[ A. Carlson, H.C. Mumm, K.L. Sharkey, M.S. Watchorn. (Jul. 08, 2022). Quantum Chemistry for Detecting Cybersecurity Threats to Information Systems. Quantum Security Alliance (QSA). Reproduced for educational purposes only. Fair Use relied upon. ]

Quantum Security Alliance (QSA)

# Quantum Chemistry for Detecting Cybersecurity Threats to Information Systems

July 8, 2022

Authors

Dr. Albert Carlson, QSA Chair for Encryption & Entropy, Computer Science Dept., Austin Community College, Orchid: 0000-0002-0087-6066

Dr. Hans C. Mumm, QSA, Chair for Continuous Diagnostic and Monitoring, Victory Systems, LLC, Reuters Researcher ID: B-8496-2013

Dr. Keeper L. Sharkey, QSME, QSA, Chair for Quantum Applied Chemistry, ODE, L3C, Orchid: 0000-0002-3767-626

Dr. Merrick S. Watchorn, DMIST, QIS, QSA Program Chair

Editor Review

Michelle M. Watchorn, QSA Program Chair for Quantum Ethics

All rights reserved. All content on this document is protected by Quantum Security Alliance (QSA) copyrights and other protective laws.

## Executive Summary

The Quantum Security Alliance (QSA) was established in December 2018, and has been working rapidly to provide context to the emerging security landscape for Quantum Computing (QC). In the last several months of activity, the QSA has worked on numerous efforts including aiding the Cloud Security Alliance (CSA), Quantum Tech Congress, and the National Defense University (NDU) in building a working knowledge-sharing model that includes the University of Maryland, University of Phoenix, and Purdue Global Online University. "Cybersecurity methods are riddled with new technologies such as Artificial Intelligence (AI), Machine Learning (ML), Natural Language Processing (NLP) and Operational Technologies (OT, IoT, SCADA, CPS, etc.), cloud computing, blockchain and Quantum Information Systems (QIS)" (Watchorn, Bishop, Mumm & Brooks, 2022).

There is a national security risk in attempting to secure QC. We must begin to explore a new approach using chemical states as a security solution. Much is being discussed in the way of hybrid-computing systems; however, little is being discussed on how to secure these hybrid systems, and even less is being discussed about securing end-to-end quantum computers. This approach allows QC to be introduced into the national security arena with no cyber security risks, no supply chain issues, an increase in performance, and an increase in natural language abilities. The threat of unchecked technology and the ability to weaponize QC continue to evolve. Quantum solid-state memory advancements have offered more sophisticated capabilities with cost-effective designs resulting in a reduced entry-level for consumers, businesses, enemy states, and terrorist organizations. As a result, 'QC's reduced barrier to entry is now a national security risk. These issues are being discussed by the Congressional Research Service (CRS) as QC "could hold significant implications for the future of military sensing, encryption, and communications, as well as for congressional oversight, authorizations, and appropriations" (Gallo, 2021).

Due to the wide and increasing strategic applications of quantum chemistry (Q-Chem) in quantum technologies (QT) and chemical industries; it is important to introduce a mechanism of measure for cyber success at the federal level. This mechanism can be mapped to mathematical be explicitly correlated to non-Born-Oppenheimer-type Hamiltonians (NBO-H) which will require a Continuous Diagnostics and Mitigation (CDM) Program. Since Q-Chem states are described by a specific set of quantum numbers (Q-N), in theory, we can assign QIS to Zero Trust Models (ZTM) and Multi-Layer Security (MLS) by defining policies at the federal level to satisfy a comprehensive Quantum Cyber-Hamiltonian (Q-CH) framework. This can be accomplished by quantum virtualization of desired chemical states with Field Programmable Gate Arrays (FPGA) and by using the Quantum Logical Electrons and Nuclei (ODE, QLEAN™) methodology.

Keyword(s): Continuous Diagnostics and Mitigation; Quantum Information Systems; Quantum Computing; Quantum Chemistry; Quantum Security; Quantum Technology; Multi-Level Security; Quantum Cyber-Hamiltonian; Quantum as a Weapon; Field Programmable Gate Arrays, Zero Trust Model; Zero Trust Architecture

All rights reserved. All content on this document is protected by Quantum Security Alliance (QSA) copyrights and other protective laws.

## Background:

Since 2013, the United States and its Allies have endured a constant, sustained effort to reduce national security, resiliency, and confidence and undermine infrastructure found within Digital Warfare Strategies espoused by its enemies. This continuous strain has incurred a strategic financial, technical, and workforce debt not seen before in the cyber domain. Cloud computing enabled distributed computing at an economically affordable scale to commerce and the first integration of quantum and cloud with its success. When cyber adversaries have access to the power of quantum computing, our modern cryptographic systems based on public keys will not stand up to the test National Institute of Standard and Technology (NIST, 2021). The White House led an effort to establish the National Quantum Initiative Act (NQIA), which became Public Law 115-368 in 2018 with the goal of accelerating American leadership in QIS, chemistry, and technology (NTSP, 2021). This announcement was followed by the National Academies of Science, Engineering, and Medicine (NASEM) efforts to Identify Opportunities at the Interface of Chemistry and QIS (Goodson, 2022).

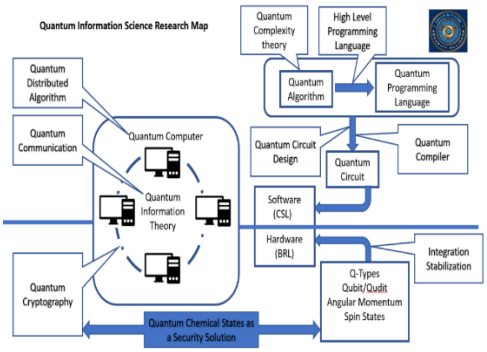


Figure 1: QIS Research Map identifying a new area of research: Q-Chem as a Security Solution that maps Q-Cryptography to Q-hardware (QSA, 2022).

Securing quantum computing will require a CDM Program that will support a dynamic approach to fortifying the cybersecurity of government networks and systems. Coupling this with the ability to explore emerging concepts such as the ZTM, and hybrid computing security controls models will enable a Digital Forensic Investigation (DFI) of an alleged cybersecurity breach to be documented and properly investigated. The proposed approach may be able to augment DFI using Quantum Chemical Encryption (QCE) for pedigree, lineage, and originality within a QIS. The stated goal of DFI is to support or refute a hypothesis of a given activity for both criminal and civil court standards of evidence collection. An area of exploration in quantum is light and solid memory allocations and their ability to influence:

- Microwave storage
- Light learning microwave conversion
- Orbital angular momentum
- Gradient Echo Memory
- Electromagnetically induced transparency
- In-Memory Computing (IMC)

All rights reserved. All content on this document is protected by Quantum Security Alliance (QSA) copyrights and other protective laws.

- Chemical memory allocation theories

Additionally, QIS is poised to fundamentally impact the way our national security institutions conduct business. Data protection, risk modeling, portfolio management, robotic process automation, digital labor, natural language processing, machine learning, auditing in the cloud, blockchain, quantum computing, and deep learning may look very different in a post-quantum world. Since 2013, the United States government has issued numerous guidelines, policies, and Executive Orders (EO) to begin building a post-quantum resistance environment required for resiliency: Improving Critical Infrastructure Cybersecurity (EO 13636, 2013), Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (EO 13800, 2017), Improving the Nation's Cybersecurity (EO 14028, 2021). These executive orders provide a roadmap for investment strategies for national research organizations tasked with implementation and execution. Using IMC will provide a high order of magnitude for memory efficiency (throttling) and enable MLS principles associated with ZTA as mandated by current federal regulations and standards. NIST states, "In zero trust, the network is always considered contested. A ZTA should be designed with the assumption that an attacker is present on the network and could observe/modify communications. Appropriate safeguards should be in place to protect the confidentiality and integrity of data in transit" (NIST SP 800-207, 2020).

**So how does the ZTA model and MLS standards align with the use of quantum chemistry?**

As early as 2019, FPGAs with quantum emulators were created (Pilch, 2019). FPGAs cannot efficiently emulate quantum algorithms on classical architectures, such that the weight of complexity can be moved from time to hardware resources. Quantum state on chip sent through FPGA to collapse chemical wave function space where the results are transmitted to another computer with an FPGA that can decode the collapsed function space and matches the counterpart chip on board. Thus, the FPGA collapse creates a mathematical form that can be calculated to a known, established good channel of logic that can be mapped to a cybersecurity functionality of operational security concepts encoded into the cyber-qubit. This would be like creating a new version of cypher-text using chemistry which validates the FPGA approach, which cannot be mutated to derive an answer that does not meet a logical assignment. This would aid in establishing the steady state of cyber resiliency and engineering principles created by NIST SP 800-160 Volumes 1 & 2. The QSA would posit the need to develop the Q-MLS qudit (Qu) concept to bring about a higher fidelity of transnational security ethos required to meet the emerging threat associated with national adversaries and nation-state actors (CNSSI, 1015).

**History of PKI**

Public key infrastructure (PKI) is a set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking, and confidential email. It is required for activities where simple passwords are an inadequate authentication method, and a more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred ("Public Key Infrastructure," 2022). PKI offers the ability to make key management much easier and was "invented in 1976 by two Stanford mathematicians, Whitfield Diffie and Martin Hellman. Their discovery can be phrased simply: enciphering schemes should be asymmetric" (Mann, 2002). Although the advent of computers was new, encrypted codes have been used throughout

history "Diffie and Hellman realized, that symmetry is the origin of the key-management problem. The solution is to have an encrypting key that is different from the decrypting key—one key to encipher a message, and another, different key to decipher it" (Mann, 2002). PKI related multi-dimensional maps/diagrams can be chemically influenced through a "Bravais" lattice-based access control (LBAC) policy by using an "i" number of Q-MLS and a "j" number of compartments which can be further treated as quantum mechanical lattices (Scholarpedia, 2020). NIST recently announced four post-quantum cryptography candidates for standardization; additionally, to candidates for a fourth round of analysis such as Crystals dilithium (Shi, 2020), which does not use quantum chemical information theory.

The exact timeframe of how long humans have been using codes and ciphers to protect secrets is unknown however the "first known examples are some clay tablets from Mesopotamia, created 3,500 years ago" (Cauche, 2018). To be historically accurate "Diffie and Hellman demonstrated only that public-key encryption was possible in theory. Another year passed before three MIT mathematicians—Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman—figured out a way to do it in the real world" (Mann, 2002). Historically, PKI is a mere blip of the 4,000-year history of cryptography, and we have many other "PKI schemes including Virtual Private Network (VPN), Identity Based Encryption (IBE), and Secure Shell (SSH) not discussed in this article" (Stapleton, 2012). PKI in its day was a breakthrough in secure communications, however in modern times, without updates to its concepts or hardening to its core abilities, PKI has been hacked many times over with drastic consequences. Completing a simple internet search offers the reader the ease with which PKI can be broken with such articles as "PKI Hacking for Fun and Profit" “How PKI was Used in the SolarWinds Orion Attack, or “Fast Russian Hackers and the End of PKI”…indeed with the speed of quantum computers new security protocols will be required, and the concept of PKI, while revolutionary in its time, may need to radically change to meet the needs of the hybrid computing models and the pure QC models.

Strengths and weaknesses-ZTMs are broken

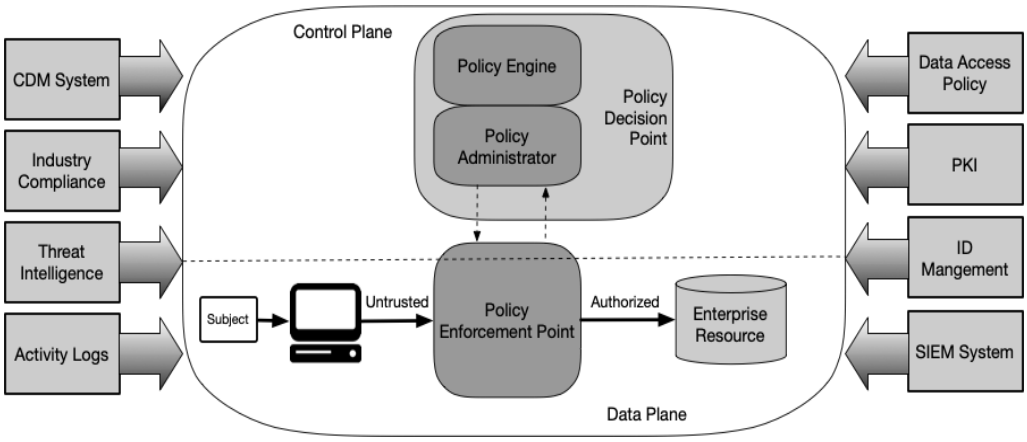


Figure 3: Core Zero Trust Logical Components: ("Public Key Infrastructure," 2022)

### Use of Quantum Annealing and Optimization for Approximation and Validation

The Sandia National Research Labs (SNRL) has built several evaluation criteria for QC testing and validation (QPL, 2019). The QSA proposes the use of these types of external validators to build a hybrid model for analysis and evaluation of the required control paradigms at each stage of dynamic quantum circuits (Q-CI). The use of the Control Paradigms by Stage (QPL, 2019) creates clearly articulated stages, which Figure 4, illustrates.

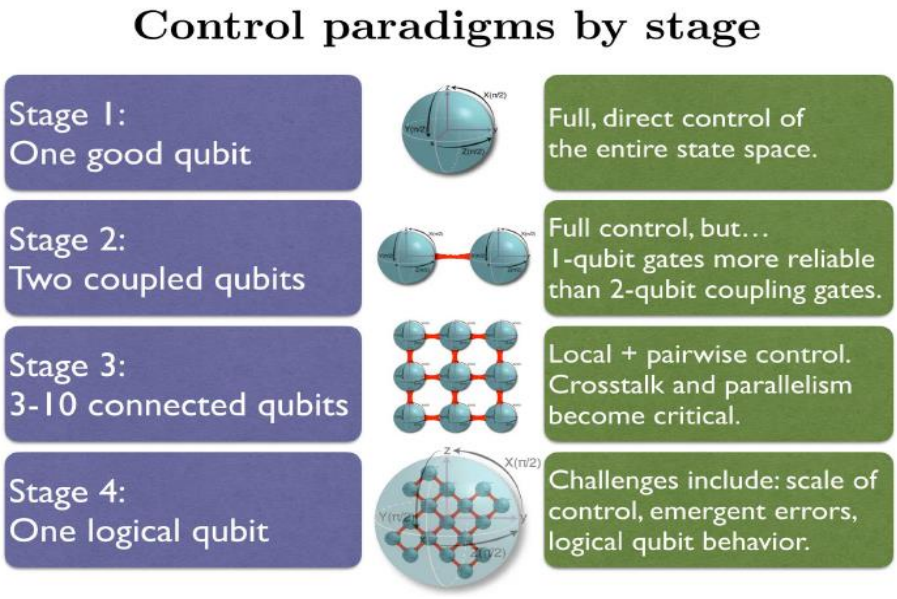


Figure 4: QPL Control Paradigms by Stage (2019).

The analysis of potential waveform frequencies may result in detecting additional noise within the signature of analysis and help to build stronger qubit processors that would provide a higher fidelity of localized polynomial scaling.

### Quantum as a Weapon (QaaW) System

Humankind has a history of weaponizing innocuous technologies and processes. Technology created for the betterment of our world is quickly altered for nefarious uses. A soybean growth enhancer became Agent Orange, the dream of human flight became the preferred method for bomb delivery, and the dream of space travel has now been turned into the next war zone. Consider that Google Earth offered an incredible free tool for humans to use to learn and explore, and sadly the technology is being used for murders “where the victims' homes or neighborhoods were scoped out on Google Earth before attacks, most infamously in the 2008 Mumbai terror attacks, where it was found that the terrorists used Google Earth to plan the attacks” (Zak, 2016).

One must recognize that quantum computing will suffer the same historical fate. Quantum computing will be advanced with an eye toward use in war, crime, and other evil applications long before it becomes centered on positive applications of allowing drug therapies to be created in a fraction of the traditional time or studying the mysteries of the universe. This inevitability of insecurity and misuse does not need to occur as with any new

technology; it is "neither infused with ethics nor bereft of them; it requires guidance. If augmented by ethical considerations, the hope is this invention will serve the public good and be profitable; if not, the outcome could be ambiguous at best, and devastating at worst" (Al Hussein, 2019).

Classical computers have proven to be a boon to society, enabling a wide variety of extensions to exist technologies and creating many new beneficial inventions and technologies. It did not take long for attackers and opportunists to find applications to enrich themselves or advance their causes/national interests using computers. The increased capabilities of computers were quickly applied to conventional warfare systems, decreasing response time, and increasing weapon efficiencies. Applying the obvious parallels between classical and quantum computers; it is certain that the same course of events will happen in the PQE.

The weaponization of quantum will occur and will "introduce new capabilities, improving effectiveness and increasing precision, thus leading to 'quantum warfare' (QW), wherein new military strategies, doctrines, policies, and ethics should be established" (Krelina, 2021). QW (see Figure 5) offers unique environments and issues that will "affect intelligence, security, and defense capabilities of all warfare domains, and its ushers in new military strategies, doctrines, scenarios, and peace as well as ethics issues" and with it the era of the quantum attach defined as "quantum attack, which refers to using quantum technologies to break, disrupt or eavesdrop on either classical or quantum security systems" (Krelina, 2021). Social media was intended to be a uniting force for families and the world, sadly it has been weaponized against governments, political candidates, religions, and even individuals. Social media has been weaponized to the point that it has been linked to suicides, homicides, crime, and the glorification of gangs and crime sprees.


Figure 5: Sketch of quantum warfare utilizing various quantum technology systems (Krelina, 2021)

The beloved internet is an obvious example of technology meant for good being weaponized for evil purposes. The Internet of Things (IOT) was meant to enhance and automate our lives for a more positive life experience, however "In December 2014, over 750,000 Wi-Fi devices - including TVs, media servers and of course a fridge - were hacked and turned into botnets, sending out millions of spam e-mails". Spam e-mail is minor issue when you consider the hacks against "smart' webcams, baby monitors and security cameras… Last year, a Russian site

appeared showing live footage from over 70,000 hacked cameras in peoples' homes as a way of demonstrating how insecure devices" can be (Zak, 2016).

> This theme is continued as QC can make conventional nuclear warfare obsolete. Nuclear weapons are tangible objects, that is a bomber, a submarine, or an ICBM that can be destroyed by conventional weapons. They can also be detected by radar, sonar, and satellite pictures. QC has no such properties of detection [and does not have a physical infrastructure, QSA, 2022]. A QC infrastructure cannot be destroyed by conventional means, but by breaking encryption codes and system encryptions (Renda, 2022).

The CRS in May 2022 published Defense Primer: Quantum Technology and indicated QC could enable advances in machine learning, a subfield of AI. Such advances could spur improved pattern recognition and machine-based target identification. This could in turn enable the development of more accurate lethal autonomous weapon systems, or weapons capable of selecting and engaging targets without the need for manual human control or remote operation (Gallo, 2021).

The key to this entire discussion on weaponization comes down to security. "As information becomes the world's most valuable commodity, the economic, political, and military fate of nations will depend on the strength of ciphers…demolish(ing) the concept of national security. A quantum computer would jeopardize the stability of the world" (Bacon, 2006). Current QISs are not optimized for cybersecurity design practices, let alone optimized for hybrid computing as the flow of information moves from classical computers (including AI and 5G systems) to quantum computers and back again.

**Securing current and future weapon systems**

Shannon's Information Theory Model describes communication as a flow of messages:

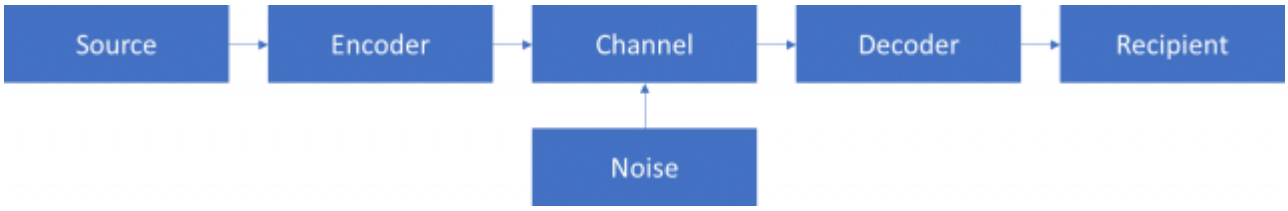


Figure 6: Shannon Information Theory Model (Shannon, 1948).

In this view (Figure 6) Shannon separated the sources of inputs that result in a complex message. Although the first use of the model indicated a loss of information due to the addition of destructive noise, it soon became clear that this noise could be reversed, and the original message recovered. Information was converted to an easy-to-transmit form and then subjected to an obscuring signal (Shannon, 1948). This model and knowledge led to the weaponizing action of encryption to keep unauthorized users from eavesdropping on military and diplomatic secrets and showed how attackers could break into a "secure" communications channel.

One important result of Shannon's work is the notion of information entropy, which is a measure of the uncertainty in a message that, in turn, determines the number of bits necessary to send the information (Shannon, 1949). Shannon used the concept of entropy to explore how much information is required to resolve

and restore obscuring in the message in terms of the unicity distance and redundancy found in routine communications. Unicity distance is the number of characters required to unambiguously eliminate all "spurious" (incorrect) possible decryptions for a message. The concept of unicity distance eventually led to the development of polymorphic encryption that is used to limit the reduction of entropy over an entire message (Carlson, 2012). Using polymorphic principles, the unicity distance is never met, and messages are made far more secure than using traditional encryption methods.

The way information is exchanged via the internet or by phone today is a direct result of Shannon's theory (Cauche, 2018). That same theory gives insight into how to manipulate the obscuring and redundancy to keep that same information secure. Shannon's work became information theory and is independent of the attacking device, classical or quantum (Cover & Thomas, 2005). The math remains unchanged in either environment. Therefore, Shannon's security theory remains applicable for both types of computing methodologies, while the implementation of those principles may differ from each other. The solution follows the mathematics, regardless of the exact implementation vector – the same principles used in classical solutions also work in the chemical security environment.

**Chemical States as a Security Solution-Quantum Chemistry for Detecting Security Threats to Information Systems**

Potentially breakthrough progress is being made in the realm of explicitly correlated particles using next generation scaling algorithms. This work has the potential to redefine the battlefield by relating PKI directly in chemical states. Highly accurate descriptions of vibrations and heat motion of atoms/ions, molecules as qubits or qudits (IEEE, 2017) that are caused by electric and magnetic fields are necessary to find and isolate security threats in information systems. Currently accepted by the broader scientific community, the Born-Oppenheimer-type Hamiltonians (BO-H) used to describe physical properties of chemical systems neglect the mass polarization interactions and explicit particle correlations that need to describe vibrations and heat motions in the excited states of qudits used for quantum information processing. By going beyond the Born-Oppenheimer (BO) approximations, The QSA proposes to:

- Develop a Q-MLS architecture using chemical sensors with virtualized validators
- Use physical properties of atoms (ions, and molecules) as qubits/qudits in quantum states:
- Ground – lowest energy of a physical system generally associated with adiabatic process, i.e., no heat transfer from neighboring quantum systems
- Excited – any energy above the lowest energy and is a non-adiabatic process, i.e., heat transfer to neighboring quantum systems
- Non-Bound – energies beyond the dissociation/ionization limit (threat detection)
- Describe these states computationally using next-generation all-particle methodologies
- Use Q-N that describes the systems exactly, including and not limited to, angular momentum (Zare, 1991) and magnetic spin dimensions

The very precise chemistry of a specific qubit/qudit quantum systems are ideal for security protocols and threat detections. Excited stationary states of atoms, ions, and molecules need highly accurate descriptions of energy to refine the detection of a change in energy. By including angular momentum, all-particle correlations, mass-polarizations, and a complete NBO-H, these highly refined and interesting states of matter can be used to validate

normal and altered information. The tertiary detections via very specific qubit designs will allow for identifying attacks on information systems and an effective implementation of a quantum attack.

The description of Rydberg atoms/molecules and ionization states of specific elements and or molecules and the vibrations and heat motion of atoms/ions caused by electric and magnetic fields with a high-level of accuracy and certainty to find and isolate attacks using the unanticipated heat or noise in a system as a *trigger/flare*.

Chemical chips, using chemical states as a key, onboard three systems as a sensor with a relationship to know system protocols either physical or virtualized: *Send System, Control System, Receive System*.

Using virtualization and containers of real systems with chemical chips onboard can work in *parallel with virtualized environments holding predicted* states.

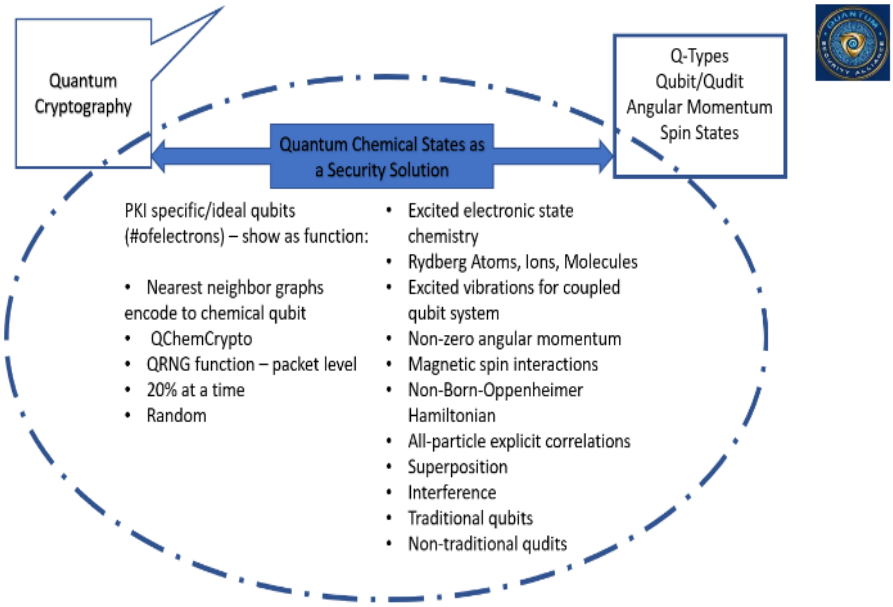


Figure 7: Concepts to be included in Q-Chem States as a Security Solution [QSA 2022]

In 2018, a member of the Department of Defense Science and Research (DoD DSR) team (Kossef, 2018), circulated a white paper with a mechanism of measuring cyber success at the federal level, which for which the definition of the proposed Cyber Hamiltonian (C-H) mentioned therein does not map to the mathematical explicitly correlated NBO-H (Sharkey, 2022). For the purposes of this white paper, we intend to show how a true C-H will map to the mathematical steady states needed for quantum information models. The definition of C-H with Q-N will be needed to move the industry forward in a secure way. Since chemical states are correlated to a specific set of quantum numbers, in theory, quantum information can be assigned to a ZTM, and policies defined at the federal level to satisfy a comprehensive C-H as proposed by Kossef (2018); including quantum elements of a multi-verse and verbose Quantum-Cyber-Hamiltonian (QC-H) concept. This can be accomplished by quantum virtualization of desired chemical states with FPGAs and the use of the QLEAN$^{TM}$ theory (Sharkey, 2018).

## Multiple Levels of Security

MLS is the application of a computer system to process information with incompatible classifications, permit access by users with different security clearances and needs-to-know while preventing users from obtaining access to information for which they lack authorization (Red Hat, 2022). What does MLS look like in the quantum realm? A state of electron-chemical-controlling declared for the purpose of securing information systems. The use of the MLS concept in quantum is use of a given computer system to process information with incompatible classifications to co-exist with users with different levels of access and common need to know, to prevent unauthorized users' access to data elements found with an information system, creating the roadmap for the QIS to Q-MLS approach for the next generation of cyber fidelity. There are numerous types of qubits that are built for a specific purpose; however, the use of the periodic table to build a future elemental for cyber encoding may provide a higher fidelity of cyber awareness and resiliency.

- The need for integrate current processes of computer security approaches to C-H qubits.
- Q-Tipper – a validated indicator of compromise.
- Q-IOC – quantum indicators of compromise.

### Research Area(s):

The QSA has adopted the DoD Technology Readiness Levels (TRLs). In 2001, DoD adopted the use of TRLs for new "Major Acquisition Programs to manage the maturity level of technology entering the programs. This 9-level assessment tool, modeled after the NASA index developed in the 1980s, enables the assignment of readiness levels from the observation of basic principles" ("Science and Technology Management-Technology Readiness," 2022).

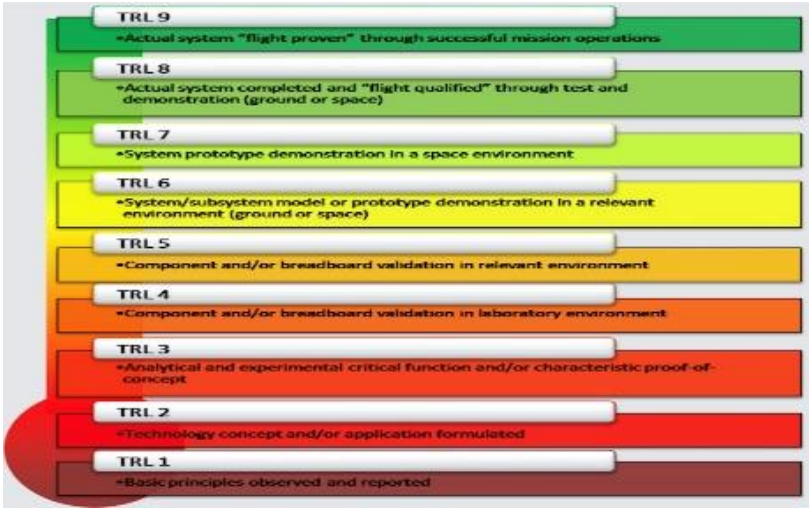


Figure 8: Technology Readiness Level [DoD, 2012)]

The QSA is suggesting the need to add TRL 0 to better recognize the need for thought leadership, innovation, and creativity in technology fields moving forward, specifically the quantum realm. The TRL 0 definition could take

shape as “Concepts requiring research and active thought leadership.” (QSA, 2022) Consider that a pin grid array (PGA) is a TRL 9, QC TRL 4, the use of Q-Chem for securing QC (and hybrid systems) would be a TRL 0.

**Challenges for QIS**

Quantum -

Computing: The activity of writing algorithms that specifically increase the efficiency in the effort of determining desired outputs defined by a process, procedure, and set of rules forming a binary decision utilizing the physical properties of magnetic spin-statistics in conjunction with angular momentum through known topologically satisfactory wave functions in a superposition and/or entanglement, and with/out (de-)constructive interference in form of a generalized qudit.

Qudit (Qu): A “d”-dimensional quantum system based on chemical states that utilizes the quantum numbers associated with angular momentum and magnetic spin in superposition.

Qudit Cyber Chemistry (QuCy-Chem): The use of cyber protocols that are encoded to various Q-Chem states to provide an Offensive Cyber Operation (OCO) & Defensive Cyber Operations (DCO) framework’s for Q-ZTM and Q-MLS with CDM.

Cybersecurity -

The National Security Agency (NSA) has reviewed quantum computing regarding encryption and has published numerous discussion topics, articles, and white papers on its diverse analysis outcomes. Additional efforts from NSA/NIST include analysis of Post-Quantum Cryptographic Algorithms (P-QCA) (lattice-based cryptography and hash-based signatures) with a clear indication of the eventual success of those two types of encryptions being workable in the near mathematical future; however, this white paper explores the use case of a quantum attack-pattern not published by the NSA. To be clear, the QSA understanding of the thought leadership being exhibited by the NSA and concedes that its approach is based on a clear use case, which does need to be articulated in this research concept. If the research as proposed findings result in the development and building of the Q-MLS function or the use of Q-Chem as a viable security solution, then the tenants of ZTM may be better met with the QSA approach toward practical and theoretical use case development. Cybersecurity is a large eco-space and has many different needs and constraints the use of a Quadratic Unconstrained Binary Optimization (QUBO) for numerical quantum computing may not provide the fidelity required for future proof analysis. The QuCy-H as proposed in this white paper affords the exploration of potential limitations of a defined QUBO {QUBO = min(objective) + y(constraints)} in its general form. It also may be possible to use the Ising model as a cross-correlation to a Hamiltonian expression for validation.

The use of the Information Technology and Cyber Conflict Divergence Theory (ITCCD) helps the QSA to define its research approach by understanding the various views that are imposed on cyber and quantum. The inclusion of cyber warfare, terrorism, system technology, information technology are just a few constraints that have been imposed on the cyber perspective of the unified theory behind the exploration of ZTM and ZTA concepts for an entire cyber ecosystem. The lack of qualified Quantum Cybersecurity Experts also poses an additional constraint of research problems. The QSA would support the development of an additional workforce framework

that includes the Technical, Knowledge, Skills, and Abilities entry into the various federal agencies that mandate skills sets associated with cyber expertise.

Polymorphic Mathematics

Adapting polymorphic algorithms for quantum implementation is a major step toward security. To date, no polymorphic algorithm has yet been programmed for use in the post-quantum environment. This method has been shown to be the safest algorithm available using symmetric key algorithms (Carlson, et al, 2021) and should be included in the suite of protection measures for quantum communications (Q-COM), regardless of the implementation method for transmission.

Quantum proofs and tools represent major research areas. The tools required for working on and simulating, the design of quantum security need to be both identified and adapted for use in PQE applications. This includes the use of the correct compiler and math simulator (presumably Python compiler and simulator, such as Mathematica). Presently control of quantum computers in the classical environment is accomplished with Python. Python is a powerful and easily learned computer language that has proven very useful in the PQE. The QSA has done extensive cyber threat analysis on the use of Python and believes a better software approach is required (QSA/TWIGI/CEAT, 2020). The Extensions to the language may be needed for the proposed implementation due to the unique needs for describing the solution. This also implies that other tools that operate on the quantum level or in terms of chemical vectors may also have to be identified and adapted for use. Typical classical math simulators are not capable of describing and completing the complex calculations required for the task. Mathematica (Wolfram, 2002) appears to be a prime candidate for this work, as it allows for simple calculation using the required continuous mathematics needed to describe quantum problems, as well as discrete math. The use of Mathematica is also widespread and well understood. However, new approaches to this security methodology will almost certainly require the development of new solution directions and algorithms.

A major research direction will involve determining the amount of entropy needed for secure quantum operations. Understanding the relationship between entropy and how it is measured using the proposed approach has not yet been undertaken. The resulting knowledge will then have to be mathematically formalized. Protocols for this information will also have to be developed. Answers will likely be found following the principles of Abstract Algebra, which says that if different problems have the same mathematical description that what works for the already known will also work for the new problem. This effort will require a wide background and the ability to blend world knowledge in novel ways.

**Python History**

Python is an interpreted, high-level, general-purpose programming language. Created by Guido van Rossum and first released in 1991, Python's design philosophy emphasizes code readability with its notable use of significant whitespace. Its language constructs and object-oriented approach aim to help programmers write clear, logical code for small and large-scale projects. Python is dynamically typed, and garbage collected. It supports multiple programming paradigms, including structured (particularly, procedural), object-oriented, and functional programming. Python is often described as a battery included language due to its comprehensive standard library. Python was conceived in the late 1980s as a successor to the ABC language. Python 2.0, released in 2000, introduced features like list comprehensions and a garbage collection system with reference counting. Python 3.0, released in

2008, was a major revision of the language that is not completely backward compatible, and much Python 2 code does not run unmodified on Python 3. The Python 2 language was officially discontinued in 2020 (first planned for 2015), and Python 2.7.18 is the last Python 2.7 release and therefore the last Python 2 release. No more security patches or other improvements will be released for it. With Python 2's end-of-life, only Python 3.5.x and later are supported. Python interpreters are available for many operating systems. A global community of programmers develops and maintains CPython, a free and open-source reference implementation. A non-profit organization, the Python Software Foundation, manages and directs resources for Python and CPython development. Figure 9: Python Critical Vulnerabilties from 2002-2020, provide more details.

| Year | Vul Count | Config Count | Ref Count | Avg Base Score | Avg Exploitability Score | Avg Score |
|---|---|---|---|---|---|---|
| 2002 | 3.00 | 4.00 | 20.00 | 5.70 | 7.97 | 5.23 |
| 2003 | 1.00 | 13.00 | 9.00 | 5.00 | 10.00 | 2.90 |
| 2004 | 3.00 | 4.00 | 23.00 | 5.83 | 10.00 | 4.07 |
| 2005 | 11.00 | 59.00 | 127.00 | 6.50 | 7.87 | 6.41 |
| 2006 | 5.00 | 94.00 | 82.00 | 6.12 | 5.94 | 7.14 |
| 2007 | 7.00 | 50.00 | 132.00 | 6.96 | 9.20 | 6.20 |
| 2008 | 23.00 | 399.00 | 359.00 | 6.77 | 7.68 | 6.93 |
| 2009 | 22.00 | 210.00 | 233.00 | 6.94 | 5.94 | 8.37 |
| 2010 | 12.00 | 134.00 | 165.00 | 6.04 | 9.15 | 4.96 |
| 2011 | 15.00 | 303.00 | 133.00 | 6.32 | 7.65 | 6.34 |
| 2012 | 15.00 | 260.00 | 133.00 | 5.00 | 7.43 | 4.61 |
| 2013 | 16.00 | 182.00 | 109.00 | 5.46 | 6.30 | 6.03 |
| 2014 | 45.00 | 980.00 | 261.00 | 5.74 | 8.01 | 5.27 |
| 2015 | 17.00 | 76.00 | 75.00 | 6.65 | 7.06 | 7.18 |
| 2016 | 15.00 | 223.00 | 125.00 | 7.35 | 2.77 | 4.49 |
| 2017 | 36.00 | 269.00 | 128.00 | 7.54 | 2.84 | 4.62 |
| 2018 | 35.00 | 254.00 | 170.00 | 7.45 | 2.82 | 4.55 |
| 2019 | 76.00 | 262.00 | 520.00 | 8.08 | 3.14 | 4.86 |
| 2020 | 44.00 | 238.00 | 147.00 | 7.42 | 2.81 | 4.49 |

Figure 9: Python Vulnerabilities History

Within the Common Vulnerabilities and Exposures / National Vulnerability Database (NVD) are three different versions on the Common Vulnerability Reporting Framework, 2.0, 3.0 and 3.1 each has a different focus and provides insight into how the temporal mathematics are used to score the risk associated with each vulnerability as

report and investigated. The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit. Scores range from 0 to 10, with 10 being the most severe. While many utilize only the CVSS Base score for determining severity, temporal and environmental scores also exist, to factor in availability of mitigations and how widespread vulnerable systems are within an organization, respectively. The current version of CVSS (v3.1), which was released in June 2019.

When creating the next analysis section of this report, a formula was crafted to look at both the CVSS Version 2.0 and 3.1 to determine, if analysis could be performed on the distinct data sets in their natural states. The research discovered different terms were used between the versions, in 3.1 the use of Critical was used to describe a vulnerability, while the keyword High was used in the CVSS v2.0, additionally, the CVSS v3.0 was also discovered within the dataset and was accounted for within the formula. The following table represent the information discovered.

| CVSS v2.0 - Score Analysis | | | | | CVSS v3.1 - Score Analysis | | | |
|---|---|---|---|---|---|---|---|---|
| Year | Low | Medium | High | | Low | Medium | High | Critical |
| 2002 | - | 2.00 | 1.00 | | - | - | - | - |
| 2003 | - | 1.00 | - | | - | - | - | - |
| 2004 | - | 2.00 | 1.00 | | - | - | - | - |
| 2005 | 1.00 | 2.00 | 8.00 | | - | - | - | - |
| 2006 | 1.00 | 1.00 | 3.00 | | - | - | - | - |
| 2007 | - | 4.00 | 3.00 | | - | - | - | - |
| 2008 | 1.00 | 10.00 | 12.00 | | - | - | - | - |
| 2009 | - | 16.00 | 6.00 | | - | - | - | - |
| 2010 | - | 8.00 | 4.00 | | - | - | - | - |
| 2011 | - | 9.00 | 6.00 | | - | - | - | - |
| 2012 | 3.00 | 11.00 | 1.00 | | - | - | - | - |
| 2013 | 2.00 | 13.00 | 1.00 | | - | - | - | - |
| 2014 | 5.00 | 28.00 | 12.00 | | - | - | - | - |
| 2015 | 1.00 | 8.00 | 8.00 | | - | - | - | - |
| 2016 | - | 9.00 | 5.00 | | - | 6.00 | 7.00 | 2.00 |
| 2017 | 3.00 | 17.00 | 16.00 | | 2.00 | 12.00 | 11.00 | 11.00 |
| 2018 | 4.00 | 21.00 | 10.00 | | 1.00 | 11.00 | 16.00 | 7.00 |
| 2019 | 3.00 | 43.00 | 29.00 | | - | 14.00 | 37.00 | 24.00 |
| 2020 | 4.00 | 24.00 | 14.00 | | 1.00 | 12.00 | 22.00 | 7.00 |

Figure 10: Python CVSS Temporal Analysis

## Conclusion

Clear national policies, laws, and governance are required as the danger of unregulated, insecure QC is becoming undeniable, and it will require a unified global response. NASEM "concludes that the development, standardization, and deployment of PQA is critical for minimizing the chance of a potential security and privacy disaster. Information intercepted prior to the deployment of PQA would not be protected" (Gallo, 2021). Currently, there is not a single sensor type, defense posture, or reliable countermeasure in place to stop any of these evolving threats from quantum computers. The U.S. does not have the policies, governance, or doctrines for tracking or identification capable of offering reliable defenses against QC; however, using Q-Chem for detecting security threats to information systems, coupled with in-memory QC, can offer this ability to track, audit, and continuously monitor quantum systems.

In May 2022, the QSA drafted an interim white paper that posited the need for Quantum thought leadership within the Cyber domain. Although, the document started the exploration of Q-Chem concept, this research effort includes several areas that were fleshed to meet the previous established recommendation, which where:

Immediately fund research:
- Explore QC for Q-Chem security concepts.
- Design solutions for in-line memory to data throttle for laser encoding.
- Design and integrate cybersecurity practices

Update the NDAA 2023 with these three options

All rights reserved. All content on this document is protected by Quantum Security Alliance (QSA) copyrights and other protective laws.

References

Al Hussein, Z. R. a. (2019). Here's what will decide whether technology becomes a force for good, or evil. Retrieved from https://www.washingtonpost.com/opinions/technology-can-be-put-to-good-use--or-hasten-the-demise-of-the-human-race/2019/04/09/c7af4b2e-56e1-11e9-8ef3-fbd41a2ce4d5_story.html

Bacon, D. (2006). Quantum Computing Shor's Algorithm. In: Department of Computer Science & Engineering, University of Washington.

Cauche, C. (2018). A brief history of modern communication security – and why PKI is the state of the art. Retrieved from https://www.nexusgroup.com/a-brief-history-of-modern-communication-security-%E2%80%AFand-why-pki-is-the-state-of-the-art/

Carlson, A. H. (2012). Set Theoretic Estimation Applied to the Information Content of Ciphers and Decryption, PhD Dissertation, University of Idaho, 2012

Carlson, A. H., Dutta, I. K., Ghosh, B., & Totaro, M. (2002). Modeling Polymorphic Ciphers, *FCST : The 4th IEEE International Symposium on Future Cyber Security*, 2021.

CNSSI 1015. (2013). Enterprise Audit Management Instruction for National Security Systems (NSS). Retrieved from https://www.cnss.gov/CNSS/openDoc.cfm?8SP9YF5rGby81Zw+3Zx68A==

Cover, T. & Thomas, J. (2005). *Elements of Information Theory*, John Wiley & Sons, 2005

Gallo, M. E. (2021). *Defense Primer: Under Secretary of Defense for Research and Engineering*. Retrieved from Washington DC: https://apps.dtic.mil/sti/citations/AD1125422

Krelina, M. (2021). Quantum technology for military applications. *EPJ Quantum Technology, 8*(1), 24. doi:10.1140/epjqt/s40507-021-00113-y

Kosseff, Jeff. (2018). Hamiltonian Cybersecurity 54 Wake Forest L. Rev. 155, Available at SSRN: https://ssrn.com/abstract=3234758

Mann, C. (2002). A Primer on Public-key Encryption. *The Atlantic.* Retrieved from https://www.theatlantic.com/magazine/archive/2002/09/a-primer-on-public-key-encryption/302574/

NASEM. (2021). "Identifying Opportunities at the interface of chemistry and quantum information science", the National Academies, 2021. Retrieved from www.nationalacademies.org/en/our-work/identifying-opportunities-at-the-interface-of-chemistry-and-quantum-information-science

NIST. (2022). PQC winner announcements. Retrieved from https://www.nist.gov/news-events/news/2022/07/pqc-standardization-process-announcing-four-candidates-be-standardized-plus

NIST. (2020). Zero Trust Architecture. (NIST SP 800-207). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-207/final

National Security Agency (NSA), (2022). Cybersecurity: Post-Quantum Cybersecurity Resources. Retrieved from https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

Pilch, J., Długopolski, J. (2019). An FPGA-based real quantum computer emulator. *J Comput Electron* 18, 329–342 https://doi.org/10.1007/s10825-018-1287-5

Public Key Infrastructure. (2022). Retrieved from https://en.wikipedia.org/wiki/Public_key_infrastructure

Red Hat (2022) Multi-Level Security (MLS). Retrieved from https://web.mit.edu/rhel-doc/5/RHEL-5-manual/Deployment_Guide-en-US/sec-mls-ov.html

All rights reserved. All content on this document is protected by Quantum Security Alliance (QSA) copyrights and other protective laws.

Renda, P. (2022). The Potential of the Weaponization of Quantum Computing. Retrieved from https://hakin9.org/potential-weaponization-quantum-computing-paul-f-renda/#:~:text=Quantum%20computing%20can%20make%20nuclear,no%20such%20properties%20of%20detection.

Science and Technology Management-Technology Readiness. (2022). Retrieved from https://www.dau.edu/cop/stm/Pages/Topics/Technology%20Readiness.aspx

Scholarpedia (2022). Lattice quantum field theory. Retrieved from http://www.scholarpedia.org/article/Lattice_quantum_field_theory

Sharkey, Keeper L., and Chancé, Alain. 2021. *Quantum Chemistry and Computing for the Curious: Illustrated with Python and Qiskit Code*. Packt, Pub. ISBN-13: 978-1803243900

Shi, B., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G. & Stehlé, D. (2020). *CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation*. NIST standard winner https://pq-crystals.org/dilithium/data/dilithium-specification-round3.pdf

Stapleton, J. (2012). A Concise History of Public Key Infrastructure. *ISSA*, 29. Retrieved from www.members.issa.org/resource/resmgr/JournalPDFs/History_of_PKI_ISSA0912.pdf

Technology Readiness Level. (2012). Retrieved from https://www.nasa.gov/directorates/heo/scan/engineering/technology/technology_readiness_level

Watchorn, M. (2020). Cyber Awareness Resiliency and Criticality. Retrieved from https://www.linkedin.com/posts/watchorn_cyber-awareness-resilience-and-criticality-activity-6688491207439585280-Zxn_?utm_source=linkedin_share&utm_medium=member_desktop_web

Watchorn, M. (2020). Cyber Exome Ancestry Tool (CEAT) 1.0.0.2 Analysis: Quantum Computing – Python (Critical) Vulnverabilites.

Watchorn, M., Bishop, J., Mumm, H. & Brooks, C. (2022). Cybersecurity Legal Elasticity Antecedent Resilience (CLEAR) System. Quantum Security Alliance (QSA).

Watchorn, M. & Bishop, J. (2018). Cyber Awareness and Resiliency.

Zak, R. (2016). 7 Well-Meaning Inventions That Turned Evil. Retrieved from https://whatculture.com/offbeat/7-well-meaning-inventions-that-turned-evil?page=4

Qudits: The Real Future of Quantum Computing? (2017). Retrieved from https://spectrum.ieee.org/qudits-the-real-future-of-quantum-computing

Wolfram, 2022. “Wolfram Mathematica: Modern Technical Computing,” https://www.wolfram.com/mathematica/

Zare, R. N. 1991. *Angular Momentum: Understanding Spatial Aspects in Chemistry and Physics, 1st Edition*. Wiley-Interscience, ISBN-13: 978-0471858928

All rights reserved. All content on this document is protected by Quantum Security Alliance (QSA) copyrights and other protective laws.