An Introduction to Quantum Computing and Its Applications

1st Lt. Mandeep Singh
Dr. Albert H. Carlson

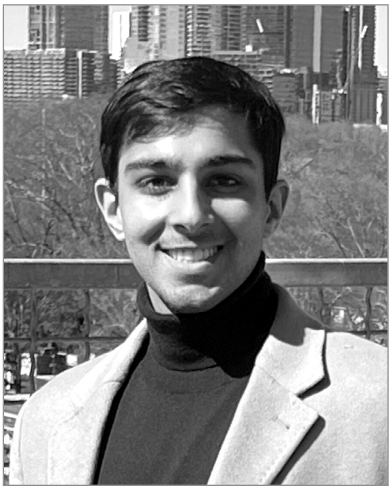
ABSTRACT

Winning is much easier if you have an edge, whether that be better personnel, strategy, and/or technology. Quantum Information Science (QIS) - which includes quantum sensing, networking, communications, and computing - provides a technology that both tactical and strategic commanders will leverage to seize the initiative and create positions of advantage. Optimizing the exploitation of quantum technology will require that senior leaders understand enough about the technology and its fast-evolving applications to outmaneuver and outthink our adversaries. This does not require expertise in all facets of QIS, any more than a computer user needs to know computer design. This article attempts to be an introduction to quantum technology and some of its potential uses in the military operational environment.

INTRODUCTION

Had the Nazis won the race to harness the power of the atom, many would agree that World War II could have been disastrously lost, leaving the maps of Europe and the Americas vastly different. But what if the Nazis had quantum technologies before the D-Day invasion?

What if the Germans had the ability to thoroughly inspect key elements of the great deception plan, called Bodyguard, which misled the Germans about the location of the



First Lieutenant Mandeep Singh grew up in Santa Clara, CA and attended college at Santa Clara University (SCU), earning degrees in Computer Science and Electrical Engineering with a minor in Mathematics. He has worked for several San Francisco Bay Area startups with roles in software development and architecture design, and currently is pursuing his graduate degree in Computer Science & Engineering at SCU. After earning his commission into the Cyber Corps, 1st Lt. Singh was the honor graduate of graduated his Cyber Basic Officer and Electromagnetic Warfare Qualification Courses at Fort Eisenhower, GA. He was then assigned to Fort Lewis, WA, where he now serves as the Electromagnetic Warfare Detachment Commander for 1st Special Forces Group (A). 1st Lt. Singh's areas of interest for research are quantum computing, post-quantum encryption algorithms, cryptography, and artificial intelligence. He recently published two articles in the fields of mathematics and cryptography with Dr. Carlson, earning best in conference at the 2024 AI IoT World Congress.

D-Day invasion? Using data from quantum LIDAR, magnetic field, and EM sensors, the Nazis likely would have known that the camps around the city of Dover and the landing crafts assembled along the southeast coast of England were phantom camps and ghost vessels, devoid of troops and actual equipment. These cleverly designed deception elements gave the Nazis every indication that the Allied invasion would cross the English Channel into Pas-de-Calais, not Normandy, which was 150 miles to the southwest.[1]

Quantum LIDAR and imaging would have enabled the Nazis to track ship movement in real-time as they approached Normandy, and identify that the large clouds of aluminum strips dropped by Allied aircraft flying toward Pas-de-Calais were not, in fact, a large fleet of Allied ships, but just a decoy.[2] What if, instead of Allied codebreakers deciphering Germany's secret communications, they were able to crack ours? QIS would have given the Nazis a powerful advantage over the Allied Forces on D-Day. Nazi decision makers would have data sets, devoid of deceptive data, that led them to reinforce Normandy, and this data-driven decision would have potentially changed the fate of the Allied D-Day invasion and the outcome of the war.

Today, quantum computing is mostly inaccessible. To be prepared to use quantum technology when it is available, we must have the discussion about how to employ the technology today. Unlike the classical computers in universal use today, the size, high cost, and mechanical and operational sophistication of quantum computers have rendered them highly limited for use today.[3] Most quantum computers are owned by governments, large corporations, and select universities. Classes and instruction on quantum computing are currently limited to a few institutions of higher learning.[4] While not generally available, it can be anticipated that offerings for quantum instruction will rapidly increase, similar to artificial intelligence. This does not

Dr. Albert H. Carlson was born and raised in Chicago, IL, and attended the University of Illinois at Urbana, graduating with a B.S. in Computer Engineering in 1981 and entered the U.S. Army as an Electronic Warfare Officer. After assignment to the 105th MI Bn at Fort Polk, he worked as a computer and electrical engineer in various civilian companies and earned his Ph.D. in Computer Science with a focus in Set Theory applied to Cryptography at the University of Idaho. Dr. Carlson holds nine patents on polymorphic cryptographic algorithms, and has taught at Fontbonne University in St. Louis and Austin Community College. He currently conducts research and mentors graduate students at the University of Louisiana at Lafayette. Dr. Carlson serves as the Chair for Entropy and Encryption for the Quantum Security Alliance and works with IEEE on Cybersecurity for Next Generation Privacy. His research areas include cryptography, artificial intelligence, generative adversarial network applications, quantum cybersecurity, and control systems for aquaria.

mean that it will remain hard to access for very long. The impact of quantum machines is already being felt disproportionately by governments, academia, the military, and policymakers, and as of June 2024 various nations have invested about $55 billion,[5] to develop a general-purpose quantum computer. Nation-states are making this investment because quantum computers are projected to be able to break what cryptographers presently see as the most secure encryption ciphers: the asymmetric Public Key Encryption (PKE) algorithms.[6]

The United States has confirmed that a cryptanalytically relevant quantum computer (CRQC) could put global communications systems, critical infrastructure, and financial transactions at risk.[7] The first country to achieve a general-purpose quantum computer, with a sufficient number of qubits, will have a significant position of advantage over others in this era of Great Power Competition. Classical computers cannot begin to achieve the same operations that quantum computers use to break PKE cipher algorithms due to their basic hardware technology.[8] Breaking PKE algorithms will require both a technology and paradigm upgrade. We are currently in a technological cold war to achieve general-purpose quantum computing. Future leaders will need to know how to leverage each new capability to create positions of advantage over our adversaries. The time for developing the people and concepts for a quantum future is now. This article presents the basics of quantum computing to assist forward-thinking leaders and technicians in how to better operationally deploy it in the future.

BASICS OF QUANTUM COMPUTING

Quantum computers are similar in structure and function to a classical computer. From an operational viewpoint, the user interface is usually a classical computer with a backend quantum coprocessor

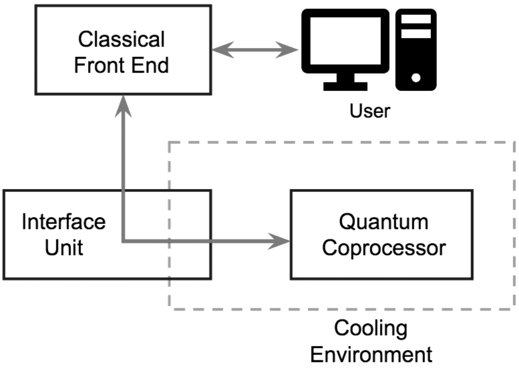


Figure 1. Classical Front End to Quantum Coprocessor.

(see Figure 1), with a classical front end interface where users do the actual programming, and where the language, compilers, algorithms, and communications protocols are found. This computer is typically programmed using Python and stores the program locally until it is transferred to the quantum coprocessor. This transfer occurs through the cooling unit or "chandelier."[9] Quantum hardware and the coprocessor are placed inside a supercooled enclosure that is large enough for technicians to work on that hardware. These rooms are typically a ten foot cube consisting of air, insulating walls, refrigeration equipment, and the computer, itself. Inside the cooled unit are the quantum computing hardware and the interface to keep things cold. Then the quantum coprocessor does the computation, arrives at the answer, and transfers the solution back to the classical computer via the interface unit in the chandelier to the user.

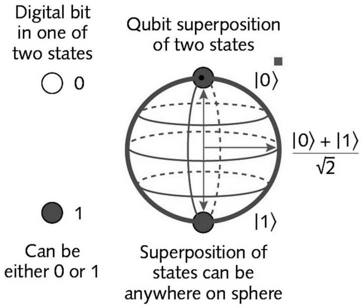

Digital bit in one of two states
0
1
Can be either 0 or 1
Qubit superposition of two states
|0⟩
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
|1⟩
Superposition of states can be anywhere on sphere

Figure 2. Multiple Positions in All Directions.[10]

Classical computers represent information in bits, the smallest encoding possible for information represented as 0 or 1, that are then combined to represent larger units of information, such as characters. Quantum computers use a similar, but more powerful type of representation for information, called quantum bits, or "qubits" for short. Qubits are like classical bits on steroids. Bits are independent units, but qubits can combine to represent even more data. In the quantum processor, qubits can be in the binary state typically depicted at a 0 or 1 like classical computers, but they can occupy multiple states simultaneously. This allows for the encoding of information at multiple positions, but also multiple positions in angles from the poles, e.g. at 90-degrees, 30 degrees, or 15 degrees (in all directions, see Figure 2)[11] not just at the poles (0 or 1). Multiple orientations of data give rise to the concept of quantum digits, or "qudits"[12] allowing for quantum computers to encode and process at a rate much faster than a classical computer.[13]

The interface between the two machines passes data from the classical computer to the Quantum Processing block shown in Figure 3. This block, or layer, contains the memory, registers, and logic gates for computing at the quantum level. It may also be the "edge" of the quantum machine where all the bookkeeping and storage that is needed by the quantum hardware. This layer interacts with the Classical Computing layer to set up a program and later report the results, while also working with the Quantum Hardware layer to run programs.

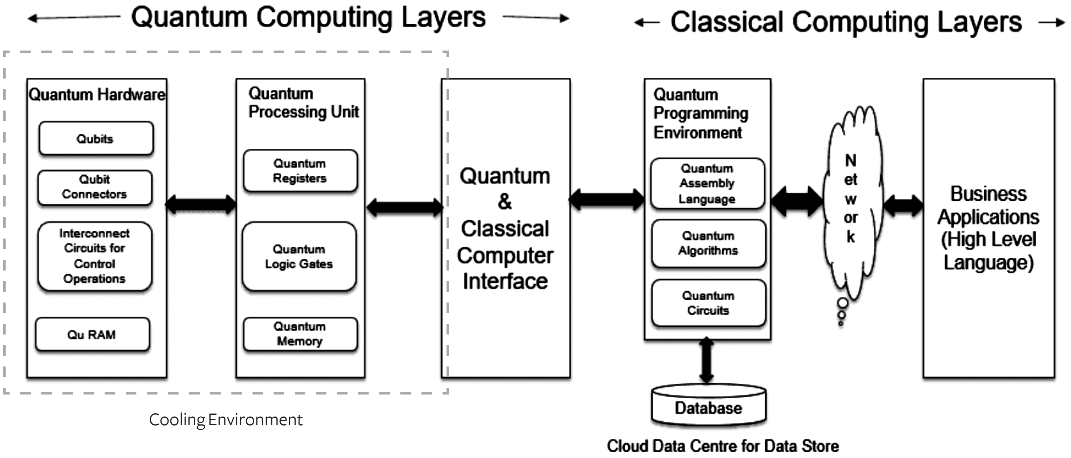

Quantum Computing Layers
Classical Computing Layers
Quantum Hardware
Qubits
Qubit Connectors
Interconnect Circuits for Control Operations
Qu RAM
Quantum Processing Unit
Quantum Registers
Quantum Logic Gates
Quantum Memory
Quantum & Classical Computer Interface
Quantum Programming Environment
Quantum Assembly Language
Quantum Algorithms
Quantum Circuits
Network
Business Applications (High Level Language)
Database
Cloud Data Centre for Data Store
Cooling Environment

Figure 3. Detailed Structure of Quantum Computer.[14]

The Quantum Hardware layer consists of the storage unit for qubit memory, called the quRAM (fast local memory), and all connectors that help conduct the processing, and must be supercooled to correctly operate. As of late 2023, the time that supercooling can be maintained was an extremely short 34 ms.[15] At the end of this process, the layer loses coherence (the ability to entangle qubits) and all computational activities end. Quantum computers also take a long time to cool down between runs to achieve the necessary cold temperature. In 2023, IBM quantum machines required up to 2.5 days to achieve that cooling.[16] This situation should be fixed by the development of room temperature qubits.

Qubits can be created using any two-level quantum system. Some of the promising types of qubits being developed include: superconducting, trapped ions, quantum dots, and photons atoms.[17]

- Superconducting qubits are made from superconducting materials operating at extremely low temperatures and can be manipulated by microwave pulses. For the last decade researchers have used superconducting transmon qubits which are favored by researchers due to their high designability, scalability, and controlability.[18] One problem with superconducting qubits is the coherence time, how long a qubit can run algorithms or perform operations before qubit drops its information, is relatively short. Researchers at MIT recently developed a superconducting qubit architecture using fluxonium qubits connected by transmon that can perform operations between qubits with high accuracy[19] that could help make superconducting qubits the path to a fault-tolerant quantum computer.[20]
- Trapped ions can also be used as qubits storing information in suspended free space around ions trapped using oscillating electromagnetic fields. Trapped ion qubits are noteworthy because the qubits have a relatively long lifetime, long internal state

coherence, and high-fidelity measurements[21] but there are challenges to scaling them. Quantum computers with ion traps contain about 30 qubits each.[22] However due to the nature of the oscillating electromagnetic field, combining more than multiple qubits on a single chip causes the trap to heat up significantly.[23] As of March 2024, new developments in using static magnetic fields instead of oscillating fields, called a Penning trap, show promise toward the realization of scaling trapped ion qubits and will benefit both quantum computing and sensors.[24]

- A quantum dot is a nanoscale crystal semiconductor capable of holding a single electron or a small group of electrons that give the dot spin. These spins represent qubits of information and can exist in two states at once, both up and down, allowing computers that use them to do many calculations simultaneously.[25] Silicon chips, etched with quantum dots holding single electrons in their spin, appeared to be a feasible solution to bringing quantum computers to the masses but researchers were unable to manage the heat generated.[26] In May 2024, MIT and MITRE researchers demonstrated a "quantum-system-on-chip" architecture that integrates thousands to qubits on an integrated circuit and then connects multiple chips via optical networking.[27] This progress toward general-purpose quantum computing was significant "...with over 4,000 qubits that could be tuned to the same frequency while maintaining their spin and optical properties."[28]
- Photon qubits can be used to send quantum information through fiber optic cables by setting directional spin states of individual light particles.[29] Photon qubits are used in quantum communication and quantum cryptography. Recent developments at Berkeley's Accelerator Technology & Applied Physics (ATAP) Lab include research on programmable spin-photon qubits uses a femto-second laser to create and destroy qubits on demand and at desirable locations.[30] Photon qubits were primarily viewed as information carriers between quantum computers to enable distributed processing. However, the development of the photonic quantum chip[31] and a metal-ion qubit that absorbs light and emits color,[32] makes a room temperature quantum computer appear to be possible.

Each type of qubit has shortcomings that must be overcome; breakthroughs cannot be accurately forecasted. However, using statistical nonlinearities it is estimated that a room-temperature quantum computer will be possible by 2031.[33] While most qubit implementations today take on the same binary values used in classical computers, many of these technologies can be used for more than representing binary values.[34]

The ability to represent more than two values results in a qudit. The multi-level unit provides a larger space to store and process information.[35] Qudits can encode up to seven numbers, unlocking more computational power with fewer components, and can be a path to effective scaling.[36] For the purposes of this article, we will continue to describe quantum particles as qubits since most research we discuss is done using qubits.

Qubits are said to be entangled when they remain connected even when separated by large distances.[37] Knowing the state of one particle automatically tells you something about its entangled partners and changing one qubit will affect all the qubits entangled with it.[38] This connection allows qubits to perform vastly more operations per qubit than a classical computer can per bit, and computing power rises exponentially with the number of qubits. As of March 2024, quantum computers are primarily being used for simulations, optimization, and data analysis problems as most applications of quantum computing are still theoretical and, according to John Preskill, a theoretical physicist at the California Institute of Technology, it is challenging to find problem sets worthy of quantum computer "...because classical computers are pretty good at a lot of the things they do."[39]

Most quantum computing capabilities and research are conducted in isolated, temperature controlled, super-cooled environments connected to the outside world via an interface unit to a classical computer. As such, most current cybersecurity considerations are indirect in nature and involve indirect attack vectors on the power, cooling, or vibration abatement systems. Cyber attacks would have to target the classical computer or its user and then move to the interface unit before trying to breach the quantum computer.

A summary comparing classical and quantum computers is in Table 1.

Classical vs Quantum Computers		
Feature	Classical Computer	Quantum Computer
Computing units	Bits	Qubits
Computing Power	Linear increase with number of transistors	Exponential increase with number of qubits
Logic Type	Binary Logic	States of spin on atoms
Targets	General Problems	Optimization, Data Analysis, Simulations
Operation size	1 per N bits	2^N for N qubits
Security	Attacks directly and indirectly to multiple aspects of the system.	Currently physical. Social engineering and electronic attacks targeting the cooling system.
Temperature	Room	Super cooled

Table 1. Comparison of Classical and Quantum Computers.

ADVANTAGES AND DISADVANTAGES OF QUANTUM COMPUTING

Some of the advantages of quantum computers include:

- Speed - Quantum computers are fast. They allow solving some problems in considerably less time than presently available classical machines. In general, a quantum machine runs faster than a classical machine due to its architecture. Quantum computers can run large-scale data problems faster than classical computers. However, the problem of cooling restricts how long a quantum computer can run. Most quantum computers take a long time to cool down enough to run again.[40]

- **Solving New Problems** - Quantum computers can solve problems not solvable by classical machines. Quantum computers open classes of problems that cannot be effectively represented and calculated using the binary approach. Drawing a similarity to mechanical engines, the mathematics and implementation of the V-8 and the rotary engine both generate power, but the method of generation is different. They perform the same function but in different ways. Among the complex problems is the ability to break asymmetrical key ciphers which are presently used for the protection of data.
- **Enhancing Classical Computers** - Quantum computers are complementary to classical computers. Both types of computers are useful for different problems and can be used together.
- **Memory Density** - Entangled qudits can represent problems that cannot be represented in the binary computational space. Entangled qudits have more than two states. Instead of rising linearly, like the information in classical memories, qudits rise exponentially. It only takes a relatively few qubits and even fewer qudits to perform complex algorithms that exceed the capability of conventional computers.[41]
- **Novel Approaches to Problems** - Quantum computers allow for a new way to view problems. Because of their new technology, new approaches to solving problems are needed and becoming available. Progress takes place when new ways to view a problem present themselves.

There are also aspects of quantum computers that are not advantages. Some of these disadvantages may be overcome with time, others are inherent to the technology. These disadvantages include:

- **Need for Supercooling** - Qubits that presently make up quantum computers require temperatures near absolute zero. Such a temperature is extremely hard to generate and maintain. Although some progress in this area was made with the photonic quantum chip and light absorbing metal-ion qubit, the need for extreme cold is still a significant problem with quantum computing today.
- **Costs** - Supercooling requires specialized equipment and power to maintain the computer’s required operational environment. Supercooling coupled with the use of exotic materials to construct the various qubits, processors, and interfaces make quantum computing a very costly venture. This problem will probably be moderated as room temperature qubits are developed, but the time until that improvement is likely ten or more years from now.
- **Thermal Errors** - Just running a quantum machine can cause thermal errors to be present in the results of calculations. The problem is solved by quantum annealing,

but will require connecting multiple hardware qubits to act as a single, logical qubit and additional qubits will be needed to monitor the behavior of the ones holding the data and make the necessary corrections.[42] Multiple runs of the same problem are required to correlate the output and decide on the correct solution, each run will also generate heat, potentially causing more thermal errors.

- **Decoherence** – Decoherence is the process in which the environment interacts with qubits, often causing uncontrollable changes to their quantum states and information to be lost.[43] Since qubits interact with the environment, they are affected by it. Changing magnetic and electric fields, radiation, other qubits, seismic activity, and physical movement can all cause decoherence.
- **Not Generally Available** - At this time, there are few quantum computers. Lack of supply of these units makes them harder to employ and limits access to the resource. The development of capabilities that can link multiple quantum computers together may help alleviate the shortage of materials needed to make a general purpose quantum computer.
- **Lack of Trained Users** - As with newer technologies, the number of trained users is limited. Few experts exist to design, develop, and operate the machines. The lack of specialists in this area means the cost of training and employing such trained personnel is high.
- **Standardization** - Quantum computers are early in their development timeline. Many solutions for the problems and implementation are being tried. There is little standardization for the designs or methodology, contributing to the confusion in the selection and implementation of quantum computers.

Quantum computing adds a new dimension to computing. It can speed up programming and provide new insight into information and data problems. However, it does not change information theory[44] and communications theory[45] but rather does things in a new way. It will provide a great deal of innovation in those fields as the technology matures. While there seems to be tension between classical and quantum computers, the two are complementary in functionality. An easy way to think of the differences between classical and quantum computers is that classical computers excel at discrete math (such as algebra and trigonometry) while quantum computers do a much better job of continuous mathematics (such as calculus-based problems). Many experts feel that the future of computing holds hybrid computing systems.[46] Both classical and quantum computers will exist in the same machine with a preprocessor that selects which unit is best suited to solve the problem presented to the computer. However, this solution is probably not practical in the short term due to the problems with supercooling and the need for a unified programming language solution.

THE IMPACTS OF QUANTUM COMPUTING ON DATA

The infrastructure of information and information processing in the U.S. is primarily that of classical computing. There are over 1 trillion (10^{12}) classical computing devices in use as of 2023 and more than 2 billion (2×10^9) personal computers.[47] In contrast, as of early 2023, there were less than 120 quantum computers in operation worldwide.[48] Part of the reason for the number disparity is that quantum computers are continuing to evolve. However, quantum sensors are already in widespread use and their use is expected to increase significantly as new ecosystems for data collection are formed from observing what used to be unobservable and training new AI models.[49] The numbers suggest QIS will have a significant impact on data and data analytics for our Army. Below we will discuss two areas that will have the most significant impacts to the Army: quantum sensing and quantum computing, the latter of which includes post quantum encryption.

Quantum Sensing Technologies

Quantum sensing applications are the most mature of the QIS technologies being developed for use in the DoD.[50] Quantum sensing technologies use trapped ions, solid-state spins, superconducting circuits, and quantum dots[51] to provide sensing capabilities across several physical environments including magnetic and electric fields, the forces of acceleration, pressure, gravity, and time.[52] The combinations of these sensing capabilities enable quantum sensors to collect data and conduct analysis that will enable us to see the previously unobservable, including undersea, underground, and in space.

While sonar is widely used for the detection of objects in deep water, in shallower depths sonar can become affected by echoes off of the seabed or shoreline.[53] Magnetic detection can discriminate magnetic objects from non-magnetic objects. Arrays of quantum sensors called atomic magnetometers have successfully detected 100% of single and multiple targets in both saline water and air, and precisely located over 93% of the objects, to include tracking of moving targets.[54] In the vast expanses of the Pacific Ocean, the application of quantum sensors to detect vessels deliberately evading satellite imagery and sonar would enable the U.S. and our allies to detect Chinese movements toward disputed waters and territories or the deployment of autonomous vessels, underwater drones, unmanned underwater vehicles,[55] or mines.

Rydberg atom electric field sensors can be used for ultra-wideband spectrum sensing and communications and high-accuracy near-field sensing.[56] Rydberg electrometry uses atoms to observe electric fields and is considered a path to accessing large operational bandwidths with one device without an array of antennas[57] paving the way for small form factor radios with autonomous hopping between multiple bands and expanding use of the electromagnetic spectrum to include frequencies higher than the 100 GHz achieved by conventional electronics.[58]

Inertial navigation systems leverage quantum sensors to measure rates of acceleration and rotation of moving objects, such as a missile, airplane, or ship, to determine its position and orientation. They are widely used for navigation in GPS-denied environments and the more advanced systems use sophisticated algorithms and data fusion techniques to filter out the effects of jamming and improve resiliency.[59] Russia's Iskander short range ballistic missile, responsible for numerous deadly attacks on Ukraine in 2023 and 2024, owes its unprecedented accuracy to its inertial navigation system.[60]

Quantum sensors for timing include both microwave and optical atomic clocks for use in GPS-denied timing, secure communications, and sensing requiring synchronized distributed sensor nodes such as radar and reflectometry.[61] Quantum based atomic clocks do not rely on satellite connectivity to operate, mitigating the risk posed by electronic jamming or GPS signal spoofing. Microwave atomic clocks have applications in communications networks, GPS, and long baseline interferometry,[62] used in measuring microscopic displacements and surface irregularities. Optical atomic clocks are used in GPS-denied navigation, distributed sensing (e.g. synthetic aperture radar), international time-keeping, and geodesy.[63]

These four quantum sensing applications, magnetic fields, electric fields, force, and time come with exponential data storage demands and algorithms. Increased applications with intelligence, surveillance and reconnaissance (ISR) and precision, navigation and timing (PNT) will enable navigation in GPS-denied environments and enable us to see in maritime and underground environments.[64] Both our allies and our adversaries will use quantum sensors to collect data on all the places military forces used to hide, whether that be camouflage to blend in with the environment, a safe house for special forces missions, the tunnels under Gaza, or in the expanses of the ocean. There will be an increased need for data storage, but more importantly, we will need people who are capable of leveraging this technology, developing the algorithms to make sense of it, and designing a new way to fight in an environment where we can no longer hide.

Quantum Communications

Quantum communications will have a significant impact on data security through quantum key distribution. It also includes the ability to network quantum computers and sensors together. In this section we will discuss one of the largest threats quantum computing poses to our national defense: the ability to render current industry PKE standard encryptions useless. Currently, two types of encryptions are considered extremely strong:

1. Advanced Encryption Standard (AES), especially when wrapped in randomizing modes such as Cipher Block Chaining (CBC). AES is a block product cipher in which the plain text is encrypted 14 times with randomized input data.[65] This is meant to mix up the ciphers so no one can follow the changing data during encryption.

2. Asymmetric key public key encryption (PKE) algorithms require two keys. The idea is that if one key is hard to break then two keys are much harder and as a result data is safer. However, one of the keys is publicly revealed, so the use of the additional key is inconsequential.

This leads to the application of Shor's algorithm in using quantum computers to break PKE ciphers.

Shor's algorithm[66] demonstrates that algorithms such as the Rivest–Shamir–Adleman (RSA) cipher[67] and Diffie-Helman[68] "secure" key exchange can be broken easily. Each of these algorithms is based on "hard"[69] ciphers built on the discrete logarithm, prime and semi-prime factorization, or Euler's totient function. These problems have not been broken by a classical computer. It is believed Shor's quantum algorithm will allow large-scale quantum computers to break these asymmetric key algorithms rendering internet traffic unsecure.[70]

Grover's algorithm,[71] a quantum algorithm for unstructured search, shows that it is possible to reduce the effectiveness of one key ciphers, like AES-256, by reducing the time to brute force symmetric algorithms by an average time and effort of a factor of 2, meaning a 256-bit key would take roughly 2^{128} iterations to crack. Further research showing attack methods on AES-256 with bolted on randomization functions[72] show this too is able to be cracked. AES has been shown, through isomorphic cipher reduction,[73] to reduce to a block substitution (S) cipher. Isomorphic cipher reduction allows mapping from one cipher to another. Even when protected by the CBC mode, a side-channel attack on parts of the hardware or surrounding software can return the original text and bypass AES.[74] Even without these outside attacks, analysis of AES in the quantum environment has resulted in an estimate that even AES-128 cannot be defeated in approximately 100 trillion years using a classical computer.[75] Smaller numbers of possible keys (known as "key spaces") than available for AES can be defeated in a matter of seconds or minutes. AES can be a component of the cryptographic solution but is not the sole answer to encryption in the post quantum environment (PQE). Symmetric key algorithms can be used in the PQE successfully and should be considered if the principles of Information Theory are properly followed.

Quantum computers will be able to break PKE-protected messages and our adversaries are preparing for that time. Both China and Russia are now implementing the Harvest Now Decrypt Later (HNDL) Attack,[76] where they collect and store encrypted data that cannot yet be decrypted and store them for a later time when quantum machines are capable of that decryption. The harvesters know that most data will not be valuable or helpful, but they hope that an occasional message will contain vital and important data that they can use.

Much of the information used in daily life is time sensitive, meaning it often loses value over time. While some users believe their data should be kept secret forever,[77] the goal of cryptography is to obscure information from an adversary until that information no longer holds value if revealed. For example, intelligence about upcoming an attack has great value, however, once the attack begins that information loses value. It becomes part of the lessons learned and is often shared with the cyber security community. The longer the data remains encrypted and hidden, the more likely the value of that data will decrease to the point that it becomes useless.

In 2022, NIST and NSA named four algorithms they consider "quantum resistant" meaning they can run on computers today and are believed to be resistant to attacks from both classical and quantum computers: Crystals-Kyber, Crystals-Dilithium, Falcon and SPHINCS+.[78] Unfortunately, all four selections have now been proven vulnerable and cannot be considered safe. Researchers from North Carolina State University were the first to present vulnerabilities in the Falcon algorithm.[79] The SPINCS+ algorithm was shown to be vulnerable to a forgery attack in September of 2022.[80] Researchers in Stockholm used recursive trained artificial intelligence combined with a side-channel attack to crack the CRYSTALS-Kyber algorithm in February of 2023.[81] In April 2024, the Dilithium based algorithms was also cracked using a side-channel attack.[82]

In May 2024, a quantum-resistant algorithm using polymorphic encryption that incorporates sharding was presented at the IEEE Artificial Intelligence IoTConfernce.[83] In this encryption method, messages are broken into shards and each shard must be independently broken. Revealing one shard does not provide clues for other shards, effectively breaking the relationship between different portions of the message. Polymorphic ciphers change the combination of ciphers and keys used independently from each other, in frequent, but irregular intervals. Changes to the cipher/key pairs are made often so the data needed for decryption cannot accumulate.

Recent advances in using these algorithms show promise, but have not yet been sufficiently studied to allow for full acceptance. In May 2024, Anne Neuberger announced that NIST expects to release four new post quantum algorithms as early as July.[84] It will take the collective efforts of academia and the government to develop the algorithms needed to protect our nation's data in the post quantum world.

CONCLUSION

Operationally deploying quantum capabilities in the future will provide positions of advantage in seeing formerly unseen areas of our environment undersea, underground, behind walls, and under camouflage. Enabled by quantum sensors, both our allies and adversaries will collect intelligence at rates exponentially higher than seen today. Data harvesting of military, industry, economic, and personal data will also increase, even for encrypted data, as quantum computing will be able to decrypt today's most secure algorithms. Any data that may provide a position of advantage will be targeted.

Research in developing hybrid architectures such as the limited resources for quantum computing will likely cause independent research efforts to team together, creating powerful architectures for general purpose quantum computers. The processing speed of these quantum computers will enable simulations of large-scale military deployments to train our forces and train with our allies. This training should include the development of new techniques, tactics, and procedures that take into account the quantum sensors that will see their every move and the AI-enabled algorithms that will try to get inside the decision cycle of our commanders. Quantum technologies will cause the way we conduct war to evolve and adapt.

Commanders will have to not just leverage our quantum capabilities to attack, but more than ever develop defensive practices to counter adversary capabilities. Deception techniques will need to be developed to frustrate sensors that can see through smoke, weather, physical obstructions, and vegetation. Breaking up the visual outline of equipment is not enough. The magnetic/gravitational outline will also have to be obscured. Therefore, alternate means of camouflage must be developed and TTPs developed for employing both at home station and while deployed.

As we develop our quantum capabilities, an equal effort needs to be applied to countering these capabilities. Once a new capability is used in the open, our adversaries and industry rapidly copy it and leverage it for their use or commercial gain. But the near-term advantage will go to the nation state which fully embraces the development and application of quantum technologies, this is why our leaders must start to understand quantum technology and start thinking about how to apply it in the future operational environment.

Leaders will have to not just maneuver troops on the battlefield. Our Soldiers and their families are in a battle for their data every day. The harvesting of personal data for future use and for cognitive warfare is real and will grow with the advent of quantum capabilities, as will the targeting of critical infrastructure around our military bases. Attention should be placed on protecting our people from these threats.

Quantum sensors will not just be used for detecting military equipment and units, quantum sensors will enable the ability to target and track individuals via their heartbeat through a crowd. Detecting and identifying individual signatures allows for the finding, fixing, isolating, and targeting of specific soldiers, equipment, and high value targets, for both sides. It will be a commander's responsibility to balance the ability to exploit the data and intelligence gained by quantum sensors and computing while, simultaneously defending friendly assets from collection and exploitation by our adversaries.

Quantum sensors, computing, and communications will provide advantages for precision fires in the near term, but it will also make our adversaries more lethal as seen in the Russian use of the Iskander missile in Ukraine. Attention should be also given to the electromagnetic spectrum. As quantum communications enable the ability to leverage more of the EMS for our secure communications via Rydberg electrometry and QKD, quantum will also enable the detection of faint changes in the EMS to pinpoint radios and the people using them for communications. The EMS will become a battlespace that must be fully integrated into plans and operations across the continuum of military operations.

The technology race to harness the power of the qubits and qudits will not just revolutionize the battlefield, it will also render the PKE encryption that protects communications over the internet useless. This will affect everything that enables our economy and critical infrastructure to operate. Our leaders should both support and monitor the efforts of NIST and the NSA to develop secure quantum algorithms. While we recommend looking at polymorphic algorithms combined with a shard-based approach as a solution for quantum-proof encryption, there is much work to be done in this area.

Advances such as the Penning Trap, MIT's Fluxonium qubits connected by transmon, MIT and MITRE's efforts to create a "quantum-system-on-a-chip," and the development of the photonic quantum chip and light-absorbing metal-ion qubit are all steps toward overcoming the issues of scaling, coherence, and heat and show that a room temperature general purpose quantum computer will be developed in the next decade. The Army needs leaders who facilitate and support these research efforts and are prepared to leverage new capabilities in the future.

ACKNOWLEDGEMENT

The authors would like to thank MAJ James Armstrong, MAJ Anna White, MAJ Stephen Willson, and Deborah Karagosian for their guidance and feedback while writing this article.

DISCLAIMER

The views expressed in this work are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

1. English Heritage Website, "D-Day Deception: Operation Fortitude South," (accessed May 22, 2024). https://www.english-heritage.org.uk/visit/places/dover-castle/history-and-stories/d-day-deception.
2. Klein, Christopher, "Fooling Hitler: The Elaborate Ruse Behind D-Day, (accessed on May 20, 2024). *History Channel Online*, https://www.history.com/news/fooling-hitler-the-elaborate-ruse-behind-d-day.
3. N. Chandra and S. Parida. "Quantum Entanglement in Photon-induced Electron Spectroscopy of Atoms and Molecules: Its Generation, Characterization, and Applications," (2016). *Advances in Imaging and Electron Physics, vol. 196*, Elsevoir, https://www.sciencedirect.com/science/article/abs/pii/S1076567016300404, 1–164.
4. Matt Swayne, "20 Top Universities for Quantum Computing Research," (May 21, 2024). *The Quantum Insider.* https://thequantuminsider.com/2024/05/21/20-top-universities-for-quantum-computing-research/.
5. Sylvain Duranton, "Quantum Computing Takes Off with $55 Billion in Global Investments," (June 26, 2024). Forbes, https://www.forbes.com/sites/sylvainduranton/2024/06/26/quantum-now/.
6. Hrithik Saini, "8 Strongest Data Encryption Algorithms in Cryptography," (March 10, 2022). *Analytic Steps Online*, https://www.analyticssteps.com/blogs/8-strongest-data-encryption-algorithms-cryptography.
7. The White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems." (May 4, 2022) Technical report, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/, sec. 1, para, b.
8. Stephen Ornes, "Inside the Quest for Unbreakable Encryption." (October 19, 2023). *MIT Technology Review*, https://www.technologyreview.com/2023/10/19/1081389/unbreakable-encryption-quantum-computers-cryptography-math-problems/.
9. Nicholas Ho, "Why Quantum Computers Resemble Chandeliers?." (accessed June 8, 2024). *Quantum Computing Vulnerabilities are Everywhere Project*, https://qcve.org/blog/why-quantum-computers-resemble-chandeliers.
10. Jeff Hecht, "Quantum Science: The Quest for Quantum Information Technology Expands," (July 14, 2020) *Laser Focus World*, https://www.laserfocusworld.com/lasers-sources/article/14176179/quantum-science-the-quest-for-quantum-information-technology-expands.
11. Li-Heng Chang, Shea Roccaforte, Rose, Xu, and Paul Cadden-Zimansky. "Geometric Visualizations of Single and Entangled Qubits." (December 7, 2022). *Cornell University Quantum Physics Repository Online*, https://arxiv.org/abs/2212.03448, p 11.
12. Yuchen Wang, Zixuan Hu, Barry C. Sanders, Sabre and Kais, "Qudits and High-Dimensional Quantum Computing," (2020). *Frontiers in Physics, vol. 8*, https://www.frontiersin.org/articles/10.3389/fphy.2020.589504.
13. R. Whitney Johnson, Kamyar Maserrat, and Jihwang Yeo, "The Basics: How Quantum Computers Work and Where the Technology is Heading," (May 23, 2024). Wahington, D.C.: Foley and Lardner LLP, https://www.foley.com/insights/publications/2024/05/basics-how-quantum-computers-work-where-technology-heading/.
14. Gopala Krishna Behara, "Overview of Quantum Computer Platform," (September 12, 2021). *Analytics Insights*, https://www.analyticsinsight.net/latest-news/overview-of-quantum-computer-platform.
15. Evan Brown, "The Devil in the Details: A Survey of Current Approaches to Building a Quantum Computer." (December 18, 2023). *Center for Strategic and International Studies*, https://www.csis.org/blogs/strategic-technologies-blog/devil-details-survey-current-approaches-building-quantum-computer.
16. Will Fox, "New Record Length for Quantum Coherence," (September 18, 2023). *Timeline.net*, http://futuretimeline.net/blog/2023/09/18-record-length-for-quantum-coherence.htm.
17. Josh Schneider and Ian Smalley, "What is a Qubit?" (February 28, 2024). *IBM Think*, https://www.ibm.com/topics/qubit.
18. He Liang Huang,Dacao Wu, Daojin Fan, and Xiabao Zhu, "Superconducting Quantum Computing: A Review," (November 3, 2020), https://www.researchgate.net/publication/342380016_Superconducting_Quantum_Computing_A_Review, 2.
19. Adam Zewe, "New Qubit Circuit Enables Quantum Operations with Higher Accuracy," (September 25, 2023). *MIT News*, https://news.mit.edu/2023/new-qubit-circuit-enables-quantum-operations-higher-accuracy-0925
20. James Dargan, "Fluxonium Qubits Bring the Creation of a Quantum Computer Closer," (November 22, 2022). *The Quantum Insider*, https://thequantuminsider.com/2022/11/22/fluxonium-qubits-bring-the-creation-of-a-quantum-computer-closer/.

NOTES

21. Colin D. Bruzewicz, John Chiaverini, Robert McConnell, and Jeremy M. Sage, “Trapped-Ion Quantum Computing: Progress and Challenges,” (April 9, 2019). *Massachusetts Institute of Technology, Lincoln Laboratory,* https://arxiv.org/pdf/1904.04178, 3.
22. Oliver Morsch, “A New Ion Trap for Larger Quantum Computers,” (March 13, 2024), *Physics*. https://phys.org/news/2024-03-ion-larger-quantum.html.
23. Shreyans Jain, Tobias Sagesser, Pavel Hrmo, Celeste Torkzaban, Martin Stadler, et al, (March 13, 2024). *Nature, vol. 627,* https://www.nature.com/articles/s41586-024-07111-x, 510.
24. Jain, et al., “Penning Micro-trapo for Quantum Computing,” 513.
25. Dexter Johnson, “The Road to a Quantum Computer Begins with a Quantum Dot,” (May 25, 2020). *IEEE Spectrum*, https://spectrum.ieee.org/the-road-to-a-quantum-computer-begins-with-a-quantum-dot.

26 John Timmer, “Quantum Computing Progress: Higher Temps, Better Error Correction,” (March 27, 2024). *ARS Technica*, https://arstechnica.com/science/2024/03/quantum-computing-progress-higher-temps-better-error-correction/.

27. Linsen Li, Lorenzo DeSantis, Isaac B. W. Harris, Kevin C. Chen, et al. “Heterogeneous Integration of Spin–photon Interfaces with a CMOS Platform,” (May 29, 2024). *Nature Communications*, https://www.nature.com/articles/s41586-024-07371-7.
28. Adam Zewe, “Modular Scalable Hardware Architecture for a Quantum Computer,” (May 29, 2024). *MIT News*, https://news.mit.edu/2024/modular-scalable-hardware-architecture-quantum-computer-0529.
29. Schneider and Smalley, “What is a Qubit?”.
30. Jhuria, K., Ivanov, V., Polley, D. et al. “Programmable Quantum Emitter Formation in Silicon. (May 27, 2024) *Nature Communications*, https://doi.org/10.1038/s41467-024-48714-2.
31. Charles Q. Choi, “In the Race to Hundreds of Qubits, Photons May Have Quantum Advantage," (March 5, 2021). *IEEE Spectrum*, https://spectrum.ieee.org/race-to-hundreds-of-photonic-qubits-xanadu-scalable-photon.
32. Kyushu University. "Generating Stable Qubits at Room Temperature." (January 11, 2024). *Science Daily*. www.sciencedaily.com/releases/2024/01/240111113125.htm.
33. Stefan Krastanov, Mikkel Heuck, Jeffrey H. Shapiro, and Dirk R. Englund, “Room-temperature Photonic Logical Qubits via Second-order Nonlinearities,” (January 8, 2021). *Nature Communications, Vol. No. 12, 191*. https://doi.org/10.1038/s41467-020-20417-4.
34. Donna Lu. “What is a Quantum Computer?” (accessed May 19, 2024). *New Scientist*, https://www.newscientist.com/question/what-is-a-quantum-computer.
35. Yuchen Wang, Zixuan Hu, Barry C. Sanders, and Sabre Kais, “Qudits and High-Dimensional Quantum Computing.” (November 2020). *Frontiers in Physics, vol. 8,* https://www.frontiersin.org/articles/10.3389/fphy.2020.589504.
36. Charles Q. Choi, “Qudit Computers Go Beyond Ones and Zeroes,” (August 1, 2022), *IEEE Spectrum*, https://spectrum.ieee.org/qudit.
37. California Institute of Technology, “What is Entanglement and Why is it Important?” (accessed February 24, 2024). *Caltech Science Exchange Online,* https://scienceexchange.caltech.edu/topics/quantum-science-explained/entanglement.
38. California Institute of Technology, “What is Entanglement and Why is it Important?” (accessed June 28, 2024)
39. Lakshmi Chandrasekaran, “Physicists Finally Find a Problem That Only Quantum Computers Can Do,” (March 12, 2024). *Quanta Magazine*, https://www.quantamagazine.org/physicists-finally-find-a-problem-only-quantum-computers-can-do-20240312/.
40. Lindsey Valich, “A Quantum Leap in Cooling Atoms for Better Computers.” (September 12, 2023). *University of Rochester*. https://www.rochester.edu/newscenter/quantum-mechanics-thermoelectricity-superposition-entanglement-565852.
41. Glenn Roberts, Jr., “Going Beyond Qubits: New Study Demonstrates Key Components for a Quitrit-Based Quantum Computer,” (April 26., 2021). *University of California, Lawrence Berkeley National Laboratory*, https://newscenter.lbl.gov/2021/04/26/going-beyond-quibits/.
42. John Timmer, “Quantum Computing Progress: Higher Temps, Better Error Correction, (March 27, 2024). *ARS Technica*, https://arstechnica.com/science/2024/03/quantum-computing-progress-higher-temps-better-error-correction/.
43. Katherine McCormick, “Decoherence Is a Problem for Quantum Computing, but...”, (March 30, 2020). *Scientific American*, https://www.scientificamerican.com/blog/observations/decoherence-is-a-problem-for-quantum-computing-but/.

NOTES

44. Claude E. Shannon, “A Mathematical Theory of Communication.” (1948) *Bell System Technical Journal,* 27; Wang, et al., “Qudits and High-Dimensional Quantum Computing;”.
45. Thomas Cover and Joy Thomas, *Elements of Information Theory*, (2005). New York: John Wiley & Sons, Inc, 2nd edition.
46. Peter Chapman and Pat Tang, “What is Hybrid Quantum Computing? (January 18, 2024) https://ionq.com/resources/what-is-hybrid-quantum-computing.
47. Richard Taylor, “How many computers are there in the world?” (accessed June 22, 2024). Quora, https://www.quora.com/How-many-computers-are-there-in-the-world.
48. Campbell, Charlie, “Quantum Computers Could Solve Countless Problems—And Create a Lot of New Ones.” (January 26, 2023), *Time Magazine*, https://time.com/6249784/quantum-computing-revolution/.
49. Yannick Bormuth, Martina Gschwendtner, Henning Soller, Amanda Stein, and Ronald Walsworth, “Quantum Sensing Can Already Make a Difference but Where?” (2024). *Journal of Information Management*, https://journalsojs3.fe.up.pt/index.php/jim/article/view/2578/848, 2.
50. U.S. Department of Defense, *Applications of Quantum Technologies*, (November 2019), Report, Defense Science Board, Office of the Under Secretary of Defense for Research and Engineering, 6.
51. David L. Chandler, “Quantum Sensor Can Detect Electromagnetic Signals of Any Frequency,” (June 21, 2022). *Massachusetts Institute of Technology, Lincoln Laboratory*, https://news.mit.edu/2022/quantum-sensor-frequency-0621.
52. Bormuth, et al., “Quantum Sensing Can Already Make a Difference but Where?,” 3.
53. Tim Wogan, “Atomic Magnetometers Detect Underwater Objects,” (April 18, 2018). *Physics World*, https://physicsworld.com/a/atomic-magnetometers-detect-underwater-objects/.
54. Cameron Deans, Luca Marmugi, and Ferruccio Renzoni, “Active Underwater Detection with an Array of Atomic Magnetometers,” (March 22, 2018). *Applied Optics, Vol. 57, No. 10*, Optica Publishing, https://opg.optica.org/ao/fulltext.cfm?uri=ao-57-10-2346&id=383870, 2346.
55. Zubeda Anjum Niazi, “Future of Maritime Security: Navigating Complex Waters in the Indo-Pacific,” (March 1, 2024). *Journal of Indo-Pacific Affairs*, https://media.defense.gov/2024/Mar/11/2003410990/-1/-1/1/FEATURE%20-%20NIAZI.PDF/FEATURE%20-%20NIAZI.PDF, 132.
56. David Anderson, Rachel Sapiro and Georg Raithel, "A Self-Calibrated SI-Traceable Rydberg Atom-Based Radio Frequency Electric Field Probe and Measurement Instrument," (September 2021). *IEEE Transactions on Antenna Propagation, vol. 69, no. 9*, https://ieeexplore.ieee.org/document/9363580, 5931-5941.
57. John Keller, “ColdQuanta Eyes Quantum Applications in Electronic Warfare (EW), Sensors, and Anti-submarine Warfare (ASW),” (April 14, 2021). *Military and Aerospace Electronics Magazine*, https://www.militaryaerospace.com/computers/article/14201305/quantum-sensors-electronic-warfare-ew.
58. Eun Oh, Maxwell Gregoire, Adam Black, et al., “A Perspective on Quantum Sensors from Basic Research to Commercial Applications,” (June 2024), *Army Research Laboratory,* https://arxiv.org/pdf/2407.00689, 12.
59. James Marinero, “Inertial Navigation – What is It, How Does It Work?” (May 7, 2024). *Medium,* https://medium.com/the-dock-on-the-bay/inertial-navigation-what-is-it-how-does-it-work-4fe11601943d.
60. Josh Holder and Constant Meheut, “Facing and Endless Barrage, Ukraine’s Air Defenses are Withering,” (May 13, 2024). The New York Times, https://www.nytimes.com/interactive/2024/05/13/world/europe/ukraine-missile-defenses.html; Deagal, “Iskander Capability Overview,” (August 15, 2023), https://deagel.com/Weapons/Iskander/a001012.
61. Nurettin Sevi, “Quantum Technology in the Defence: A Paradigm Shift,” (October 23, 2023). *Defense Domain*, https://defensedomain.com/quantum-technology-in-the-defence-a-paradigm-shift.
62. U.S. Department of Defense, *Applications of Quantum Technologies*, 22.
63. Joe Kinast, “Prospects and Priorities for Emerging Quantum Sensors,” (September 2022), *Quantum Economic Development Consortium*, https://quantumconsortium.org/sensing22, 10.
64. U.S. Government Accounting Office, “Defense Navigation Capabilities: DoD is Developing Position, Navigation, and Timing to Complement GPS,” (May 10, 2021). Report. https://www.gao.gov/products/gao-21-320sp.
65. Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C,* (1996). New York: John Wiley and Sons Inc., 2nd Edition.

NOTES

66. Peter W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.” (August 4, 2006) *Society for Indistrial and Applied Mathematics Review*, Volume 41, https://inspirehep.net/literature/2743879, 303-331.
67. Richard Chirgwin. “Quantum Computers Won’t Break RSA Encryption Anytime Soon,” (January 25, 2023). *IT News Online*, https://www.itnews.com.au/news/ quantum-computers-wont-break-rsa-encryption-any-time-soon-590115.
68. Whitfield Diffie and Martin Hellman, “New Directions in Cryptography.” (November 1976). *IEEE Transactions on Information Theory, Vol. 22, No. 6*, https://ieeexplore.ieee.org/document/1055638, 644 – 654.
69. Jose Balcazar, Josep Diaz, and Joachin Gabarro. *Structural Complexity I.* (1998). New York: Springer-Verlag.
70. Edward Parker, “When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret,” (September 13, 2024). *Lawfare*, https://www.lawfaremedia.org/article/when-a-quantum-computer-is-able-to-break-our-encryption-it-won-t-be-a-secret.
71. Lov K. Grover, “A Fast Quantum Mechanical Algorithm for Database Search.” (July 1, 1996). *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Association for Computing Machinery*, New York, 212–219.
72. Albert Carlson, Bhaskar Ghosh, and Indira K. Dutta. “Using the Collision Attack for Breaking Cryptographic Modes.” (October 2022) *IEEE 13th International Congress on Computing, Communication, and Networking Technologies (ICCCNT).* Kharagpur, India. https://ieeexplore.ieee.org/document/9984325, 1-7; David McGrew. “Impossible Plaintext Cryptanalysis and Probable-plaintext Collision Attacks of 64-bit Block Cipher Modes.” (March 2013). *Proceedings of the Fast Software Encryption Workshop*, Singapore, https://eprint.iacr.org/2012/623.
73. Bhaskar Ghosh, Indira Dutta, Shivanjali Khare, Albert Carlson, and Michael Totaro, “Isomorphic Cipher Reduction.” (October 2021). *IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, Canada, https://ieeexplore.ieee.org/document/9623135.
74. David McGrew, “Impossible Plaintext Cryptanalysis and Probable-plaintext Collision Attacks of 64-bit Block Cipher Modes;” and Bhaskar Ghosh, et al., “Isomorphic Cipher Reduction.”
75. Ron Franklin, “AES vs. RSA Encryption: What Are the Differences?” (November 14, 2022). *Precisely*, https://www.precisely.com/blog/data-security/aes-vs-rsa-encryption-differences.
76. Keyfactor. “Harvest Now, Decrypt Later: A New Form of Attack,” (April 29, 2024). https://www.keyfactor.com/blog/harvest-now-decrypt-later-a-new-form-of-attack/.
77. Ueli Maurer, “A Universal Test for Random Bit Generators,” (March 1, 1992). *Journal of Cryptography*, Vol. 5, No. 2, https://dl.acm.org/doi/10.5555/148544, 89-105.
78. Alexandra Kelley, “Federal Researchers are One Step Closer to Protecting U.S. Data from Quantum Computing Decryption Capabilities,” (July 5, 2022). *NextGov,* https://www.nextgov.com/cybersecurity/2022/07/nist-identifies-four-quantum-resistant-encryption-algorithms/368954
79. Emre Karabulut and Aydin Aysu, “Falcon Down: Breaking Falcon Post-Quantum Signature Scheme Through Side-Channel Attacks,” (December 5, 2021), *IEEE Design Automation Conference,* https://ieeexplore.ieee.org/document/9586131.
80. Ray Perliner, John Kelsey, and David Cooper, “Breaking Category Five SPHINCS+ with SHA-256,” (September 21, 2022). *International Conference on Post-Quantum Cryptography*, https://link.springer.com/chapter/10.1007/978-3-031-17234-2_23.
81. Kevin Townsend, “AI Helps Crack NIST-Recommended Post-Quantum Encryption Algorithm,” (February 21, 2023). *Security Week*, https://www.securityweek.com/ai-helps-crack-a-nist-recommended-post-quantum-encryption-algorithm.
82. Kalle Ngo, “Single-Trace Side-Channel Attacks on CRYSTALS-Dilithium,” (April 10, 2024). Presentation, T*he Fifth PQC Standardization Conference*, Rockville, MD: NIST, https://csrc.nist.gov/Presentations/2024/single-trace-side-channel-attacks.
83. Mandeep Singh and Albert Carlson, A., “Watermarking Using Polymorphic Algorithms for Increased Data Security,” (May 2024). *IEEE World AI IoT Congress (AIIoT)*, Seattle, WA.
84. Matt Swayne, “White House Advisor Says NIST To Release Post-Quantum Cryptographic Algorithms in Coming Weeks,” (May 24, 2024). *The Quantum Insider*, https://thequantuminsider.com/2024/05/24/white-house-advisor-says-nist-to-release-post-quantum-cryptographic-algorithms-in-coming-weeks/.