



LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers

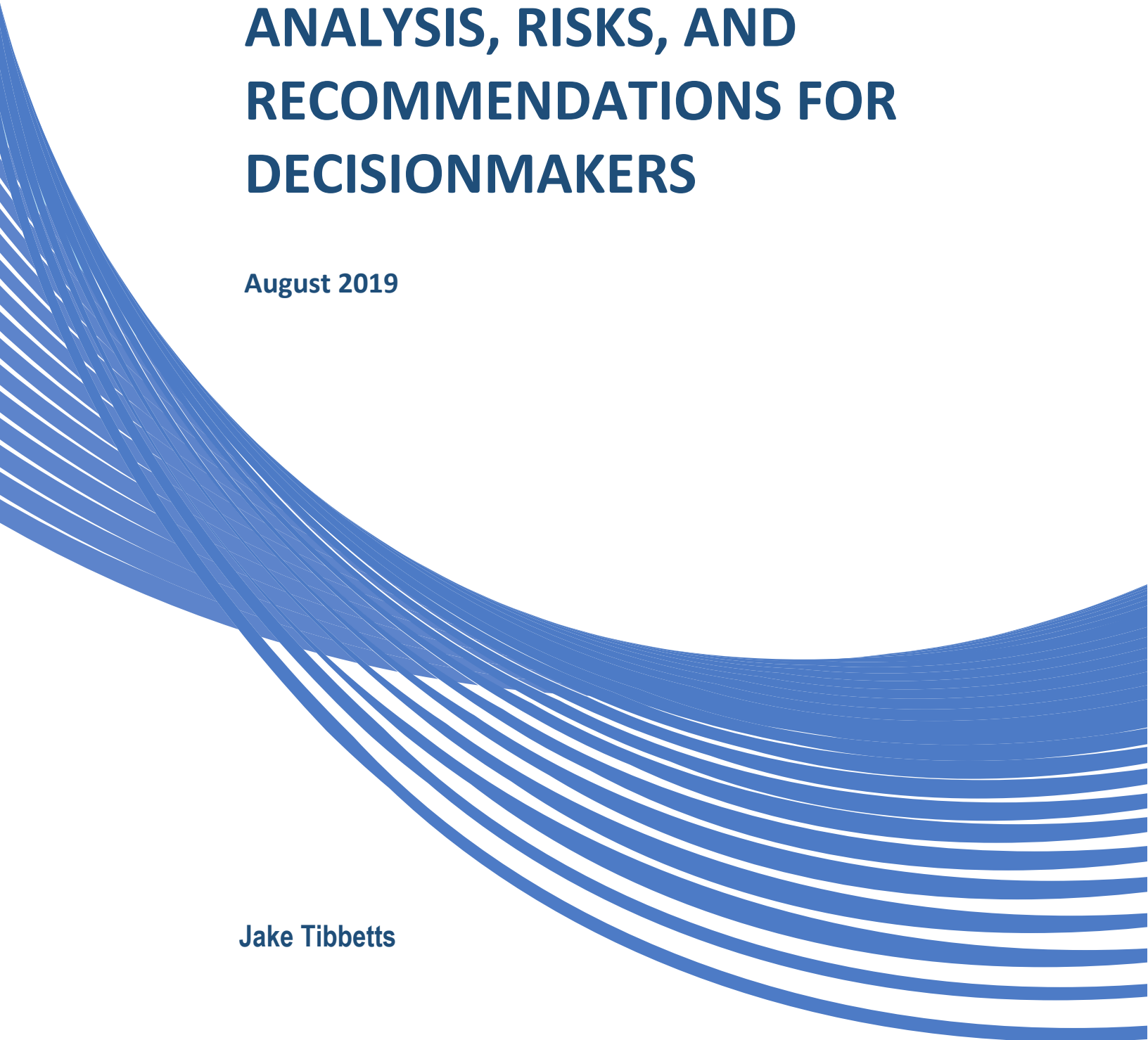
J. Tibbetts

September 20, 2019

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.



QUANTUM COMPUTING AND CRYPTOGRAPHY: ANALYSIS, RISKS, AND RECOMMENDATIONS FOR DECISIONMAKERS

August 2019

Jake Tibbetts

Center for Global Security Research
LAWRENCE LIVERMORE NATIONAL LABORATORY

Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers

Jake Tibbetts¹

UC Berkeley

Introduction

Some influential American policymakers, scholars, and analysts are extremely concerned with the effects that quantum computing will have on national security. Similar to the way space technology was viewed in the context of the US-Soviet rivalry in the Cold War, they view scientific advancement in quantum computing as a race with significant national security consequences and a part of the emerging US-China rivalry. It is claimed that the winner of this race will be able to thwart all the cryptographic efforts of the loser and gain unfettered access to any state secret of the losing government. Additionally, it is suggested that the winner will be able to protect their secrets with a higher level of security than contemporary cryptography guarantees at the moment. This paper argues that these three claims are considerably overstated, and that policymakers and scholars should shift focus to a different national security problem that quantum computing will create. Maintaining the long-term security of secret information secured by contemporary cryptographic protections, which will fail against an attack by a future quantum computer, is the predominant challenge needing attention.

This paper takes a technically-informed approach to this issue. It first lays out the national security problems that are envisioned in much of the current discourse surrounding quantum computing. Then, it will assess the technical advantages that quantum computers will have over classical computers in the field of cryptography. Next, it will provide an explanation of the specific ways that the technical realities of quantum computing are inconsistent with the predominant areas of concern. Following, it will highlight the more pressing national security problem posed by quantum computing that the public discussion has, for the most part, missed. The piece will conclude with recommendations for how to mitigate this issue.

Areas of Predominant Concern

Some of the current policy discourse around quantum computing is centered around three related themes:

1. The race for quantum supremacy between the US and China.
2. Failure of cryptographic schemes due to quantum computing.
3. Increased security through quantum computing enabled encryption schemes.

More broadly, many assert that the US is in a race against China for supremacy in quantum computing and that this race has significant national security implications. These views are derived from the scientific community's assessment that quantum computing will provide an

¹ *The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes*

advantage in deciphering an adversary's encrypted messages² and that quantum computing will allow for the sending of messages using quantum encryption schemes that provide an improved level of security compared to current encryption schemes.³ Moreover, they are concerned that the country that achieves proficiency in quantum computing first will gain these advantages over its adversary.

Theme 1: The Race for Quantum Supremacy

Quantum supremacy is an artificial benchmark set by those in the scientific community that marks the moment that a quantum computer computes an answer to a well-defined problem more efficiently than a classical computer.⁴ While it is largely meant as a scientific goal, many writers and analysts have co-opted the term and set it as a goal that the US should rapidly advance towards and achieve first. In fact, they draw links between achieving quantum supremacy and the historical competition for supremacy in space and missile technology between the US and the Soviet Union. For example, the Washington Post has called quantum computing "The Most Important Tech Contest Since the Space Race"⁵ and the Council on Foreign Relations has called it "The Quantum Race the US Can't Afford to Lose".⁶ Also, similar to the technological competition for missile technology with the Soviet Union and the widely-shared assessment in the 1950s and 1960s that the United States was playing catch-up⁷, some say today that "Chinese scientists are at the forefront"⁸ of this technological race, there exists a "quantum gap"⁹ between the US and China, and the US is at a disadvantage.

These analyses have had real policy implications. Some in the US policy community such as John Costello¹⁰ very seriously fear that if China achieves quantum supremacy first, it will have a direct negative impact on the national security of the US. Costello's reporting suggests that China would gain a significant strategic advantage by "frustrating US cyber espionage and signals intelligence capabilities" and "placing sensitive [US] information systems at risk" if China achieves quantum supremacy.¹¹ Moreover, Congressman Will Hurd¹² (R-TX) has called quantum computing "the next big security risk".¹³

These views are shared by key figures in both the Republican and Democratic parties. In 2018, the White House released a policy memo that outlined the administration's research and

² Majot A. and Yampolskiy R. (2015, September). Global Catastrophic Risk and Security Implications of Quantum Computers.

³ Biercuk V. and Fontaine R. (2017, November 17). The Leap Into Quantum Technology: A Primer For National Security Professionals.

⁴ Harrow A. and Montaro A. (2018). Quantum Computational Supremacy.

⁵ Nikias C. (2018, May 11). This is the Most Important Tech Contest Since the Space Race, and America is Losing.

⁶ Ashbaugh L. (2018, April 18). The Quantum Race the United States Can't Afford to Lose.

⁷ Kaplan F. (1983). Wizards of Armageddon.

⁸ Whalen J. (2019). The Quantum Revolution is Coming, and Chinese Scientists are at the Forefront.

⁹ Ricks T. (2017, November 28). The Quantum Gap with China.

¹⁰ John Costello has served in various positions in the US government including positions at DHS, NSA, USCYBERCOM, and CISA.

¹¹ Kania E. and Costello J. Quantum Hegemony? (2018, September 12). China's Ambitions and the Challenge to U.S. Innovation Leadership.

¹² Congressman Will Hurd is known to be a valuable technically literate member of congress and is considered an authority on many issues relating to computing technology. Congressman Hurd holds a computer science degree from Texas A&M, served in the CIA for a decade, was a senior advisor to a cybersecurity firm prior to joining congress, and was formerly the chairman of the House Oversight and Government Reform Subcommittee on IT.

¹³ Hurd W. (2017, December 7). Quantum Computing is the Next Big Security Risk.

development priorities which listed quantum computing as a key area in “[maintaining] US leadership in strategic computing”.¹⁴ Moreover, President Trump signed the National Quantum Initiative Act¹⁵ and released the National Strategic Overview for Quantum Information Science¹⁶ as parts of an effort to accelerate US scientific advancement in quantum computing. Also in 2018, Senator Kamala Harris (D-CA) proposed the Quantum Computing Research Act which was meant to “establish a Department of Defense Quantum Computing Research Consortium to spur development of a competitive edge for America in quantum computing”.¹⁷ Senator Harris also tweeted in support of her proposed legislation “Quantum computing is the next technological frontier that will change the world and we cannot afford to fall behind”.¹⁸

The policy community supports the ideas that the race for quantum supremacy is on, the US is losing, and it is of critical national and strategic importance that the American scientific community rapidly advances towards technological superiority just as the US did in the Space Race.

Theme 2: Quantum Computing Makes Current Encryption Obsolete

Some analysts and scholars who have reviewed technical literature have found that quantum computers will be able to run algorithms that allow for the decryption of encrypted messages without access to a decryption key. According to them, these quantum algorithms will make “current cryptographic methods trivial to break”.¹⁹ When these algorithms can be broken, it exposes the victims to significant strategic and security risks,²⁰ and would allow the US’s adversaries to read military communications, diplomatic cables, and other sensitive information. This situation has been compared to the way that Great Britain and the US broke the German Enigma code and Japanese Purple code in World War II which gave the Allies a significant strategic advantage over the Axis Powers.²¹

Some of the policy discussion around this issue is influenced by suggestions that the US could itself become the victim of a *fait accompli* in code breaking after quantum supremacy is achieved by an adversary. For example, the Executive Director of the Quantum Industry Coalition, Paul Stimers,²² specifically calls out that the ability to “break encryption” is a “game-changing military application”.²³ Some point out that this is one of the major strategic risks that the US could be exposed to should it lose the race for quantum supremacy against China.

¹⁴ Mulvaney M. and Kratsios M. (2018, July 31). Memorandum for the Heads of Executive Departments and Agencies – FY 2020 Administration Research and Development Budget Priorities.

¹⁵ H.R. 6227 – National Quantum Initiative Act. (2018, December 21).

¹⁶ National Strategic Overview for Quantum Information Science. (2018, September).

¹⁷ Harris Introduced Bill to Increase Resources for Quantum Computing and Research to Benefit National Security. (2018, June 07).

¹⁸ Ibid.

¹⁹ Ashbaugh L. (2018, April 18). The Quantum Race the United States Can’t Afford to Lose.

²⁰ Majot A. and Yampolskiy R. (2015, September). Global Catastrophic Risk and Security Implications of Quantum Computers.

²¹ Ricks T. (2017, November 28). The Quantum Gap with China.

²² Paul Stimers is a veteran lobbyist in Washington DC representing emerging technology companies and is the founder and executive director the the Quantum Industry Coalition, a lobbying group for the emerging quantum technologies industry.

²³ Stimers P. (2019, May 5). Insights and Intelligence Episode 37: A Quantum Leap Forward.

Theme 3: Quantum Computing Makes New Encryption More Secure Than Current Encryption

The analysts and scholars who have reviewed the technical literature have also found that quantum computers will be able to use cryptographic schemes that do not rely on mathematical assumptions. This new concept of “quantum communications ... seeks to enable new cryptographic protocols, using the rules of quantum physics to guarantee security”.²⁴ Statements such as these imply that the security guarantees of quantum physics are significantly greater than the security guarantees of mathematical assumptions. This has led to the notion in the policy community that quantum communications is significantly more secure than classical cryptography.

The view that quantum communications will provide a significantly higher level of security than encryption based off of classical computing has been presented before the US Congress. Congressional testimony by Dr. James F. Kurose²⁵ in the House Committee on Science, Space, and Technology has even suggested that quantum communications “offers the promise of ... absolutely secure communication”.²⁶

Technical Aspects of Quantum Computing

Quantum computing will have a real, substantial impact on the technical field of cryptography. However, the exact technical impacts on cryptography have yet to be explained in the context of national security implications. While policymakers and scholars have made an effort to understand the technology, the technical nuances that are difficult even for technical practitioners to understand, are often missed. These omissions have, unfortunately, led to overstated or erroneous claims about the implications of quantum computing on national security.

Cryptography Before Quantum Computing

The field of cryptography is a subfield of mathematics that investigates methods by which the properties of confidentiality, integrity, and non-repudiation can be mathematically guaranteed.²⁷ *Confidentiality* is the property that when a ciphertext, the encrypted message, is sent across an insecure channel, no information about the corresponding plaintext, the unencrypted message, can be learned from ciphertext. *Integrity* is the property that messages sent across an insecure channel are not modified in transit. *Non-repudiation* is the property that a malicious individual cannot send a message that appears to be sent from another individual - the sender of a message cannot repudiate that they sent that message.

²⁴ Biercuk V. and Fontaine R. (2017, November 17). The Leap Into Quantum Technology: A Primer For National Security Professionals.

²⁵ Dr. James F. Kurose is currently a professor of computer science at UMass Amherst, holds a PhD in Computer Science from Columbia University, and formerly served as the Assistant Director of the National Science Foundation for Computer and Information Science and Engineering. He gave this testimony in his capacity as an assistant director at the NSF.

²⁶ Testimony of James F. Kurose before the Subcommittee on Research and Technology and the Subcommittee on Energy on American Leadership in Quantum Technology. (2017, October 24).

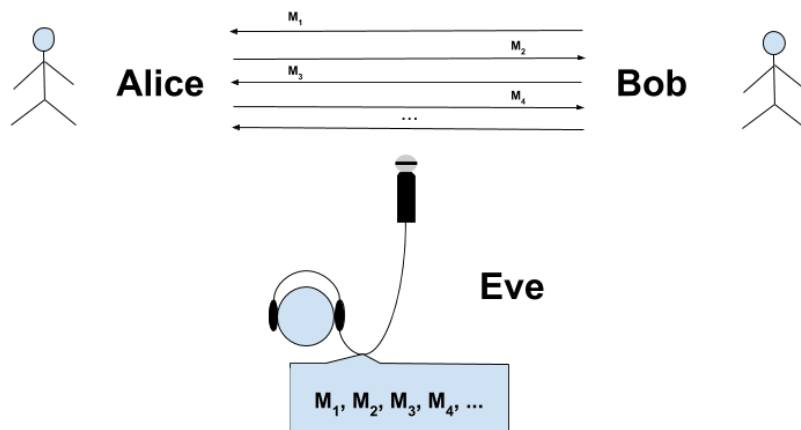
²⁷ Katz J. and Lindell Y. (2015). Introduction to Modern Cryptography.

Confidentiality, integrity, and non-repudiation are all properties that are interesting because they have direct analogs to real world applications. For example, simply sending a message on any messaging platform relies on the fact that cryptography guarantees all three of these properties. As for its relation to national security in the US, the National Institute of Standards and Technology (NIST)²⁸ and the National Security Agency (NSA)²⁹ both provide requirements and recommendations for cryptographic protocols that underpin the security of critical operations involving financial transactions, health care information, military communications, and the storage of state secrets.

Of these three properties, the property that is most important for national security is confidentiality. This is because confidentiality is the only exclusively long-term goal of the three properties that the field of cryptography concerns itself with. Confidentiality requires that an attacker, for example an enemy state, who intercepts a ciphertext cannot, even with a large amount of resources and an extremely long period of time, learn anything about the corresponding plaintext.³⁰ While integrity and non-repudiation are important for other reasons, this paper will only focus on the confidentiality property of cryptography.

Encryption Schemes

Confidentiality is guaranteed by encryption schemes. Encryption schemes are protocols that two communicating parties can use to send information to each other across an insecure channel that guarantee the confidentiality of messages sent across the channel.³¹ Encryption schemes are often explained through a game and a cast of characters: Alice, Bob, and Eve. The game is setup such that Alice and Bob are attempting to send messages to each other confidentially and Eve is an eavesdropper who intercepts the messages sent across the channel. If Eve can learn anything about the secret message being sent across the channel, Eve wins and the encryption scheme is not secure. Otherwise, Alice and Bob win and the encryption scheme is secure.³²



²⁸ Barker E. (2016, August). Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms.

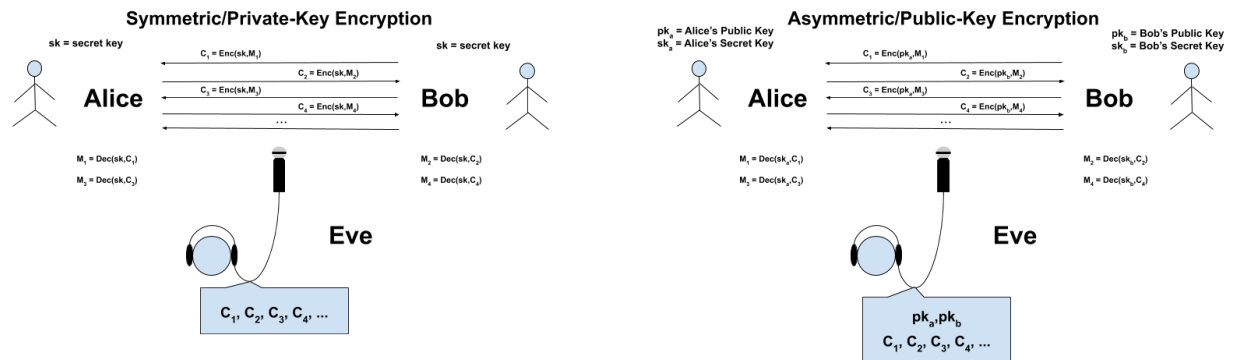
²⁹ Commercial National Security Algorithm Suite. (2015, August 19).

³⁰ Katz J. and Lindell Y. (2015). Introduction to Modern Cryptography.

³¹ Katz J. and Lindell Y. (2015). Introduction to Modern Cryptography.

³² Katz J. and Lindell Y. (2015). Introduction to Modern Cryptography.

There are two types of encryption schemes: symmetric and asymmetric.³³ For symmetric encryption, Alice and Bob share a secret, prior agreed-upon, private key that is used to both encrypt and decrypt the messages. For asymmetric encryption, Alice and Bob do not share a secret, prior agreed-upon, secret key and must instead encrypt messages using Alice's and Bob's published, public keys and decrypt received messages with their respective private keys. Symmetric encryption and asymmetric encryption are also known as private-key encryption and public-key encryption respectively.



How Do We Guarantee that an Encryption Scheme Provides Confidentiality?

This question lies at the heart of cryptography. It essentially boils down to the idea that there are some problems that are *hard* to solve and breaking the confidentiality of an encryption scheme - learning something about plaintext - is as difficult as solving a *hard* problem. This leads to the question of how the idea of *hardness* can be captured mathematically. This is the focus of a different, related subfield of mathematics called complexity theory.³⁴

Complexity theory is the study of the difficulty of solving problems. This is a confusing notion at first, but it can be understood through the analogy of counting marbles. Let's say that you have a large bag of marbles. Each marble is one of two colors: red or blue. The bag is exactly 50% red marbles and 50% blue marbles. Suppose that you are given two different problems. The first problem is to pick a red marble. The second problem is to give an exact count of all the marbles in the bag. To solve the first problem, all you have to do is look in the bag, find a red marble, and pick it. It would only take a second. To solve the second problem, you have to count all the marbles in the bag one by one. Depending on the size of the bag, it could take a few seconds or minutes. We would say the second problem is *harder* than the first because the problem requires more work.

Now let's say that you were given a much larger bag and asked to solve the same two problems. You could solve the first problem the same way. It would only take a second as before. Once again, to solve the second problem, you have to count all the marbles in the bag one by one. But now because the bag is larger, the second problem takes a lot more time to solve than it did with the first bag. In short, it only takes about a second to solve the first problem regardless of the size of the bag, whereas the time it takes to solve the second

³³ Katz J. and Lindell Y. (2015). Introduction to Modern Cryptography.

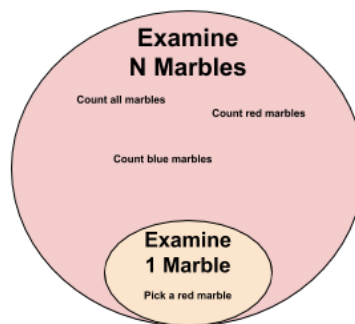
³⁴ Dasgupta S., Papadimitriou C., and Vazirani U. (2006, July 18). Algorithms.

problem is correlated with the size of the bag. Intuitively, the first problem and the second problem are in different classes of problems. We call these complexity classes.

Now let's say that you are given a third problem and a third bag. The third problem is to count only the red marbles. Remember that the bag is 50% red and 50% blue. One way to solve the problem is to solve the second problem, count all the marbles, and divide by two. Also, you could solve the counting all marbles problem by counting only the red marbles and multiplying by two. Additionally, you could use this technique with the blue marbles too. In short, by solving just one of these tasks, you can now solve all the other related problems as well. Because of this, your second problem, counting marbles, is in the same complexity class as the third problem, counting red marbles. If you solve one problem in a complexity class, you have actually solved all of the problems in that class.

Intuitively, all the problems in a lower, examine-one-marble complexity class are also in the examine-n-marbles complexity class. This is because one could always choose to count more marbles and come to the correct answer inefficiently.

Marble Complexity Classes



Going back to quantifying *hardness* as it relates to the confidentiality and encryption schemes, a problem is considered *hard* if it cannot be solved by a computer *efficiently*. *Efficiency* and *hardness* are related terms in complexity theory. A problem cannot be solved *efficiently* if the size of the problem increases exponentially with the size of the input.³⁵ This means that if the size of the problem is n and it takes 2^n computer operations to solve the problem, and then the size of the problem increased by 1 to $n+1$, the number of computer operations needed to solve the new problem is now 2^{n+1} . This is $2 \cdot 2^n$, which is twice the operations of the previous problem.

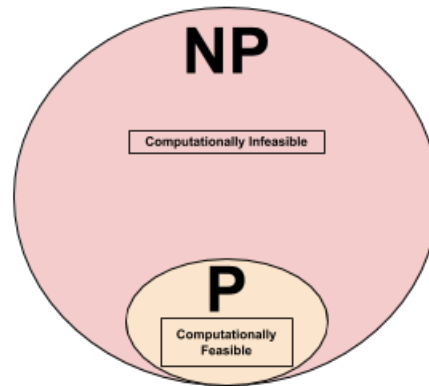
Problems that can be solved efficiently, meaning the size of the problem does not increase exponentially, by a computer are in the complexity class called P, which is the class of problems that are *not hard*.³⁶ Problems that cannot be solved efficiently by a computer are in the complexity class called NP which is the class of problems that are *hard*. Intuitively, all problems in P are also in NP³⁷ because a computer can be programmed to do an exponential number of useless operations to solve a problem in P. Even for medium sized problems, a problem in the class NP, that is not in P, cannot be solved by a computer in an acceptable amount of time.

³⁵ Dasgupta, Papadimitriou, and Vazirani, Algorithms

³⁶ Dasgupta, Papadimitriou, and Vazirani, Algorithms

³⁷ Dasgupta, Papadimitriou, and Vazirani, Algorithms

Complexity Classes



Therefore, to guarantee the confidentiality of an encryption scheme one needs to choose a problem in NP that is not in P, and construct the scheme in a way such that the problem of violating confidentiality - learning something about the plaintext from the ciphertext - is as difficult as solving a problem in NP.³⁸ In fact, the problem of violating the confidentiality of an encryption scheme is in the same complexity class, NP, as the underlying problem. By reducing the problem of violating the confidentiality of an encryption scheme to solving a problem in NP, the problem of violating the confidentiality of an encryption scheme cannot be solved by a computer in a reasonable timeframe.

The assumption that there exists separate complexity classes P and NP, and that cryptography relies on the hardness of problems in NP, was essentially how cryptography experts thought about cryptography before quantum computing was a concept.

Asymmetric Encryption

There are two popular asymmetric encryption schemes today that are recommended by NIST and the NSA.^{39 40} They are RSA, named after its creators Rivest, Shamir, and Adleman, and ECDH, Elliptical Curve Diffie-Hellman. Breaking the confidentiality of RSA and ECDH are as difficult as the problems of factoring a number and solving the discrete logarithm problem.⁴¹ Also, the factoring and discrete log problems are both as difficult as another related problem called order finding. It is not important what these problems actually are. What is important to recognize is that the five problems of violating the confidentiality of RSA, violating the confidentiality of ECDH, factoring a number, discrete log, and order finding, are all in the same complexity class NP and therefore are all essentially the same problem.

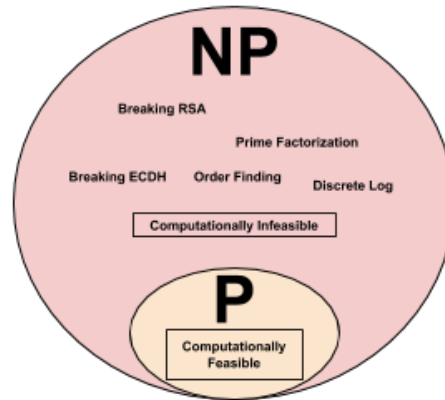
³⁸ Katz J. and Lindell Y. (2015). Introduction to Modern Cryptography.

³⁹ Barker E. (2016, August). Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms.

⁴⁰ Commercial National Security Algorithm Suite. (2015, August 19).

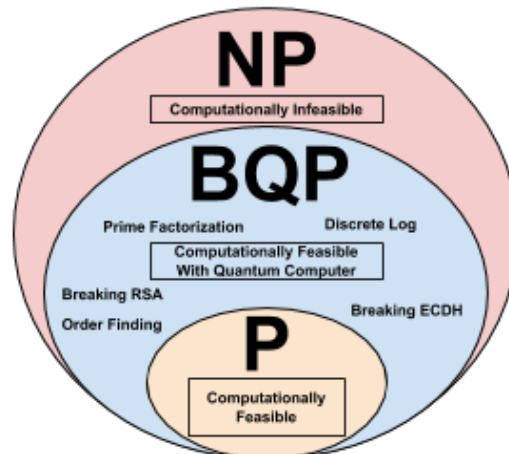
⁴¹ Katz J. and Lindell Y. (2015). Introduction to Modern Cryptography.

Complexity Classes



In 1995, Peter Shor presented an algorithm that can be executed by a quantum computer that efficiently solves the problem of factoring a number.⁴² This is now known as Shor's algorithm. Through this algorithm, Shor proved that the problem of factorization is also in a complexity class called BQP,⁴³ the set of problems that can be solved efficiently by a quantum computer. Because the aforementioned five problems are related, it turns out that all these problems can be efficiently solved by a theoretical quantum computer.

Complexity Classes



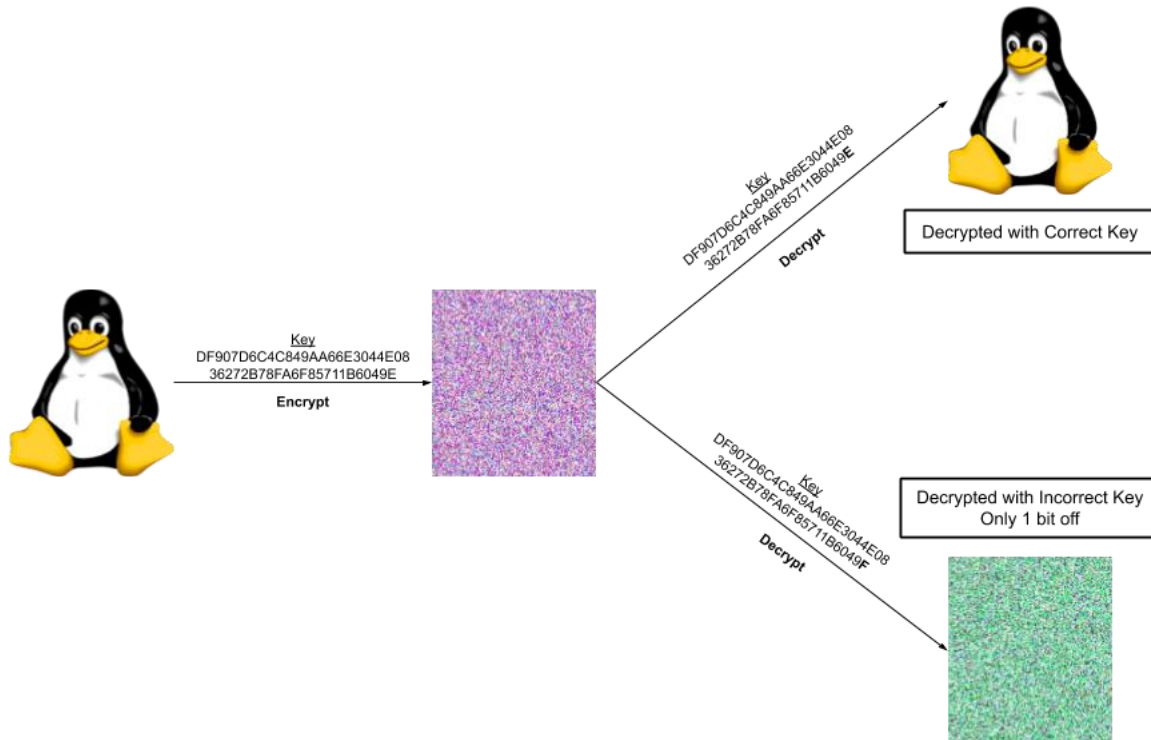
⁴² Shor P. (1997, October). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.

⁴³ Bernstein E. and Vazirani U. (1997, October). Quantum Complexity Theory.

⁴⁴ This image is actually somewhat simplified compared to the technical reality. It has been proven that BQP is not strictly a subset of the polynomial hierarchy. This model better represents BQP's relation to these specific problems rather than the BQP complexity class as a whole. This is done for the sake of simplicity.

Symmetric Encryption

There is one popular symmetric encryption scheme today that is recommended by NIST and the NSA. It is called AES which stands for the Advanced Encryption Standard.^{45 46} AES can be used in three modes, 128-bit key, 192-bit key, and 256-bit key. Breaking the confidentiality of AES requires finding the encryption key that is used to encrypt and decrypt the target message. A key is made up of bits. A bit is a 0 or a 1. There is not a better algorithm on a classical computer for finding a key used in AES encryption than to simply try every key until the correct one is found. This is because there are no “close guesses” when guessing keys. Meaning, one cannot tell the difference between being 1 bit off and n bits off of the correct key.



Because of this, the problem is in NP. A good way to see why this is in NP is if a key is made up of n bits, there are 2^n possible keys. Thus, finding the correct key requires potentially trying 2^n keys. If the key is made up of $n+1$ bits there are 2^{n+1} , $2 \cdot 2^n$ keys to potentially try. This means that by increasing the key size by 1, the size of the problem of finding the correct key is doubled. This is exactly the criteria for a problem to be in NP.

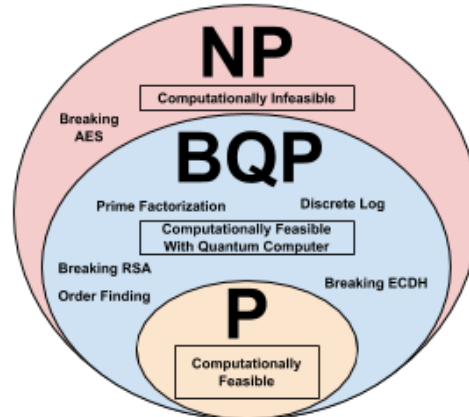
Remember AES has 3 modes, 128-bit, 192-bit, and 256-bit. This means that a classical computer would have to try 2^{128} , 2^{192} , and 2^{256} keys. The reason these numbers were chosen is because of a fundamental physical limit called the Landauer limit.⁴⁷ The Landauer limit suggests that even just listing all 2^{128} keys requires more energy than the sun has emitted since its birth.

⁴⁵ Barker E. (2016, August). Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms.

⁴⁶ Commercial National Security Algorithm Suite. (2015, August 19).

⁴⁷ Landauer R. (1961, July). Irreversibility and Heat Generation in the Computing Process.

Complexity Classes



In 1996, Lov Grover presented an algorithm that can be executed by a quantum computer, providing a quadratic speedup to the key search problem.⁴⁸ This is known as Grover's algorithm. Quadratic speedup means that finding the correct key when there are 2^n possible keys requires checking only $\sqrt{2^n}$ keys, which is $2^{n/2}$ keys. Grover's algorithm does not make the problem of guessing the correct encryption key in a complexity class lower than NP. This means that a quantum computer cannot solve this problem efficiently when n is too big. For example, if there were 2^{2n} possible keys, which only means adding n more bits to the actual key, Grover's algorithm requires checking 2^n keys, which is as good as before.

The problem is that this does cause issues for algorithms where the key size is too small. As happened with the precursor to AES, the Data Encryption Standard (DES), the increase in computing power will make certain that current AES key sizes are too small. This means that trying all keys can be done inefficiently but in a reasonable timeframe still. The 128-bit and 192-bit AES modes only require the attacker to try 2^{64} and 2^{96} keys respectively. This is certainly within the realm of possibility for a large array of computers to brute force.

Quantum Key Distribution

In practice, asymmetric encryption and symmetric encryption are used together. Asymmetric encryption, which is less efficient than symmetric encryption, is used to share a symmetric encryption key which is then used for the remainder of the encrypted messages.

Quantum Key Distribution (QKD) is another way by which Alice and Bob may exchange (distribute) keys that are used for symmetric encryption schemes.⁴⁹ Rather than relying on the mathematical hardness of a problem that asymmetric encryption relies on, it relies on the properties of quantum mechanics to guarantee security. Additionally, QKD allows Alice and Bob to exchange keys or detect an eavesdropper. Through the use of quantum mechanics, if Eve is eavesdropping on a channel where Alice is sending a private key to Bob, Eve will destroy some

⁴⁸ Grover L. (1996), A Fast Quantum Mechanical Algorithm for Database Search.

⁴⁹ Bennett C. and Brassard G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing.

of the information being sent to Bob. Bob will detect this and ask Alice to abort the current key and send a new key. This continues until no eavesdropper is detected and the derived secret key is used to communicate the secret message.

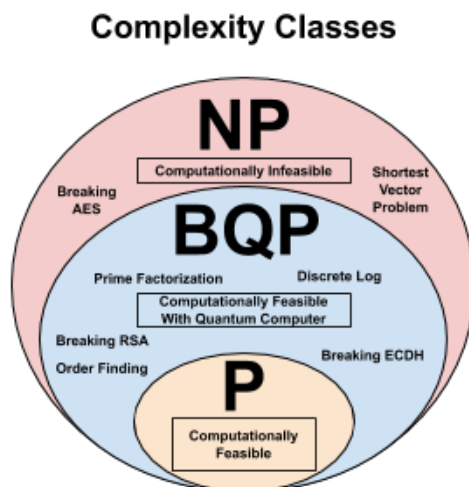
Inconsistencies Between Policy Concerns and Technical Realities

Quantum Computing Will Not Make Encryption Obsolete

It is true that quantum computing threatens the viability of *current* encryption systems RSA, ECDH, and smaller-key AES. But this significantly overstates the issue in a way that makes it appear that there are no solutions to this impending problem when, in fact, there are.

As for symmetric encryption, the 256-bit mode of AES is still secure against all known attacks. While it is notable that it is on the edge of being insecure, it is still secure against the best attacks by adversaries who have a significant amount of time and resources to dedicate. Additionally, constructing a scheme with a stronger level of security by multiple applications of AES, as was done with DES and 3DES, would be a simple and easy extension that would create a more secure cryptosystem.

As for asymmetric encryption, there is an entire movement in the field of cryptography at the moment investigating post-quantum cryptography.⁵⁰ The aims of this movement are to find efficient asymmetric schemes to replace RSA and ECDH with new quantum-secure encryption schemes. These newly proposed schemes are based on new problems in NP that are not in P or BQP, such as the shortest-vector problem or the syndrome decoding problem.⁵¹



In fact, NIST is currently in the process of standardizing a quantum-safe public key encryption system which will be completed by 2024.⁵² The NSA has followed suit by announcing its CNSA

⁵⁰ Chen L., Jordan S., Liu Y., Moody D., Peralta R., Perlner R., Smith-Tone D. (April 2016). Report on Post-Quantum Cryptography.

⁵¹ McEliece R.J. (1978, January). A Public-Key Cryptosystem Based on Algebraic Coding Theory.

⁵² Chen L., Jordan S., Liu Y., Moody D., Peralta R., Perlner R., Smith-Tone D. (April 2016). Report on Post-Quantum Cryptography.

Encryption Suite which is meant to be a transitional encryption standard before quantum-safe encryption becomes standardized.⁵³ These new algorithms can be run using a classical computer. In the future, there will be encryption schemes that provide the same level of security against quantum and classical computers as the level provided by current encryption schemes against classical computers.

Quantum Computing Does Not Provide A Significantly New Encryption Capability

It is true that QKD solves the problem of eavesdropper detection. Because of this, policy scholars have made the claim that the ability of “the recipient and sender [to] determine if the message has been intercepted” is a “major advantage” over classical cryptography.⁵⁴ While it is an interesting advancement in technology, it does not actually provide a comparative advantage in secure communications over classical cryptography because eavesdropper detection is not a problem in secure communications in the first place.

When Alice and Bob use QKD, Eve cannot get ciphertext and therefore cannot get any corresponding plaintext. When Alice and Bob use classical cryptography, Eve can get ciphertext. But, Eve cannot solve the underlying NP problem required to decrypt the ciphertext without the decryption key, so Eve cannot get any corresponding plaintext. While QKD and classical cryptography use completely different methods, the level of security provided to Alice and Bob is indistinguishably the same amongst the two methods. The operational difference between an eavesdropper not being able to eavesdrop and an eavesdropper not being able to derive value from recovered ciphertext is negligible. From this, the conclusion to be drawn is that quantum computing does not provide a higher level of security over classical computing.

The Race For Quantum Supremacy Is Primarily an Economic Race

Quantum computing will not pose a threat to secure communications guaranteed by cryptography after the standardization of post-quantum encryption schemes. Future US communications will be guaranteed the same level of security against future computers that current cryptography provides against today’s computers. Adversary intelligence organizations will still be challenged by US encryption schemes. By the same token, adversaries will not gain a higher level of security against the US’s intelligence efforts through the use of quantum-aided cryptography. The US will just be as stymied as it is today, but not any worse off. Essentially, nothing will change about the intelligence gathering and information protection capabilities of the US and its adversaries. There is no national security risk in these areas from the perspective of a cryptographer after post-quantum encryption standardization.

This calls into question why the “race for quantum supremacy” appears to be focused on the effects of quantum computing on cryptography. The “race for quantum supremacy” with China has a lot more to do with economic dominance and technological prestige than it does with national security. Quantum technologies do have many extremely valuable commercial applications and the country that develops it the fastest will likely gain a first-mover economic

⁵³ Commercial National Security Algorithm Suite. (2015, August 19).

⁵⁴ Kania E. and Costello J. Quantum Hegemony? (2018, September 12). China’s Ambitions and the Challenge to U.S. Innovation Leadership.

advantage. While economic capacity is certainly an extension of state power, this “race for quantum supremacy” is less pressing than the race for supremacy in missile technology that played out through the Space Race.

The More Pressing National Security Problem

While the technical realities of quantum computing demonstrate that there are no completely permanent security implications of quantum computing, there is a notable longer-term national security problem. The problem is the compromise of classified information with long-term intelligence value secured by contemporary encryption schemes that can be broken in the future by a quantum computer.

The Problem

The power of the US government to classify sensitive information is currently derived from the Office of the President through Executive Order 13526 which was enacted in 2009. It specifies that classification is limited to 8 broad areas:

“military plans, weapons systems, or operations; foreign government information; intelligence activities (including covert action), intelligence sources or methods, or cryptology; foreign relations or foreign activities of the United States, including confidential sources; scientific, technological, or economic matters relating to the national security; United States Government programs for safeguarding nuclear materials or facilities; vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or the development, production, or use of weapons of mass destruction”.⁵⁵

The most important aspect of EO 13526, as it relates to the discussion of quantum computing and cryptography, is that this order allows for the classification of all types of information for as long as 25 years.⁵⁶ Along the same lines, the NSA provides guidelines to its contractors that classified information has a potential “intelligence life” of up to 30 years.⁵⁷ This means that information with long-term intelligence value currently being secured by the RSA, ECDH, and AES encryption schemes today will be relevant to national security through at least 2049.

This would not be a notable fact if the encryption schemes used to secure this information would not be threatened within this time frame, but because of quantum computing they could be. Even the most conservative estimates suggest that quantum computing will be a reality before 2049. It is additionally notable that the US has had intelligence programs where operators intercepted and stored encrypted messages for the expressed purpose of breaking the encryption at a later time.⁵⁸ There is no reason adversaries would not be doing the same things today knowing that quantum computing is in the future.

⁵⁵ The President Executive Order 13526. (December 29, 2009).

⁵⁶ The President Executive Order 13526. (December 29, 2009).

⁵⁷ Commercial National Security Algorithm Suite and Quantum Computing FAQ. (2016, January).

⁵⁸ Crowell W. Remembrances of VENONA.

In summary, information regarded as important to national security today that is protected by today's encryption schemes will not be secure in the future against cryptanalysis enabled by a quantum computer. This is the major national security implication of quantum computing.

Venona Project

As previously stated, in the past the US has had a program where intelligence efforts were focused on intercepting and storing encrypted information for later cryptanalysis. Towards the end of WW2, the US became suspicious of the intentions of the USSR and began to intercept encrypted Soviet messages. Because of operator error, some of the messages were partially decryptable. When the US realized this, a program was conceived to decrypt these messages. It was known as the Venona Project.⁵⁹

The Venona Project proved to be extremely damaging to Soviet national security interests. The US was able to identify and neutralize noted Soviet spies Julius and Ethyl Rosenberg, Klaus Fuchs, Alger Hiss, and many others regarded by Soviet intelligence to be particularly important. The project remained an active program from 1943 to 1980.⁶⁰ This is notable because it confirms the notion that the intelligence life of the intercepted encrypted data can be many decades long.

There is no reason something like this could not happen again when quantum computers become a reality. It is very likely that both the US and its adversaries will have their own Venona-style projects in the future. The US will benefit from being able to use this form of espionage against its adversaries and be hurt by the fact that the US's adversaries will be using this form of espionage against it.

This problem is recognized by a few scholars and individuals in the policy community. Most notably Richard Clarke and Robert Knake⁶¹ have stated that "governments have been rumored for years to be collecting and storing other nations' encrypted messages that they now cannot crack" with the hope of cracking them in the future when a quantum computer is acquired.⁶² For example, an article by Jon Lindsay⁶³ has also recognized this potential future problem too.

Institutional Contribution To Long Term Risk

As long as the US continues to use encryption algorithms that are not quantum resistant, sensitive information will be exposed to this long-term risk. And the later the US switches to a quantum resistant algorithm, the more the US will be exposed to this risk.

⁵⁹ Crowell W. Remembrances of VENONA.

⁶⁰ Crowell W. Remembrances of VENONA.

⁶¹ Richard Clarke and Robert Knake have combined served in four different presidential administrations on various security issues at the Department of Defense and Department of Homeland Security.

⁶² Clarke R. and Knake R. (2019, July). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats.

⁶³ Lindsay J. (2018, July 10). Why Quantum Computing Will Not Destabilize International Security : The Political Logic of Cryptology.

NIST is currently in the process of standardizing a quantum resistant algorithm for this exact reason and it is projected to be completed with standardization in 2022 at the earliest, or 2024 at the latest.⁶⁴ Shortly after standardization, the NSA will publish its own standard that will reflect the NIST standardized encryption schemes. The NSA has stated that “algorithms often require 20 years to be fully deployed on NSS [National Security Systems]”.⁶⁵ Because of this, some parts of the US national security apparatus will be using encryption algorithms that are not quantum resistant as late as 2044. Any information secured by encryption schemes that are not quantum resistant up to that point is at risk of long-term decryption by US adversaries.

Considering that quantum computing technology is rapidly advancing, the 20-year deployment timeline adds another 20 years of significant long-term risk to any assessment of this problem.

Recommendations

There are a number of short-term precautionary measures that can mitigate this problem. While the US cannot take back any encrypted data already in the possession of adversary intelligence agencies, the US can institute a number of short-term reforms that can make the impact of this reality less of a security issue by stemming the flow of future data to adversaries.

Recommendations for NIST Standards

Despite having recognized the need for encryption schemes that are resistant to attacks by quantum computers and that some current encryption schemes do not provide this protection,⁶⁶ official NIST standards currently do not line up with this position. Specifically, NIST still specifies that the use of the 128-bit and 192-bit modes of the AES encryption schemes to provide cryptographic protection for federal government data is allowed beyond 2031.⁶⁷ These algorithms are not resistant to an attack by Grover’s algorithm. NIST should invalidate the aspects of FIPS 197, which is the official NIST specification of AES,⁶⁸ which allows for the use of AES-128 and AES-192. While it is important to recognize that IT best practices suggest that AES-256 solely be used anyways, a government agency or a government contractor can still be federally compliant using a weaker encryption scheme. This is a security risk that can be easily solved by the invalidation of AES-128 and AES-192 as cryptographically secure encryption schemes beyond 2031.

Moreover, the NSA has withdrawn its support of AES-128 and AES-192 as cryptographically secure long-term encryption schemes because of quantum computing.⁶⁹ The NSA only allows these schemes to be used on legacy systems that it plans to phase out and only in exceptional circumstances. By withdrawing support for AES-128 and AES-192, NIST would become consistent with its counterpart in the way that US cryptography standards are set.

⁶⁴ Post-Quantum Cryptography – Workshops and Timeline. (2017, January 03).

⁶⁵ Commercial National Security Algorithm Suite. (2015, August 19)

⁶⁶ Chen L., Jordan S., Liu Y., Moody D., Peralta R., Perlner R., Smith-Tone D. (April 2016). Report on Post-Quantum Cryptography.

⁶⁷ Barker E. (2016, January) Recommendation for Key Management Part 1: General.

⁶⁸ Announcing the Advanced Encryption Standard (AES). (2001, November 26).

⁶⁹ Commercial National Security Algorithm Suite. (2015, August 19).

While it is important to note that a practical attack may not materialize for a long time even after quantum supremacy is achieved, there is no reason to take the risk that an attack may materialize earlier. The downside of invalidating AES-128 and AES-192 as cryptographically secure encryption schemes beyond 2031 would be the economic costs of forcing government agencies and contractors to update their encryption schemes over a 10 year period. This is nothing compared to the downside of the status quo, which would be the national security costs of losing sensitive and/or classified federal government information to adversaries. After all, accurately predicting the pace of technology has proven to be nearly impossible even when the predictions come from the foremost experts in the field. There is little to lose by betting against these predictions and a lot to lose by betting in favor of them. Because of the issue of long-term intelligence, this should be done as quickly as possible.

Additionally, NIST could develop and standardize a version of AES with a longer key size. Similar to the way that 3DES, Triple DES, replaced DES by applying the same encryption scheme multiple times with different keys,⁷⁰ NIST could develop and standardize 3AES which applies AES multiple times with different keys to get a higher level of security.

Recommendations for NSA Standards

As previously stated, the NSA has noted that it takes approximately 20 years to fully deploy any cryptographic algorithm across national security systems.⁷¹ This should be considered unacceptable in light of the threat of quantum computing against long-term intelligence. Twenty years to fully deploy a new cryptographic algorithm directly translates into an extra 20 years of long-term intelligence that could become compromised. The amount of time to fully deploy a cryptographic algorithm across NSS should be lowered to the smallest timeframe that is feasibly possible. At the very least, it should be significantly below 20 years, which is an excessively long time to implement cryptographic standards. Even if this time period cannot be significantly reduced, the NSA should take steps to triage modernization efforts and ensure that the most sensitive systems and information are updated first with quantum-safe encryption schemes.

Recommendation for Risk Mitigation

Luckily for the defenders of classified information, the use of encryption still has advantages that can be magnified. While attackers with quantum computers could successfully break a significant number of encryption schemes within a reasonable timeframe, it still may take an extremely large amount of time and resources to carry out such attacks. While the encryption schemes being used today can eventually be broken, risk mitigation efforts can be undertaken that can make it longer to decrypt information.

This can be done by setting up honeypots - systems disguised as vulnerable classified networks that contain only useless encrypted data - and allowing them to be exploited by US adversaries. This would force adversaries to waste substantial amounts of time using valuable computer cycles decrypting useless information. Depending on the extent to which such an operation is

⁷⁰ Update to Current Use and Deprecation of TDEA. (2017, July 11).

⁷¹ Commercial National Security Algorithm Suite and Quantum Computing FAQ. (2016, January).

undertaken, this could double or triple the average amount of time and resources it takes for adversaries to decrypt a useful piece of intelligence information. Such an operation would be classified as defense by deception⁷² which is a well-proven strategy⁷³ to stymie hackers looking to steal sensitive information. This strategy is simply an application of an old counterintelligence strategy to deal with a new problem.

Conclusion

Quantum computing will have an impact on national security, just not in the way that some of the policy community claims that it will. Quantum computing will not significantly reduce or enhance the inherent utility of cryptography in providing confidentiality guarantees on messages sent across insecure channels. Additionally, while the US may be in an economic and technological competition with near-peer economic competitors in the realm of quantum computing, the outcome of this competition will not fundamentally change the distribution of military and intelligence advantages between the great powers.

That being the case, the US needs to be wary of long-term threats to the secrecy of sensitive information being protected by contemporary cryptographic schemes. These threats can be mitigated by updating NIST recommendations to be consistent with the NSA's recommendations, triaging cryptographic updates to systems that communicate and store sensitive and classified information, and taking countermeasures that significantly increase the amount of time and resources it takes for adversaries to exploit stolen encrypted information.

Whereas some believe that quantum computing poses an existential threat to secrecy, in reality the threats of quantum computing are manageable as long as the governing institutions of the US implement a few simple, common sense reforms.

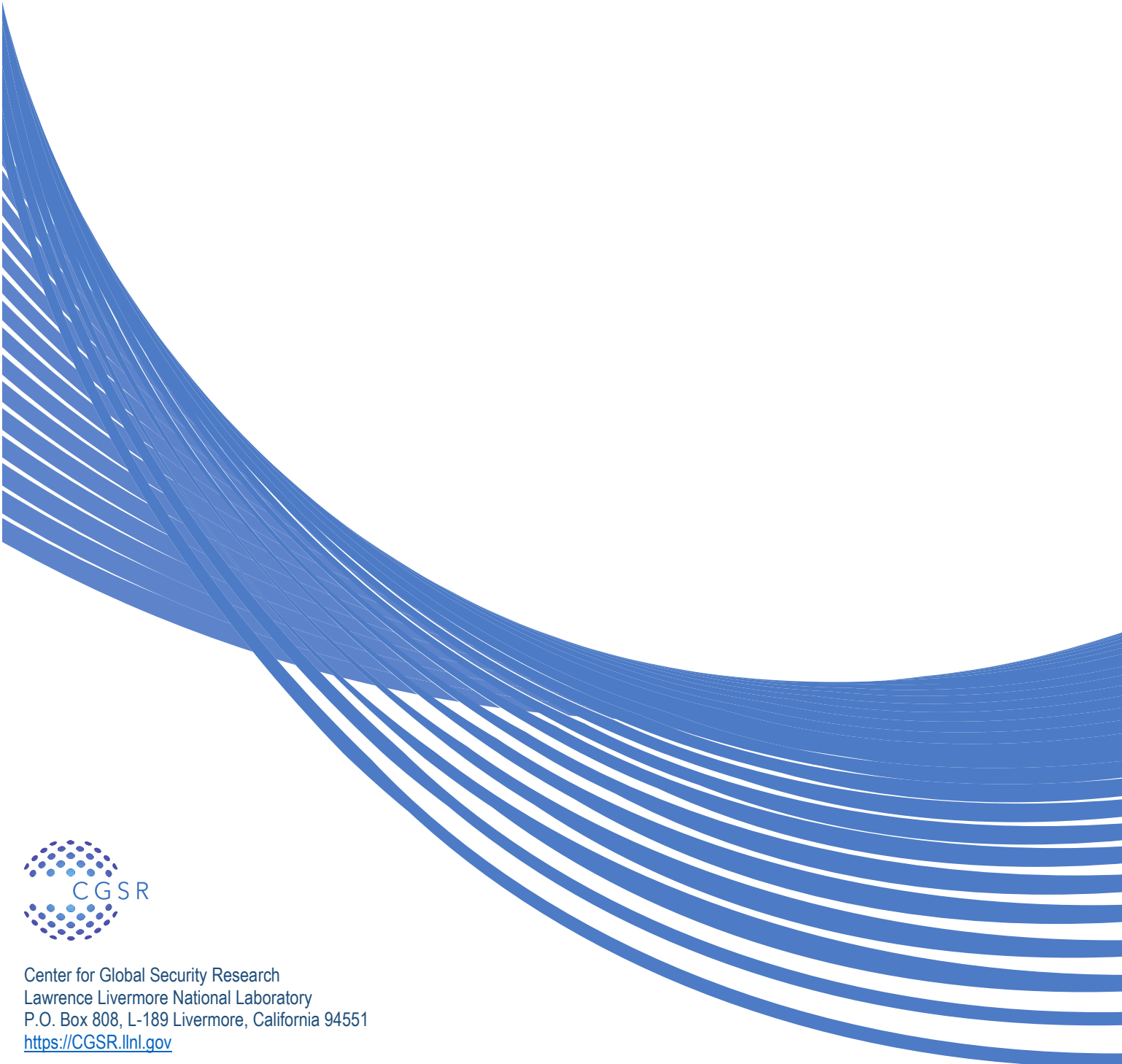
⁷² Gartzke E. and Lindsay J. (2015, June 22). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace.

⁷³ Stoll C. (1989). The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage.

References

1. Harrow A. and Montaro A. (2018). Quantum Computational Supremacy. Retrieved from <https://www.nature.com/articles/nature23458>
2. Nikias C. (2018, May 11). This is the Most Important Tech Contest Since the Space Race, and America is Losing. Retrieved from https://www.washingtonpost.com/opinions/this-is-the-most-important-tech-contest-since-the-space-race-and-america-is-losing/2018/05/11/7a4a4772-4e21-11e8-b725-92c89fe3ca4c_story.html?utm_term=.52d04321761d
3. Ashbaugh L. (2018, April 18). The Quantum Race the United States Can't Afford to Lose. Retrieved from <https://www.cfr.org/blog/quantum-race-united-states-cant-afford-lose>
4. Kaplan F. (1983). Wizards of Armageddon
5. Whalen J. (2019, August 18). The Quantum Revolution is Coming, and Chinese Scientists are at the Forefront. Retrieved from <https://www.washingtonpost.com/business/2019/08/18/quantum-revolution-is-coming-chinese-scientists-are-forefront>
6. Ricks T. (2017, November 28). The Quantum Gap with China. Retrieved from <https://foreignpolicy.com/2017/11/28/the-quantum-gap-with-china/>
7. Hurd W. (2017, December 7). Quantum Computing is the Next Big Security Risk. Retrieved from <https://www.wired.com/story/quantum-computing-is-the-next-big-security-risk/>
8. Mulvaney M. and Kratsios M. (2018, July 31). Memorandum for the Heads of Executive Departments and Agencies – FY 2020 Administration Research and Development Budget Priorities. Retrieved from <https://www.whitehouse.gov/wp-content/uploads/2018/07/M-18-22.pdf>
9. H.R. 6227 – National Quantum Initiative Act. (2018, December 21). Retrieved from <https://www.congress.gov/bill/115th-congress/house-bill/6227>
10. Majot A. and Yampolskiy R. (2015, September). Global Catastrophic Risk and Security Implications of Quantum Computers. Retrieved from <https://doi.org/10.1016/j.futures.2015.02.006>
11. Biercuk V. and Fontaine R. (2017, November 17). The Leap Into Quantum Technology: A Primer For National Security Professionals. Retrieved from <https://warontherocks.com/2017/11/leap-quantum-technology-primer-national-security-professionals/>
12. Testimony of James F. Kurose before the Subcommittee on Research and Technology and the Subcommittee on Energy on American Leadership in Quantum Technology. (2017, October 24). Retrieved from <https://science.house.gov/imo/media/doc/Kurose%20Testimony%20FINAL%20w%20Bio.pdf>
13. Katz J. and Lindell Y. (2015). Introduction to Modern Cryptography.
14. Barker E. (2016, August). Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms. Retrieved from <http://dx.doi.org/10.6028/NIST.SP.800-175B>
15. Commercial National Security Algorithm Suite. (2015, August 19). Retrieved from <https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm>
16. Dasgupta S., Papadimitriou C., and Vazirani U. (2006, July 18). Algorithms.
17. Shor P. (1997, October). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. Retrieved from <https://doi.org/10.1137/S0097539795293172>
18. Bernstein E. and Vazirani U. (1997, October). Quantum Complexity Theory. <https://doi.org/10.1137/S0097539796300921>
19. Landauer R. (1961, July). Irreversibility and Heat Generation in the Computing Process. Retrieved from <https://ieeexplore.ieee.org/document/5392446>
20. Grover L. (1996), A Fast Quantum Mechanical Algorithm for Database Search. Retrieved from <https://arxiv.org/abs/quant-ph/9605043>
21. Bennett C. and Brassard G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. Retrieved from <https://doi.org/10.1016/j.tcs.2014.05.025>

22. Chen L., Jordan S., Liu Y., Moody D., Peralta R., Perlner R., Smith-Tone D. (April 2016). Report on Post-Quantum Cryptography. Retrieved from <http://dx.doi.org/10.6028/NIST.IR.8105>
23. McEliece R.J. (1978, January). A Public-Key Cryptosystem Based on Algebraic Coding Theory. Retrieved from <https://doi.org/10.1109/ICCCC.2016.7496747>
24. Mosca M. (2015). Cybersecurity in an era with quantum computers: will we be ready? Retrieved from <https://doi.org/10.1109/MSP.2018.3761723>
25. The President Executive Order 13526. (December 19, 2009).
26. Commercial National Security Algorithm Suite and Quantum Computing FAQ. (2016, January). Retrieved from <https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm>
27. Crowell W. Remembrances of VENONA. Retrieved from <https://www.nsa.gov/News-Features/Declassified-Documents/venona/remembrances/>
28. Next Generation NC3 Enterprise Challenge. (2018, November 27). Retrieved from <https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=390609791364842047d3ab34aa7d1441>
29. Post-Quantum Cryptography – Workshops and Timeline. (2017, January 03). Retrieved from <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline>
30. Barker E. (2016, January) Recommendation for Key Management Part 1: General. Retrieved from <http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4>
31. Announcing the Advanced Encryption Standard (AES). (2001, November 26). Retrieved from <https://doi.org/10.6028/NIST.FIPS.197>
32. Update to Current Use and Deprecation of TDEA. (2017, July 11). Retrieved from <https://csrc.nist.gov/News/2017/Update-to-Current-Use-and-Deprecation-of-TDEA>
33. Gartzke E. and Lindsay J. (2015, June 22). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. Retrieved from <https://doi.org/10.1080/09636412.2015.1038188>
34. Stoll C. (1989). The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage.
35. Kania E. and Costello J. Quantum Hegemony? (2018, September 12). China's Ambitions and the Challenge to U.S. Innovation Leadership. Retrieved from <https://www.cnas.org/publications/reports/quantum-hegemony>
36. National Strategic Overview for Quantum Information Science. (2018, September). Retrieved from <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf>
37. Harris Introduced Bill to Increase Resources for Quantum Computing and Research to Benefit National Security. (2018, June 07). Retrieved from <https://www.harris.senate.gov/news/press-releases/harris-introduces-bill-to-increase-resources-for-quantum-computing-and-research-to-benefit-national-security>
38. Lindsay J. (2018, July 10). Why Quantum Computing Will Not Destabilize International Security : The Political Logic of Cryptology. Retrieved from <http://dx.doi.org/10.2139/ssrn.3205507>



Center for Global Security Research
Lawrence Livermore National Laboratory
P.O. Box 808, L-189 Livermore, California 94551
<https://CGSR.llnl.gov>

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. LLNL-TR-790870