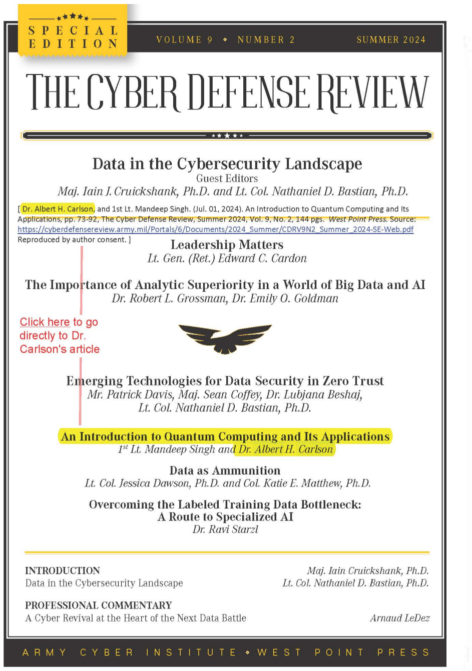
MySQIF™ polymorphic encryption is the future say leading cryptologists in the Army Cyber Institute's *Cyber Defense Review, Summer 2024*

A ground-breaking polymorphic encryption application has just been introduced named MySQIF™ Privacy App™ and is available now from https://www.mysqif.com



SPECIAL EDITION VOLUME 9 • NUMBER 2 SUMMER 2024

THE CYBER DEFENSE REVIEW

Data in the Cybersecurity Landscape
Guest Editors
Maj. Iain J. Cruickshank, Ph.D. and Lt. Col. Nathaniel D. Bastian, Ph.D.

[Dr. Albert H. Carlson, and 1st Lt. Mandeep Singh. (Jul. 01, 2024). An Introduction to Quantum Computing and Its Applications, pp. 73-92, The Cyber Defense Review, Summer 2024, Vol. 9, No. 2, 144 pgs. *West Point Press.* Source: https://cyberdefensereview.army.mil/Portals/6/Documents/2024_Summer/CDRV9N2_Summer_2024-SE-Web.pdf Reproduced by author consent.]

Leadership Matters
Lt. Gen. (Ret.) Edward C. Cardon

The Importance of Analytic Superiority in a World of Big Data and AI
Dr. Robert L. Grossman, Dr. Emily O. Goldman

Click here to go directly to Dr. Carlson's article

Emerging Technologies for Data Security in Zero Trust
Mr. Patrick Davis, Maj. Sean Coffey, Dr. Lubjana Beshaj, Lt. Col. Nathaniel D. Bastian, Ph.D.

An Introduction to Quantum Computing and Its Applications
1st Lt. Mandeep Singh and Dr. Albert H. Carlson

Data as Ammunition
Lt. Col. Jessica Dawson, Ph.D. and Col. Katie E. Matthew, Ph.D.

Overcoming the Labeled Training Data Bottleneck: A Route to Specialized AI
Dr. Ravi Starzl

INTRODUCTION
Data in the Cybersecurity Landscape — *Maj. Iain Cruickshank, Ph.D. Lt. Col. Nathaniel D. Bastian, Ph.D.*

PROFESSIONAL COMMENTARY
A Cyber Revival at the Heart of the Next Data Battle — *Arnaud LeDez*

ARMY CYBER INSTITUTE • WEST POINT PRESS

Aug. 08, 2024—The U.S. Army Cyber Institute just published its Summer 2024 Cyber Defense Review through *West Point Press*.

The Institute asked civilian MySQIF™ principal mathematician Albert H. Carlson, PhD to co-author:

> [“An Introduction to Quantum Computing and Its Applications.”]()

Dr. Carlson and co-author 1st Lt. Mandeep Singh have written a no-hype overview of the strengths, weaknesses, and prospective uses of Quantum Computing. They set expectations early that the venture banking feeding frenzy surrounding quantum computing should be tempered by a strong dose of reality:

> “Quantum computing is mostly inaccessible.”
>
> “A quantum bit, or qubit, can exist in an infinite number of states simultaneously.”
>
> “Qubits are highly prone to error and only operate in specific physical environments.”
>
> “Each type of qubit has shortcomings that must be overcome, breakthroughs cannot be accurately forecasted.”

- Need for super-cooling
- Very high cost
- Thermal errors in calculations are endemic currently

- “Decoherence” disturbs qubits from temperature, scalability, controllability, vibration, electromagnetism; colloquially: a sneeze fails a qubit, euphemistically called decoherence
- Lack of sufficient supply of qubits
- Few trained users and very high R&D cost
- Very large physical plants with sophisticated ground vibration absorbers required
- No standardization to approaches currently

Dr. Carlson provides an overview of the foundational component: Qubits.

He explains that classical computing works with 0s and 1s serially (one at a time).

By contrast, Qubits operate in a three-dimensional mode where up to a theoretically infinite number of 0s and 1s can circulate in a Qubit, performing calculations simultaneously. It is like the difference between rapid-firing bullets out of a rifle one at a time in classical computing versus an infinite number of bullets swirling simultaneously inside a theoretical Qubit sphere.

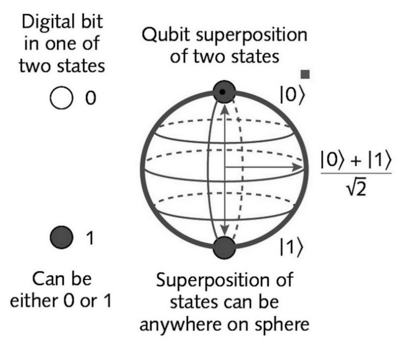

Digital bit in one of two states
○ 0
● 1
Can be either 0 or 1
Qubit superposition of two states
$|0\rangle$
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$|1\rangle$
Superposition of states can be anywhere on sphere

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

Figure 1: Introduction to Quantum Computing and its Applications (Carlson, Singh), p. 76 (2024: West Point Press).

Experiments are occurring on various Qubit structures from trapped ions and quantum dots to fluxonium and photon atoms. Each has strengths and limitations. Right now their operating time is in microseconds (one millionth of a second) after which the computer must then cool down for days.

The authors discuss the likely applications of quantum computing including:

- Solve new kinds of problems not yet envisioned
- Enhance classical computing
- Entangled qubits enhance memory density for new types of problems
- Optical fiber photon atoms as a security feature
- Quantum sensor applications, magnetic fields, electric fields, force, time
- Global Positioning Systems (GPS), penetration and masking
- Quantum communications
- Quantum clocks

1st Lt. Singh tips his hat to his U.S. military bosses by using electronic warfare scenarios set in Russia, Pacific Ocean, China, and Gaza propaganda narratives. Dr. Carlson is a well-known advocate for the peaceful uses of technology.

For example:

- Harvest Now Decrypt Later (HNDL) for China and Russia,
- Detect human use of tunnels in Gaza under-water activity in the Pacific Ocean,
- Location masking using inertial GPS navigation systems in Russia, and
- Breaking one-key AES-256 ciphers

Whether these examples are real, imaginary, or half-truths, they make a good story for the military narrative. For example, “Harvest Now” has been Five Eyes policy for decades. The Russians and Chinese did not invent that, but are most likely copying it.

The authors close by discussing the future of encryption post AES-256. They posit that **polymorphic encryption** is the answer to the broken AES-256 ciphers used currently for which quantum computing will speed up, but will hardly affect polymorphic encryption whose approaches will be only strengthened further by quantum computing.

That said, quantum photons traveling through fiber optics will be able to detect snoopers who are only looking at the transmission (their passive viewing bends the path of the photons).

Once detected, that quantum-to-quantum transmission can be stopped, thus protecting the information. However, resending a transmission will be cost-prohibitive in quantum computing for the foreseeable future, except for very specific scientific applications.

POSTCRIPT

Quantum-proof polymorphic encryption, highlighted in the article, as the future of post-quantum encryption, gives the private citizen what the military is looking for: “information advantage” and “decision dominance.”

A polymorphic encryption application has just been introduced named **MySQIF™ Privacy App™** and is available now from https://www.mysqif.com

Dr. Carlson provided in-depth consultation to the development of MySQIF™

PROTECT YOURSELF & - CLICK HERE TO LEARN MORE
MySQIF™ Privacy App™
Quantum-proof Encryption

MySQIF™ Privacy App™ uses polymorphic encryption that generates tens of thousands of one-time, unclonable keys for a single encrypted file. These one-time key clusters or "shards" are based upon unique hardware fingerprints on the sending and receiving devices.