



Quantum Security Alliance (QSA)

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

Quantum Chemistry for Detecting Cybersecurity Threats to Information Systems

Authors

Dr. Hans C. Mumm, Chair Continuous Diagnostic and Monitoring, QSA, Victory Systems. LLC
Dr. Keeper L. Sharkey, Chair of Quantum Applied Chemistry, QSA, ODE, L3C
Dr. Merrick S. Watchorn, DMIST, QIS, Program Chair QSA, Huntington Ingalls Industries (HHI)

May 13, 2022

Issue: There is a national security risk in attempting to secure quantum computers. The threat of unchecked technology and the ability to weaponize quantum computing continues to evolve. Quantum 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, quantum computers reduced barrier to entry is now a national security risk. Hybrid-computing systems are coming online with no ability for the quantum computer to inherit the security controls of the current computer systems. There is no ability to secure these hybrid systems, much less securing an end-to-end quantum computer. We must begin to explore a new approach using chemical states as a security solution. This approach allows quantum computing 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.

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 (NIST, 2021). The White House led an effort to establish the National Quantum Initiative (NQI) Act, which became Public Law 115-368 in 2018 to accelerate American leadership in quantum information science and technology (NTSP, 2021).

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. In the last six months of activity, it has work on numerous efforts to include aiding the Cloud Security Alliance (CSA), Quantum.Tech Congress, and the National Defense University (NDU) in building a working knowledge sharing model that included the University of Maryland, University of Phoenix, and Purdue Global Online University. In the last six months of activity, it has work on numerous efforts to include aiding the Cloud Security Alliance (CSA).

Secure quantum computing will require a Continuous Diagnostics and Mitigation (CDM) Program. This will provide a dynamic approach to fortifying the cybersecurity of government networks and systems. Coupling this with the ability to explore emerging concepts such as the Zero Trust Models, 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 for pedigree, lineage, and originality within a Quantum

Information System (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.

Proposed Solution: Chemical States as a Security Solution-Quantum Chemistry for detecting security threats to information systems. Highly accurate description of vibrations and heat motion of atoms/ions, molecules as qubits (or qudits) 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 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 especially in the excited states of qubits (or qudits) used for quantum information processing. By going beyond the Born-Oppenheimer approximations, we propose to:

- Develop a Multi-Layer security architecture using chemical sensors with virtualized validators
- Use physical properties of ground and excited states of atoms, ions, and molecules as qubits (or qudits)
- Describe these states computationally using next-generation all-particle methodologies
- Use quantum numbers that describe the systems exactly, including and not limited to angular momentum and magnetic spin dimensions

The very precise chemistry of a specific qubit/qudit quantum systems are ideal for security protocol and threat detection. Excited stationary states of atoms, ions, and molecules need highly accurate description of energy to refine the detection in a change in energy. By including angular momentum, all-particle correlations, mass-polarizations, and a complete non-Born-Oppenheimer Hamiltonian, 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 the quantum distributed denial of service (Q-DDoS).

Recommendations: Immediately fund research to explore quantum computer security concepts.

1. Use of quantum chemical states as a cybersecurity solution.
2. Design solutions for in-line memory to data throttle.
3. Design and integrate cyber security best practices to include CDM, DFI and PKI for hybrid systems.
4. Update the NDAA 2023 with these three options

POC: Dr. Merrick S. Watchorn, DMIST, QIS, Program Chair, QSA- Huntington Ingalls Industries (HHI).

Authors background:

Dr. Hans C. Mumm- Founder and CEO of Victory Systems, LLC (SDVOSB) which specializes in cyber security, autonomous systems/robotic infrastructure, and integration. Dr. Mumm has eight published books on the subjects. The key to success is creating solutions on “How to harmonize the speed of innovation and change with the human spirit’s need for leadership” ®.

Dr. Keeper L. Sharkey- Founder and CEO of ODE, L3C which is a social enterprise that serves through Quantum Science, Technology and Research (qSTAR). We offer Quantum Logical Electrons and Nuclei (QLEAN™) - next-generation accuracy for Quantum Computational Chemistry. Our mission is to change the world with algorithms that solve non-deterministic polynomial-time hardness chemistry problems.

Dr. Merrick S. Watchorn, DMIST – Co-Founder, QSA, his current research is focused on quantum information science, cloud computing, cybersecurity, and open-source intelligence technologies.