military bases with a secure, uncrackable network. However, this approach would require a large amount of processing power to enable decrypting and re-encrypting potentially terabytes of data at each node. Additionally, a large number of trusted personnel would be required at each node, aggravating the risk of a compromised person intercepting the unencrypted data and transferring it onto an unsecure channel.

A potential benefit of this approach is that each node would be linked with fewer other nodes than a wholly interconnected web. This would reduce the impact of the handshake problem and the data could be decrypted at each node and re-encrypted to travel to one of a few subsequent nodes. There would also be a lower administrative burden on the staff at each node to manage fewer entangled particles, further assisted by the short distances facilitating an easier exchange of entangled particles should they lose their entanglement.

The node approach further assists the core requirement in maintaining the requirement for dynamic re-routing and required in the original ARPA net. Failure at a single node could be mitigated by routing around the failed node and finding an alternate path.

The benefits of such a network are obvious. Above SECRET communications could be performed easily, and with a lesser administrative burden, through the conventional internet. Such communications would have been validated to have come from where they claim to have come from, due to the requirement to exchange entangled particles. The fact that the encryption is quantum teleported prevents the interception of the one-time pads required to encrypt the data.

Once an above SECRET communications channel has been established through the existing fibre optic networks, classified data could be passed across the whole country securely. This would enable distribution of and access to the data across the many outstations who would require it.

Though the cost of establishment is high for such a network, it is achievable with current technology and the benefits of its establishment would facilitate easier collaboration between the distributed intelligence sites around the UK.

6 Naval Scenario

The maritime, ship to ship, scenario offers many unique challenges which must be included in any perspective communication solution. In brief these are: all communications must be wireless; communications must be able to be obtained beyond the horizon; secure communications must be able to be established with other units without requiring prior exchange of cryptographic keys; solutions must be ruggedized and capable of surviving rough seas; and all items must be easily replaced while at sea. Each of these points will now be examined in turn.

The field of wireless quantum key exchange has had substantial advances. A joint Chinese Austrian project has been investigating the possibility of satellite born QKD systems to facilitate quantum encrypted communications between continents. The first quantum capable satellite was launched in 2016 (Lin et al., 2016) and the capability was tested with a video call between China and Austria (Nordum, 2017). The data rate required for such a call would exceed the operational requirement for a ship.

China's target is a worldwide Micius satellite network by 2030 designed to give worldwide, quantum enabled, communications. China is evidentially preparing for a world post quantum computers and is heavily investing in infrastructure to prepare for the result of a breakthrough. This presents a large threat as the level of investment from a peer adversary is clearly anticipating a breaking the quantum barrier.

Such a network of satellites would allow for ships to obtain beyond the horizon communications with each other, essentially becoming a quantum equipped Tactical Satellite. Additionally, geostationary quantum ready satellites would allow for quantum encrypted strategic communication between a deployed ship and home base. However, entanglement based encryption would not be suitable for these uses. This is due to the significant inconvenience and cost factor introduced should the ground station's and satellite's particles lose their entanglement.

Furthermore, the nature of naval warfare means that Task Groups are regularly formed from several units across coalitions of nations and rarely, if ever, does the same composition remain for together for the entirety of an operation. This fact fully eliminates the possibility of utilising an entanglement based QKD solution as this would necessitate prior meeting.

A line of sight quantum communications solution would be more suitable for Task Groups and ship to ship tactical communications as well as applications for shore to shore communications. The current understood limit for this is 144km for both optical based (Schmitt-Manderbach et al., 2007) and entanglement based solutions (Ursin et al., 2007).

Since the two parties would need to convene beforehand and share entangled particles, the entanglement based solution is impractical for rolling task group compositions with multinational components, where communications flexibility is a necessity. However, since at sea line of sight is unlikely to be blocked, the optical based solution within a task group is much more feasible.

Rolling Task Group composition also introduces another weakness of quantum cryptography: the no cloning theorem (Wootters and Zurek). This theorem dictates that it is impossible to make a perfect copy of an arbitrary particle without first measuring it and retransmitting. Despite the no cloning theorem playing a key role in the security proofs of QKD methods such as BB84, it also prevents the same key being used across a Task Group. Instead, each unit would have to perform key exchange with every other unit. Despite no prior exchange being required, there still is a requirement for key exchanges growing proportional to n^2, similar to the handshake problem. This presents a massive drawback and reduction in capability from the current system. In addition this key exchange problem would make simultaneous transmission of communications very difficult as multiple simultaneous transmissions would be required to communicate with all units.

The difficulties suffered by the Chinese teams in deploying their quantum satellites are worth examining prior to designing and deploying a maritime quantum encryption solution. Though the maritime environment does not have the immense forces and vibrations experienced during a spacecraft launch, the maritime environment will continue to affect all equipment mounted on a ship while a satellite, especially a geostationary satellite, is calm and stable once in orbit.

Subjecting sensitive quantum scale equipment to constant disturbances means that the equipment is almost certainly going to lose its alignment during the course of its lifetime. The equipment must be rugged enough to withstand these near-constant perturbations for long enough so that the operators can gain a reasonable amount of usage in between recalibrations. In addition, the equipment must be able to be recalibrated by a maintainer while at sea, since wear and tear must be expected on a deployed warship. It must be also be expected that it is impractical to call out a specialist to the deployed unit in order to repair the system. Repairs must therefore be able to be made by the Ship's maintainer.

These practical engineering issues are not impossible to find a solution for. However they would have a high cost in both money and time prior to being able to be deployed on a warship. Combining this with the difficulties of key exchange with multiple units, it becomes undeniable that QKD is not yet a feasible path to explore for maritime units.

7 Conclusion

Encryption as a whole is threatened by the upcoming quantum revolution. Industry is increasingly moving to conventional "post quantum" algorithms in their implementations of online services. The disastrous outcome which is promised by broken encryption necessitates that this example must be followed in the military context.

There have been substantial advances in the field of "post quantum" cryptography allows for quantum resistant algorithms to be implemented with little impact to the experience for the end user. When the end user cannot, and should not, be considered to be an expert, the simplest solution must be implemented. In this situation, the simplest solution is the one which is most similar to the current cryptography implementation.

As the military increasingly follows the overall trends towards future cloud based services, accessible to personal devices, the amount of data available increases the problem presented by failed encryption. This necessitates the adoption of "post quantum" encryption to increase the resistance of the organisation to the threat posed by advances in quantum computing.

Quantum cryptography technology itself offers an opportunity for an arbitrarily large amount of one time pads to be distributed and used without the traditional difficulty associated with one time pad distribution. This allows uncrackable communications between assets giving a huge advantage in a military context and presenting an option for securing the most sensitive data distributed across several shore sites for redundancy.

However, quantum equipment is fragile, expensive, and requires a high level of competence to operate. These drawbacks, coupled with the requirement for each pair of units to have their own one time pads, mean that quantum cryptography is not feasible for maritime units as current technology allows. Therefore, the military should follow the example of AWS and adopt conventional "post quantum" algorithms on maritime units due to their low cost entry and utilisation of current equipment.

Despite this, there are obvious advantages to implementing a quantum ready network between shore bases, allowing current infrastructure to be used and further decentralisation around the country, increasing redundancy in the networks. Investment and adoption of these technologies must be made a priority for the MOD to enable diversification and decentralisation of intelligence hubs and distribution of their data.

A One Time Pad Cryptography

Before exploring different encryption methods, it is necessary to understand the gold standard of encryption: One Time Pad Cryptography.

In 1919 by Joseph Mauborgne applied the one time tape system to military communications. It is still considered uncrackable to this day (Kahn, 1996), since it would be possible to decrypt any message which has the same number of characters. However, the following conditions must be maintained:

1. The key must be truly random.
2. The key must be at least as long as the plaintext.
3. The key must never be reused in whole or in part.
4. The key must be kept completely secret.

However, there are problems with the one-time pad which weaken the practical cryptographic effectiveness. These are:

1. True randomness
2. Key distribution
3. Authentication

Each of these will now be examined in turn.

A.1 True Randomness

It is difficult to generate a large number of truly random numbers. Modern computers are not able to do so and instead generate pseudo-random numbers. As such, it is possible that the resulting sequence can be identified and exploited by a potential adversary.

A.2 Key Distribution

The one time pad requires all parties who are communicating to be using prior shared secrets. This is not a problem when short, infrequent communication is required, however it is a very large problem when a large number of large messages needs to be sent as it is likely that the communicating parties will run out of one time pads.

A key example of this is naval vessels which are required to be away for long periods of time, often without secure channels through which to receive additional one time pads. Should they run out of pads they would be unable to communicate securely with other platforms, a massive weakness.

A secondary issue of this problem is that the one-time pad should only be used for communication between two parties. This means that the number of pads that is required grows in proportion to n^2 where n is the number of parties communicating, in a similar fashion to the handshake problem. For an organisation which needs to communicate with a large number of platforms over arbitrarily long periods separated, the problems presented by the need for effective key management are massive and almost insurmountable when prior storage is required.

A.3 Authentication

There is no way to tell if the person actually sending the message is truly the person that claims to be sending the message. An adversary could intercept the message, decrypt it (with a captured one time pad copy), and substitute a different message to disrupt the plans. For example, the message “meet Jane and me tomorrow at three thirty pm” could be changed to “three thirty meeting is cancelled, stay home”. This would create a large amount of chaos for the parties planning. However, this is mitigated by the difficulty of obtained the pad’s key.

References

Public Key Encryption. URL hiips://wwwtutorialspointcom/cryptography/public_key_encryption.html. Publication Title: Tutorialspoint.

Model risk management principles for banks, June 2022. URL hiips://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2022/june/model-risk-management-principle-for-banks.pdf.

E. Barkan, E. Biham, and N. Keller. Instant ciphertext-only cryptanalysis of GSM encrypted communication. *Journal of Cryptology*, 21(3):392–429, 2008. Publisher: Springer.

P. Beesly. *Room 40: British Naval Intelligence 1914-18*. Hamilton, 1982. ISBN 978-0-241-10864-2.

C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014. ISSN 0304-3975. doi: hiips://doi.org/10.1016/j.tcs.2014.05.025. URL hiips://wwwsciencedirectcom/science/article/pii/S0304397514004241 .

Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, and others. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 589 (7841):214–219, 2021. Publisher: Nature Publishing Group.

C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh. Current status of the DARPA quantum network. In *Quantum Information and computation III*, volume 5815, pages 138–149. International Society for Optics and Photonics, 2005.

J. Ferris. *Behind the Enigma: The Authorised History of GCHQ, Britain's Secret Cyber-Intelligence Agency*. Bloomsbury Publishing, 2020. ISBN 978-1-5266-0549-8. URL hiips://books.google.co.uk/books?id=fDztDwAAQBAJ.

S. Grobman. Quantum Computing's Cyber-Threat to National Security. *PRISM*, 9(1):52–67, 2020. Publisher: JSTOR.

L. K. Grover. A framework for fast quantum mechanical algorithms. In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 53–62, 1998.

T. Güneysu, V. Lyubashevsky, and T. Pöppelmann. Practical lattice-based cryptography: A signature scheme for embedded systems. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 530–547. Springer, 2012.

D. Kahn. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Schribner, 1996. ISBN 978-1-4391-0355-5.

T. Keary. Circuit Switching vs Packet Switching: Differences, Pros & Cons, June 2020. URL hiips://wwwcomparitechcom/net-admin/circuit-switching-vs-packet-switching/ . Publication Title: Comparitech.

J. Lin, P. Singer, and J. Costello. China's quantum satellite could change cryptography forever. *Popular Science*, 3, 2016.

Y. Lu, W. Meier, and S. Vaudenay. The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption. In V. Shoup, editor, *Advances in Cryptology – CRYPTO 2005*, pages 97–117, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg. ISBN 978-3-540-31870-5.

A. Nordum. China demonstrates quantum encryption by hosting a video call. *IEEE Spectrum*, 3:16–19, 2017.

A. Nurhadi and N. Syambas. Quantum Key Distribution (QKD) Protocols: A Survey. *2018 4th International Conference on Wireless and Telematics (ICWT)*, pages 1–5, 2018.

P. Padfield. *War Beneath the Sea: Submarine Conflict During World War II*. Wiley, 1995. ISBN 9780471146247.

C. Peikert. Lattice cryptography for the internet. In *international workshop on post-quantum cryptography*, pages 197–219. Springer, 2014.

T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, and others. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters*, 98(1):010504, 2007. Publisher: APS.

B. Schneier. *Applied Cryptography: Protocols, Algorithms and Source Code in C*. Wiley, 2015. ISBN 978-1-119-09672-6. URL hiips://books.google.co.uk/books?id=VjC9BgAAQBAJ.

P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994. doi: 10.1109/SFCS.1994.365700.

P. W. Shor and J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.*, 85(2):441–444, July 2000. doi: 10.1103/PhysRevLett.85.441. URL hiips://link.aps.org/doi/10.1103/PhysRevLett.85.441. Publisher: American Physical Society.

D. R. Simon. On the power of quantum computation. *SIAM journal on computing*, 26(5):1474–1483, 1997. Publisher: SIAM.

S. Tzu. *The Art of War*. Diamond Pocket Books Pvt Ltd, 2021. ISBN 978-93-90960-03-3. URL hiips://books.google.co.uk/books?id=JmAkEAAAQBAJ.

R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, and others. Entanglement-based quantum communication over 144 km. *Nature physics*, 3(7):481–486, 2007. Publisher: Nature Publishing Group.

F. Winterbotham. *The Ultra Secret*. A Dell book. Harper & Row, 1974. ISBN 978-0-06-014678-8. URL hiips://books.google.co.uk/books?id=HNKEAAAAIAAJ.

W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*.

Y. Yuan, J. Xiao, K. Fukushima, S. Kiyomoto, and T. Takagi. Portable Implementation of Postquantum Encryption Schemes and Key Exchange Protocols on JavaScript-Enabled Platforms. *Security and Communication Networks*, 2018, 2018. Publisher: Hindawi.

Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, and H. Guo. Continuous-variable QKD over 50 km commercial fiber. *Quantum Science and Technology*, 4(3):035006, May 2019. doi: 10.1088/2058-9565/ab19d1. URL hiips://doi.org/10.1088/2058-9565/ab19d1. Publisher: IOP Publishing.