Proceedings of the INMM & ESARDA Joint Virtual Annual Meeting
August 23-26 & August 30-September 1, 2021

Quantum Information Science and its Implications for International Safeguards

Alec Poczatek
Argonne National Laboratory

Claudio Gariazzo
Argonne National Laboratory

Sean Martinson
Argonne National Laboratory

Charles Broomfield
Argonne National Laboratory

David Farley
Sandia National Laboratory

ABSTRACT

Quantum technologies promise great benefits to society through enabling development of advanced materials and pharmaceuticals, for example. However, they may also pose some consequences, in particular the ability of quantum computers and associated quantum algorithms to break currently used encryption protocols. We provide a background on the various quantum technologies being developed, including not only quantum computing, but also quantum sensing and simulation as well as quantum encryption. We highlight some quantum sensing examples that could be of benefit to the IAEA through the ability of quantum sensing to provide ultrasensitive measurements and super-resolution of images and spectra. Moreover, we assess quantum computing's ability to break generally-used encryption standards, especially those prescribed today for IAEA instrumentation and communications. We studied every data security prescription as published by the IAEA to assess the overall and specific needs for the IAEA in a post-quantum era. We provide specific recommendations, namely that all symmetric encryption keys be at least doubled in length, and all asymmetric protocols currently used be upgraded to forthcoming quantum-resistant asymmetric protocols. We believe that an assessment needs to be done in the near-term by the IAEA regarding upgrades to currently deployed data encryption and communication schemes used by the IAEA, rather than delaying until practical quantum computers are realized, to protect both current data as well as future data.

1. INTRODUCTION

Digital data and information systems are essential elements of the International Atomic Energy Agency (IAEA) system of international safeguards. Without confidence in the integrity or authenticity of the data submitted by Member States about nuclear materials and facilities or the data collected by inspectors and remote monitoring systems, the process of implementing and verifying declarations (not to mention reporting anomalies) would be near impossible. It is not hyperbole to suggest that, absent reliable and secure IAEA information systems, the viability of the nuclear nonproliferation regime would be called into question. The IAEA is well aware of this dependency on digital information systems and the potential consequences of disruptions or breaches in the flow of digital data. It has developed sophisticated information security protocols for its headquarters and field operations to avoid or minimize the occurrence and effect of such disruptions or breaches, and threats to those systems are constantly evolving.

Improvements in quantum technologies of various forms could present the IAEA safeguards systems with new tools to collect data (e.g. from remote monitoring and inspections) and to ensure the integrity of deployed systems (e.g. with advanced seals). They could also pose severe challenges to the encryption capabilities upon which the agency relies to secure its data and information systems [1]. Not only could an advanced quantum computing capability compromise specific ongoing IAEA safeguards activities but it could lead to revelations about historical IAEA data and reporting that could affect the agency's ability to function technically and politically for years to come due to a loss of trust that the IAEA can adequately protect sensitive data.

Argonne National Laboratory's work was supported by the U.S. Department of Energy, National Nuclear Security Administration (NNSA), Office of International Nuclear Safeguards.

2. Quantum Technology Implications to IAEA Safeguards

Quantum computing poses severe threats to IAEA safeguards operations, primarily through the ability of adversaries to break current IAEA encryption standards. The IAEA handles sensitive, country-specific information which must be reliably available, authentic, and complete for the IAEA to make meaningful conclusions. Also, the IAEA is obliged to protect data coming from facilities in Member States with which it has signed a Comprehensive Safeguards Agreement (CSA). In both contexts, the information and data must be confidential in order to protect it from adversarial manipulation as well as maintain trust between the IAEA and Member States. While these requirements are provided by current, pre-quantum-era encryption schemes, a practical quantum computer (capable of utilizing Shor's or Grover's algorithms) could put this information and, hence, trust in the IAEA in jeopardy. Capable quantum hardware is the limiting factor, as useful quantum algorithms already exist in theory [2] [3].

More efficient and effective data processing via quantum technology could ultimately improve the international safeguards regime. With that said, there does not appear to be a near- to mid-term availability of such a quantum capability, and such systems are likely to be prohibitively expensive, meaning classical means to thwart quantum technologies may be a better first step when preparing for a quantum future.

Quantum cryptography, such as Quantum Key Distribution (QKD) could be of significant utility to the IAEA, but limiting factors exist that make near-term adoption of such standards unrealistic for implementation. We do not expect large-scale deployable systems in the immediate future due to limitations in speed, distance, cost, and robustness. The benefits and challenges of quantum key distribution schemes will be discussed later in Section 4.

Quantum sensing could be of utility for the IAEA and safeguards in the near- to mid-term. Significantly enhanced sensitivity of instruments could allow for measurements that otherwise would have too low signal-to-noise ratios (SNR). Also, new modalities of measurement might be possible, such as using quantum gravimetry to detect heavy metal in inaccessible locations. The overall field of quantum sensing is still nascent and only a handful of practical applications of quantum sensing have been identified by industry [5], [6]. Consideration of quantum sensing for safeguards is thus even less explored, although a separate study funded by NA-241 is considering use-cases of quantum sensing for IAEA safeguards [7].

Similarly, we do not believe the IAEA will have any need for quantum simulations. Such quantum simulations are for fundamental R&D efforts in physics, chemistry, and biology, which is beyond the projected scope of the IAEA, especially for safeguards (for now). The IAEA might leverage such fundamental R&D results, such as better nuclear cross sections, etc., but there is no near- to medium-term data likely.

2.1. Quantum technology and IAEA cryptography utilization

We assess the implications of quantum computing on IAEA cryptography standards to be the most relevant and pressing future concern for the IAEA. Therefore, we will spend an appreciable portion of this report describing the cryptography situation that will have potentially large effects on the IAEA and the international safeguards regime at large.

2.1.1. Current cryptographic systems used by the IAEA

According to prescribed IAEA data security requirements [8], which are consistent with other references on recommended data security services [9], applied cryptography schemes should provide the following three key elements: *confidentiality* to keep information secret from all but authorized parties; *integrity* to ensure messages/data are not modified in transit; and *authenticity* for verifying the origin/sender of a message.

The IAEA uses both symmetric and asymmetric cryptography protocols to accomplish the above data security services. Symmetric protocols utilize the same key to both encrypt and decrypt messages, while asymmetric protocols utilize a public key and a private key. Both have advantages and disadvantages. Symmetric schemes, such as the Advanced Encryption Standard (AES), operate significantly faster than asymmetric schemes and can utilize much smaller keys but are limited in capability. The primary issue facing purely symmetric protocols is efficient and secure key exchange. Since both parties must have access to the same key, both must be certain the key has been securely transmitted and both must be aware when it is compromised.

Asymmetric schemes, such as Rivest-Shamir-Adleman (RSA) and Elliptic-Curve Diffie-Hellman (ECDH), avoid the secure key exchange issue of symmetric protocols. The public key may be freely published on the network if the private key is kept secret. Rather than use the same key for encryption and decryption, as is the case for symmetric encryption, the sender may encrypt the message with the receiver's public key and be assured that only the intended recipient may be capable of decryption using their own private key. Note that both symmetric and asymmetric protocols require that the owner, or instrument, holding the secret key *must* protect that key from an adversary. For IAEA purposes, protection of secret keys is critical regardless of whether asymmetric or symmetric protocols are used.

Additionally, to prevent impersonation, modern schemes have the sender encrypt a hash (a unique and irreversible identifier derived from the message contents) with their own private key. The receiver may then decrypt the hash with the sender's public key, calculate the hash on the received message, and be certain that the message not only came from the declared sender but has also not been in any way changed in transit. In practice, to benefit from the strengths of both cryptographic schemes, asymmetric cryptography is typically used for secure transmission of a symmetric key which may be used for the remainder of the communication. Asymmetric encryption schemes are the backbone of Transport Layer Security (TLS), which is the secure transport protocol for web traffic over HTTPS services. Virtual Private Networks (VPNs) are also heavily reliant on asymmetric encryption to facilitate transmission over an untrusted network.

2.1.2. Effects of quantum computing on cryptographic systems used by the IAEA

When Shor's and Grover's algorithms are able to be executed on a quantum computer, almost all currently used encryption standards will be significantly weakened [1]. This includes the public-key infrastructure relied upon by the IAEA [8] to provide secure remote communication and even many symmetric schemes [1].

To understand how quantum computing may degrade existing standards, most analysts determine what will be needed in post-quantum security to achieve the same pre-quantum security that is currently employed. At-scale quantum computing power will affect the viability of symmetric and asymmetric protocols differently. While an AES 256-bit key or an RSA 15,000-bit key is necessary to provide 256 bits of security against a classical computer, an AES 512-bit key will be necessary to provide 256-bit security against a quantum computer, whereas RSA will be insecure, no matter the key length. In general, quantum computers may reduce the protection of most symmetric schemes by half; while asymmetric schemes will provide negligible protection against a quantum-enabled adversary.

The requirement for larger symmetric keys and the necessary infrastructure to enable symmetric schemes will affect the IAEA information infrastructure significantly. A quantum computer capable of Shor's algorithm will make most currently used VPN technology obsolete. VPN technology typically relies on a combination of public-key and private-key infrastructure. Many implementations of VPNs, including many relied upon by the IAEA, will become vulnerable, such as the use of pre-shared keys (though acceptable, not recommended by the IAEA) [1] [8] [9].

The IAEA's practice of having facilities report safeguards data via mailbox declarations is a particular concern. A mailbox declaration usually contains operational data – which cannot be retracted or altered once deposited – that is transmitted to a secure repository, akin to a postal drop box or mailbox [8]. The virtual mailbox may remain in-country and on-site or be located at IAEA headquarters in Vienna. The data in the mailbox declaration must be encrypted. Safeguards reporting via mailbox declarations therefore suffers a similar vulnerability as other remote communication methods: in a post-quantum world, digitally stored operational data transmitted via the internet will be insecure using current public-key options. Data could be intercepted and decrypted, or falsified reports could be forged by quantum-capable adversaries. Furthermore, due to the stagnant nature of a facility's mailbox declaration (i.e., the virtual repository wherein reported data is collected), if compromised, subsequent unauthorized access to future mailbox declarations and decryption of past declarations would likely follow causing further damage to the IAEA's mission. The IAEA also maintains public-key infrastructure to facilitate communication throughout IAEA headquarters [8]. Compromise of this system could result in all information transmitted through, or stored at, Vienna headquarters to be captured and decrypted.

One often-overlooked facet of the post-quantum world is that quantum computing power may also be used to decipher historical ciphertext previously lost, stolen, or otherwise intercepted. Unlike OTP encryption, current schemes do not offer forward security. Existing ciphertext may be deciphered at any time in the future when a practical quantum computer becomes available to an adversary who has access to stored ciphertext.

Indeed, all sensitive information encrypted using a post-quantum insecure standard is at risk of decryption, whether a powerful quantum computer exists at the time of transmission or not. And while sensitive information contained on lost or stolen devices may be accounted for and documented, the full amount and nature of information that has been or will be intercepted over communications networks is unknowable. This particular risk is one reason why priority should be given to adopting quantum-resistant standards well before practical quantum computers become available. If the sensitive information being protected with cryptography is not sensitive after a certain number of years, then the IAEA may not need worry about the exposure of such information. The IAEA should undertake an assessment of what data is truly sensitive and over what timescale is it important.

2.1.3. Threat Models and Discussion

Chapter 5 (Standards and Guidelines) of the IAEA's Information Security Requirements (ISR) publication [8], in particular Section 5.10 (Development), conveys requirements and steps for equipment security before use and in-field deployment. The requirements include defining a threat model and conducting a vulnerability assessment. The purpose of a threat model is to simulate threats to the system being developed, and a vulnerability assessment examines potential vulnerabilities due to such threats that may be present in the system or equipment. One of these threats is a brute force method to break encryption keys. The results of two brute force attack threat models applied to several encryption systems are discussed herein.

A. Analysis of threat models

Table 1 contains results of the number of calculations, n_i, required to break current wide-use 128-bit equivalent encryption as well as the corresponding 256-bit equivalent encryption schemes. Notably, we convey the agnosticism of the classical adversary to the symmetric and the asymmetric schemes by including the identical results and showing the differences with the quantum adversary.

Possibilities	128-bit equivalence [n_i]		256-bit equivalence [n_i]	
	AES – 128	**RSA - 3072**	**AES - 256**	**RSA - 15360**
Classical Adversary	$3.4x10^{38}(n_{128})$		$1.2x10^{77}(n_{256})$	
Quantum Adversary	$1.8x10^{19}$ $(n_{Grov128})$	$1.0x10^{11}$ $(n_{Shor128})$	$3.4x10^{38}$ $(n_{Grov256})$	$1.5x10^{13}$ $(n_{Shor256})$

Table 1. Maximum number of attempts required to break current encryption schemes.

The major conclusion we draw from our analysis is the significant loss of security for asymmetric keys (RSA) in a post-quantum era. Asymmetric keys against a quantum foe would exhibit a large vulnerability by requiring only microseconds (using Shor's algorithm) to factor the prime numbers of the asymmetric protocol's public key (which then also reveals the private key) up to 256 bits in length. Classically, asymmetric keys of sufficient length can be secure, but it is clear that asymmetric keys are at a significant disadvantage against quantum computers, regardless of key length. For symmetric cryptographic protocols like AES, breaking the secret key using Grover's algorithm is still difficult with a quantum computer, so long as the key is sufficiently long (i.e. 256 bits or more to satisfy IAEA's security mandates [22]). This demonstrates the potential strength of Shor's and Grover's algorithms with a quantum computer.

3. Possible Post-Quantum Paths Forward for IAEA Cryptography

While quantum computing threatens to put many current encryption standards at risk, multiple protocols exist or are being developed that will be resistant to both traditional attacks and the capabilities of quantum computers. Herein, we discuss strategies and tactics that could enhance security measures against a quantum-capable adversary. We advise continued discussions and engagements with the IAEA to best devise a strong cyber-defense posture in a post-quantum world.

3.1. Quantum Cryptography

As described earlier, quantum technology can provide encryption protocols resistant to infinite computing power using information-theoretic secure key exchange. QKD-+ leverages quantum sensitivity to measurement and the no-cloning theorem to enable secure symmetric key exchange. The original QKD protocol is the BB84 protocol [10], but there are now multiple QKD protocols, often derived from BB84, that also provide secure key exchange. Each approach has relative advantages and disadvantages that are appropriate for specific applications.

QKD offers great improvements in some areas and has been demonstrated in numerous applications, but it lacks the services provided by public-key encryption and remains expensive, slow, and difficult to implement. Other nearer-term solutions are needed to mitigate the threat posed by quantum computers.

3.2. New Post-Quantum Cryptography Algorithms

Interestingly, the future of cryptography in a post-quantum world may not need to be quantum-based like QKD. Scientists are engaged in research to identify problems that are difficult for both classical and quantum computers to break and that are easily adaptable for cryptographic purposes.

Bernstein & Lange [1] detail some of the leading solutions. Lattice schemes are considered some of the most promising solutions [11] and may even outperform traditional encryption standards [12] [13]. The U.S. National Institute of Standards and Technology (NIST), an approved standardizing body for IAEA systems

[8], is likely to declare a post-quantum cryptography standard in early 2022 [13]. Outside the United States, it is too soon to know which future post-quantum encryption protocols will become standard.

With the adoption of a fast, efficient, and lightweight post-quantum encryption standard potentially only a few years off, the threat of quantum-enabled decryption may be greatly reduced for all, including the IAEA. With a standard declared in the next few years, post-quantum cryptography will likely arrive faster than computers capable of performing Shor's or Grover's algorithm [13] [15]. Devices not able to be configured to provide post-quantum encrypted data should be assumed to be compromised once a powerful quantum computer exists. While it is difficult to predict when quantum computing capabilities will be available for this purpose, the process of transitioning to a new encryption standard may not be quick. *In other words, the work to upgrade current security requirements and update or replace communication infrastructure needs to begin in the near-term.*

3.3. Future Threat Model and Discussion

Following the same threat model methodology used in Section 2.1.3 applied to current, pre-quantum encryption protocols, the following defines a threat model and conducts a vulnerability assessment assuming post-quantum encryption protocols and again using the IAEA's own Information Security Requirements (ISR) publication, in particular Section 5.10 (Development) of that report [8].

A. Threat Model – Future Systems

Two future cryptographic methods are compared: a post-quantum, lattice-based key-encapsulation mechanism (Saber) and a generic quantum key distribution scheme coupled with a one-time pad (QKD+OTP).

As of July 2020, Saber is a finalist of NIST's Post-Quantum Standardization project [14]. Two variants of the asymmetric encryption protocol Saber (LightSaber and FireSaber) provide 125-bit and 283-bit security, respectively, against a classical adversary, and 113- and 257-bit security against a quantum-capable adversary. Both LightSaber and FireSaber have set key lengths, but they offer different security depending on the adversary. *Just as was included with the first threat model in Section 3.1.3, this threat model includes results for the different bit lengths* n_i *in* Table 2.

As mentioned, OTP encryption remains secure against any adversary, even if they were to have infinite computing power. As an OTP is, by definition, at least as long as the message, it would be infeasible to attempt every option with any conceivable computer. However, even if an adversary were to attempt every possible key successfully, no information would be gained. As each bit in the OTP is independent of the last, every possible message is just as likely as any other. It would be impossible to determine the correct message. If m were to be the message length, then, even after brute-forcing every option, each of the 2^m possible plaintext solutions would be just as likely as any other.

The benefit of QKD is not in that it enhances the protection of ciphertext, but rather that it protects the key itself as it is in transit. As Bennett & Brassard described, [10] the legitimate parties of a communications channel could leverage quantum phenomenon to be made aware of an eavesdropper attempting to capture the OTP before its use. Man-in-the-middle attacks, a significant risk to symmetric-key encryption, could thus be avoided. QKD with an OTP is thus likely secure against a classical and quantum adversary and suffers from less of the attack vectors than currently used symmetric encryption protocols.

B. Results and Discussion

Possibilities	**LightSaber [n_i]** **125-bit** **113-bit**	**FireSaber [n_i]** **283-bit** **257-bit**	**QKD+OTP**
Classical Adversary	$4.3x10^{37}(n_{LS\text{-}125})$	$1.6x10^{85}(n_{FS\text{-}283})$	Information-Theoretic Secure
Quantum Adversary	$1.0x10^{34}(n_{LS\text{-}113})$	$1.2x10^{77}(n_{FS\text{-}283})$	

Table 2. Maximum number of attempts required to break quantum-resistant encryption protocols (under development).

Table 2 contains the results of the calculations presented in this section. The second threat model provides different conclusions than the first (see Table 1). It is understood that a QKD+OTP system can be considered information-theoretic secure, even in the scenario of an adversary with a quantum computer. Due to OTP implementations, there is not a standard key length as the key is, by definition, at least as long as the message. The system would be information-theoretic secure regardless. The next conclusion is that lattice-based asymmetric encryption schemes, such as Saber, can be secure against both a classical computer and a quantum computer. Adopting lattice-based asymmetric encryption standard, or another quantum-resistant standard, will be a more feasible approach than QKD+OTP for the IAEA in terms of resources, although as stated above the IAEA should still monitor progress in QKD developments. Therefore, we assess that if the IAEA must update or replace currently used asymmetric encryption schemes, it may be of benefit to adopt post-quantum asymmetric protocols rather than relying on increasing the bit lengths of symmetric encryption schemes alone.

4. Recommendations

As a result of the analysis conducted in this study, we have developed a series of recommendations for the IAEA to consider as it looks to meet evolving information security requirements in light of ongoing developments in quantum computing. The following recommendations are categorized by technical area. Each area also lists the individual IAEA requirements (taken from the IAEA's own documents [8] [9]) that relate directly to it.

Quantum Key Distribution

QKD provides many potentially promising advancements in cryptography, but the cost, implementation, and existing technology will likely make the technique prohibitive in the near term [4]. While we do not recommend adoption of such schemes in the near-term, we do recommend that the IAEA consider future uses of QKD and its applications, such as tamper-indicating seals.

Symmetric Cryptography (2013 Requirements 5.2 R19 C14 and C15 [8]; 2018 R24, R51, R52 [9])

Symmetric protocols benefit from inherent quantum resistance (for sufficient key length), existing wide-scale implementation, and widespread supporting infrastructure [1]. While most symmetric schemes must double key length in order to retain current security complexity against quantum computers, many devices will be capable of this [1]. The implementation of larger symmetric key lengths, and the upgrade of instruments that cannot currently work with longer key lengths, are important near-term objectives, as the transition to longer-length symmetric keys may protect current data against future quantum computing capabilities. Additionally, with the use of Message Authentication Codes (MACs), symmetric keys can create digital signatures, that, if the key has been appropriately shared and secured, is similar to public-key digital signatures [8].

Asymmetric Cryptography (2013 Requirements 5.2 R11, 5.2 R13, 5.2 R19 and C16 [8], 5.2 R30; 2018 R17, R19, R20, R22, R24, R51, R52 [9])

Current asymmetric protocols will be compromised by quantum computing capabilities [1] and must be replaced, as was highlighted multiple times above. Post-quantum asymmetric protocols being evaluated

currently (e.g. Saber) appear to be the most promising, as these schemes can fully replace current asymmetric schemes in terms of functionality without requiring a dramatic increase in processing power and no new network infrastructure [1]. Additionally, 15 standards are currently being considered by the U.S. National Institute of Standards and Technology (NIST), which entails community review of the protocols by premier experts in cryptography [14]. A standard is expected within the next two to four years, which precedes our best estimates for availability of a quantum computer capable of breaking current encryption schemes [13]. We believe post-quantum asymmetric cryptography protocols are the best solution to the threat of quantum computers and encourage implementation of a NIST-type standard in technology where possible.

VPN (2013 Requirements 5.1 R6 [8], 5.1 R7, 5.1 R9, 5.2 R17 C7 [9])

Much of the IAEA's current VPN technology requires replacement or significant updates and could realize great benefit from the adoption of post-quantum cryptography. As discussed previously, symmetric key lengths must be doubled to provide the same level of security [1]. This requirement may be difficult for some devices, such as devices already operating at their maximum key length, to employ post-quantum symmetric keys. To avoid the challenges of symmetric key security for most devices, post-quantum encryption standards should be employed in VPN technology. These standards may be used in conjunction with symmetric key schemes for increased speed, as is done currently.

Web Server (2018 R25, R31, R50 [9])

The web servers that the IAEA uses to access information or that serve as the public face of the IAEA also require post-quantum security. Transport Layer Security (TLS), the backbone of the secure web traffic protocol HTTPS, is not quantum-resistant [1]. Certificate Authorities (CAs) are working on quantum-resistant versions using post-quantum standards, and the adoption of such tools will be necessary for sensitive sites [16]. Other IAEA web traffic, such as mailbox declarations, remote data transmissions, other email traffic, file transfer protocols, and others may require a post-quantum secure version. The agency should ensure that security providers offering post-quantum resistant services are utilized.

Headquarters Public-Key Infrastructure (2013 Requirements 5.2 R20, 5.2 R23 [8])

The asymmetric public-key infrastructure at IAEA headquarters is not quantum-resistant and will need to be updated to post-quantum standards. The sensitive information that comes into, circulates within, and/or leaves headquarters is an attractive target for adversaries, and infiltration poses threats to the confidentiality of information. Additionally, a quantum-enabled adversary could forge or intercept safeguards data.

The public-key infrastructure currently in use at headquarters must be entirely replaced by a quantum-resistant standard. Additionally, it may be prudent to adopt the use of symmetric keys to provide better forward security for the most sensitive of communications within headquarters.

Secure Storage (2013 Requirements 5.2 R15, 5.2 R16 and C5, 5.2 R18, 5.2 R21 [8])

What constitutes secure data storage and appropriate technical safeguards against theft or disruption is subject to change with the availability of quantum computers. Encryption on storage devices previously considered secure may not be quantum resistant. The IAEA should review appropriate encryption standards for different sensitivities of information to adjust requirements; the acceptable standards for legacy, current, and future use should also be adjusted. Future devices, such as hardware security modules (HSMs), VPN boxes, and other devices performing encryption at the hardware level should be capable of performing post-quantum standards.

Threat Models (2013 Requirements 5.2 R40, 5.2 R41 [8])

The IAEA should consider quantum security, and quantum-capable adversaries, in threat models and vulnerability assessments. This will require additional training and the creation of IAEA-specific analytical approaches. Current threat models do not account for a quantum-capable adversary, and therefore do not adjust for the weaknesses in current encryption protocols. In the near-term, such a threat analysis will likely

require persons with some expertise in quantum mechanics, as well as cryptography. No current best practice is available to allow the agency to craft a quantum-based threat analysis.

Previously Disclosed Ciphertext

The decryption of previously transmitted ciphertext using quantum computing systems will present a potentially large threat to the IAEA and other stakeholders, including Member States. While appropriate adoption and implementation of post-quantum and enhanced symmetric schemes may mitigate the threat of quantum computers to current information, the loss of past ciphertext is unavoidable. Current, and past, encryption schemes do not provide forward security. Information encrypted using current asymmetric public-key protocols may be decrypted at any time, such as when a much more powerful computer becomes available, assuming this encrypted information has been intercepted and stored by an adversary. While some symmetrically encrypted information may be difficult to break, symmetric keys are often agreed upon through the use of public-key encryption [1].

Facility design and layout, security procedures and techniques, and typical operations and capabilities are all sensitive, and may already be in adversaries' hands waiting to be decrypted. As the risk of ciphertext disclosure grows, a reevaluation of appropriate security techniques is warranted to better protect even encrypted messages. This risk is also the primary driver behind our recommendation of using enhanced symmetric key communication for the most sensitive systems as these schemes will remain secure against a quantum adversary [1]. We strongly recommend that the IAEA attempt to account for potentially disclosed information in order to mitigate the risk of future decryption and to reassess the security of communications with respect to forward security.

5. Conclusion

Advances in quantum computing could undermine the IAEA's ability to function effectively and efficiently due to their ability to break current encryption standards, and we believe that post-quantum cryptography standards present the most realistic countermeasure for the agency to adopt. Without adopting an improved standard, the IAEA risks being unable to make meaningful conclusions from collected data, as well as losing the trust of states that disclose sensitive information to the IAEA.

Considering the time needed for new implementation, and the uncertainty of the first quantum computer capable of Shor's or Grover's algorithm, the issue is too pressing to ignore. Preparations should begin now in order to implement a NIST-like standard soon after its announcement. All devices reliant on insecure encryption standards, meaning all devices using current public-key encryption and all devices using an inadequate symmetric key, should be identified. This list will include VPN technology, the public-key infrastructure at IAEA headquarters, and likely stored data. A plan for phasing out devices incapable of adopting a new standard should be created. New technology purchases should ensure that new equipment is capable of transitioning to a post-quantum standard unless the device handles insignificant data or has a very short lifespan. Installing new technologies in State facilities presents a substantial challenge in not only travel costs for IAEA instrumentation experts but also Member State approval of such new technologies. As such, phasing out devices should be looked at immediately and done over time in order to lessen the burden of such an endeavor.

Upon the creation of a practical quantum computer, all information utilizing current public-key standards should be assumed to be disclosed. Devices not transitioned by this time should operate in a pre-shared symmetric key mode, with the keys lengths at least doubled. Symmetric key encryption with less than a 256-bit key should be considered insecure and should only exist in legacy devices. This applies to data in transit as well as at rest. Ideally, all information in transit should utilize a post-quantum public-key cryptography standard to establish a secure connection. This will affect currently used VPN technology and safeguards data caches (e.g., virtual mailboxes for declarations), among other systems.

Quantum technology promises great advancements in processing power, data processing, sensing, and communications. However, the timeline for the public availability of quantum technology is prone to changes and delays. Despite this uncertainty, the IAEA should prioritize implementing post-quantum cryptographic systems before quantum computers capable of Shor's or Grover's algorithm are operable. Doing so will help the IAEA maintain the confidentiality, integrity, and authenticity of safeguards data and systems in the near future and prepare for the quantum-capable adversaries of tomorrow.

6. References

[1] D. L. T. Bernstein, "Post-quantum cryptography," *Nature,* vol. 549, p. 188–194, 2017.

[2] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, Santa Fe, 1994.

[3] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *28th Annual ACM Symposium on Theory of Computing*, Philadelphia, 1996.

[4] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum Cryptography.," *Reviews of Modern Physics,* vol. 74, p. 145–195, 2002.

[5] T. Bowler, "How quantum sensing is changing the way we see the world," *BBC News,* 8 March 2019.

[6] D. Kim, M. I. Ibrahim, C. Foy, M. E. Trusheim, R. Han and D. R. Englund, "A CMOS-integrated quantum sensor based on nitrogen–vacancy centres," *Nature Electronics,* vol. 2, pp. 284-289, 2019.

[7] D. Farley, "Quantum Sensing and its Potential for Nuclear Safeguards," Sandia National Laboratories, 2020, draft.

[8] IAEA, "Information Security Requirements for the Development of IAEA Safeguards Equipment," IAEA, 2013.

[9] IAEA, "Remote Monitoring Requirements for the Development of IAEA Safeguards Equipment.," IAEA, 2018.

[10] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing.," *Theoretical Computer Science,* vol. 560, p. 7–11, 2014.

[11] H. Nejatollahi, N. Dutt and R. Cammarota, "Special session: trends, challenges and needs for lattice-based cryptography implementations," in *International Conference on Hardware/Software Codesign and System Synthesis*, New York, 2017.

[12] S. Fan, W. Liu, J. Howe, A. Khalid and M. O'Neill, "Lightweight Hardware Implementation of R-LWE Lattice-Based Cryptography," in *IEEE Asia Pacific Conference on Circuits and Systems*, Chengdu, 2018.

[13] "NIST's Post-Quantum Cryptography Program Enters 'Selection Round'," NIST, 2020. [Online]. Available: https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round. [Accessed August 2020].

[14] M. Dustin and e. al., "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process," NIST, 2020.

[15] T. Fernández-Caramès and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," *IEEE Access,* vol. 8, pp. 21091-21116, 2020.

[16] Sectigo, "The Search for Quantum-Resistant Cryptography," 2019. [Online]. Available: https://sectigo.com/resource-library/the-search-for-quantum-resistant-cryptography-understanding-the-future-landscape. [Accessed August 2020].