Phiston TECHNOLOGIES® INC.
Innovation, Ingenuity, Integrity

Quantum Computing and Its Impact on Data Security

phiston.com | info@phiston.com | 305-517-1744

QUANTUM COMPUTING AND ITS IMPACT ON DATA SECURITY

Many experts believe that quantum computing will eventually become the primary choice over what we would call today's conventional technologies. Quantum computers, in particular, promise to be applied to several practical problems, including cryptography, artificial intelligence, and even financial modeling.

But why is data security so crucial within quantum computing? Are encryption and wiping good data destruction techniques? Or is physical destruction the only viable solution? Let's take a look.

WHAT IS QUANTUM COMPUTING?

Quantum computing (or QC) is a cutting-edge field that leverages the principles of quantum mechanics to perform complex calculations at speeds potentially far beyond the capabilities of classical computers. Unlike classical bits, which use resistors to represent either a 0 or a 1, quantum bits or qubits can exist in multiple states simultaneously due to a phenomenon known as superposition.

Simply put, quantum computers are machines that can solve complex problems fast. Qubits are a very special type of unit, as they can basically exist in multiple states simultaneously. This property enables quantum computers to perform complex calculations at a much faster rate.

Let's see an example. Suppose you need to find the most subtle patterns used in financial transaction fraud. Your best bet today would be to use a supercomputer or a machine with thousands of classical CPU and GPU cores. Unfortunately, this wouldn't be enough to analyze the many variables required to understand the problem. This is not just expensive and time-consuming. It's also most likely impossible, as you would not be able to reach the needed processing power - no matter how many components you added.

The solution? Not brute force in the shape of countless CPUs and GPUs... but cutting-edge quantum computers that make calculations using the quantum states of bits.

UNDERSTANDING QUANTUM COMPUTING PRINCIPLES

As we mentioned above, qubits or quantum bits can exist in multiple states simultaneously - as opposed to classical bits, which can be in a state of either 0 or 1 at any given time. This difference is due to the principles of quantum mechanics. So, let's see the fundamental principles that set qubits apart.

- **Superposition:** A qubit can represent both 0 and 1 simultaneously. This means that until it is measured, a qubit exists in a probabilistic combination of both states. This rather unique property allows quantum computers to perform many calculations in parallel - thus significantly increasing their processing power for certain problems.

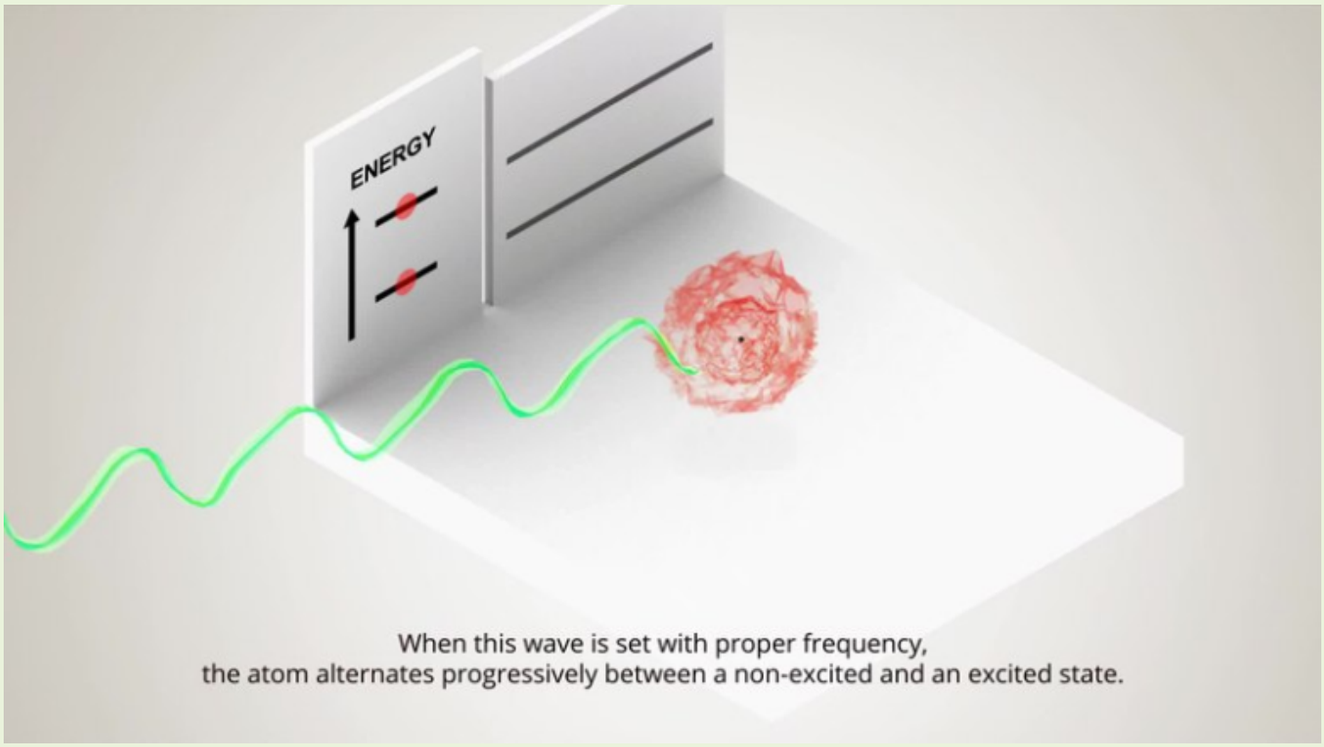


Image alt: An animation showing the quantum superposition of states.
VIDEO: https://en.wikipedia.org/wiki/File:Quantum_superposition_of_states_and_decoherence.ogv

- **Entanglement:** Qubits can become entangled, where the state of one qubit becomes linked with the state of another, regardless of the distance between them. This means that any changes in one qubit will instantly affect the other, making them highly correlated. In terms of computing, entanglement is a powerful resource because it can allow for more efficient computation and communication.

- **Quantum interference:** Lastly, manipulating qubits can enhance correct answers to computations while minimizing errors. This is due to the interference phenomena, or the ability of quantum computers to operate on the principles of constructive and destructive interference (something that boosts the accuracy of the final results).

A HYBRID MODEL OF COMPUTING

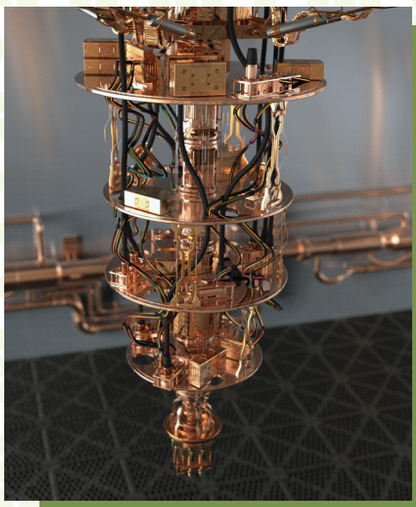
The concept of hybrid computing combines a traditional or classical computer (like a regular laptop) with a quantum processor to leverage the unique capabilities of quantum computing.

In a hybrid quantum-classical system, the classical computer serves as a controller or orchestrator, managing and interfacing with the quantum processor. The quantum processor is typically maintained at extremely low temperatures (close to absolute zero) to create an environment conducive to maintaining the delicate quantum states necessary for qubits to function.

This way, the processor can exploit quantum phenomena like superposition and entanglement. The classical computer can then interact with the quantum processor, sending instructions and receiving results.

CURRENT CHALLENGES OF QUANTUM COMPUTING

Quantum computers can process vast amounts of data in parallel and potentially solve complex problems more efficiently than classical computers. However, there are a few considerations to keep in mind.



- Qubits are highly sensitive to environmental interference and can be easily disturbed, leading to errors in computation.
- This is a significant challenge in building and maintaining stable qubits for practical quantum computing. Luckily, researchers are making significant advances in various qubit implementations, such as superconducting circuits, trapped ions, photons, and other quantum systems that improve both stability and scalability for future machines.
- Today much of the research is still trial and error. However, the field is advancing rapidly, so you shouldn't be surprised to learn that quantum algorithms are already being experimented with for finance, machine learning, and chemistry.

WHY IS DATA SECURITY IMPORTANT?

- Data security ensures the **protection of sensitive personal, financial, and corporate information** from unauthorized access, theft, or manipulation.
- Secure systems **maintain the privacy of individuals** by safeguarding their personal data from being exposed or exploited.
- Ensuring data security **builds trust** among users, customers, and businesses, fostering strong relationships and reliability in the use of technology and services.
- Data security measures often **correspond to legal requirements** and industry standards. Companies are obligated to protect certain types of data, and failure to comply can result in legal repercussions.
- Data breaches can severely impact business operations, causing financial losses, damage to reputation, and **potential interruptions in services**.

NIST, NSA, AND DIN GUIDELINES

Various organizations provide guidelines and standards to help enterprises and individuals establish robust data security practices. For example:

- **NIST Guidelines:** The NIST, a U.S. federal agency, offers comprehensive guidelines and frameworks for enhancing cybersecurity. The NIST Cybersecurity Framework is widely adopted and provides a set of best practices, standards, and guidelines to manage and improve an organization's cybersecurity risk management. For instance, SP 800-53 and SP 800-171 provide detailed controls for federal information systems and non-federal systems, respectively. Its worth noting that NIST guidelines are not limited to the U.S. government sector; they are widely recognized and implemented across industries globally.

- **NSA Guidelines:** The NSA's Information Assurance Directorate provides resources and recommendations for enhancing the security posture of both government and private sector entities. The NSA's Commercial Solutions for Classified (CSfC) Program facilitates the use of commercial technologies to protect classified national security information. It provides guidelines for configuring systems to meet specific security requirements.

- **DIN Guidelines**: DIN, a German standards organization, plays a crucial role in setting technical standards, too, including those related to data security. DIN 66399, for example, focuses on data destruction and secure disposal of information media and categorizes security levels for data destruction and specifies requirements for shredding or destroying various types of media. This includes guidelines on particle size (down to 2mm x 2mm), ensuring that data is effectively and irreversibly destroyed.

DATA SECURITY AND QUANTUM COMPUTING HARDWARE

1

Issues With Current Encryption Methods

Quantum computing poses a potential threat to current cryptographic methods that secure sensitive data. For example, quantum algorithms like Shor's algorithm on a sufficiently powerful computer could break widely used encryption schemes, leading to a risk of data exposure.

2

Urgent Need for Quantum-Safe Cryptography

The development and implementation of quantum-resistant cryptographic methods, often termed post-quantum cryptography, is crucial to counter the potential threats posed by quantum computers, too. Quantum computers can solve certain math problems much faster than regular computers. This could be a problem for the security of sensitive data that's protected by commonly used encryption methods like RSA and ECC.

Although we don't have quantum computers that can break current encryption, it's becoming more important to start protecting data from future quantum threats.

It's important to remember that when large-scale, fault-tolerant quantum computers become available, they could potentially compromise the security of data encrypted with current cryptographic standards. This no doubt poses a threat to sensitive information, including personal data, financial transactions, and confidential communications that rely on these encryption methods.

QUANTUM COMPUTING SECURITY: CHALLENGES ON THE HORIZON

One key thing to keep in mind is that provided quantum computing continues its current trajectory, we will have to transition to new standards. This process, which is bound to be complex and multifaceted, will need a smooth migration plan that does not compromise the security of existing data and systems.

There are several key aspects that will need to be considered during this traditional-to-quantum-computer transition period. Let's quickly go through some of them.

Integration of New Encryption Methods

Implementing quantum-resistant cryptographic methods will involve integrating new encryption algorithms into existing systems. This process can include, for example, updating software, hardware, and protocols to support the new cryptographic standards.

Backward Compatibility

Maintaining compatibility with existing systems and data formats will be crucial, too. Specifically, as organizations gradually shift to quantum-safe cryptography, they must ensure that the new cryptographic methods can work alongside or be integrated with the current infrastructure to decrypt and access previously encrypted data.

Coexistence of Multiple Systems

During the transition period, there will likely be some time when both classical and quantum-safe cryptographic systems operate simultaneously. This coexistence necessitates the ability for systems to handle both types of encryption, decrypting data using either current or quantum-resistant methods based on the encryption used.

Interoperability and Standards

Establishing industry-wide standards and protocols for quantum-safe cryptography is essential to ensure interoperability between different systems and organizations as well. Standardization can simply facilitate a smoother transition and compatibility between other implementations of quantum-resistant algorithms.

Updating Protocols and Infrastructures

Updating and upgrading cryptographic protocols, key management systems, and infrastructures to support quantum-safe cryptography is a fundamental aspect of the transition. This process involves reconfiguring networks, databases, and security measures to accommodate the new encryption standards.

STAYING AHEAD OF THE CURVE

The invention of quantum computing presents both opportunities and challenges in the realm of data security. However, there's good news! With the correct strategies in place, your company can mitigate the risks. All you need is an understanding of the potential impacts and a few proactive methods to stay ahead of the curve.

Education and Training

Understanding the potential impact of quantum computing on data security is (and will remain) crucial for individuals, organizations, and governments. Education programs, workshops, and information dissemination can help raise awareness about the threats and implications of quantum computing for data protection.

This approach could include educating IT professionals, developers, and security personnel on the new algorithms, potential threats from quantum computing, and best practices for maintaining data security in the quantum era.

Quantum Computing Research and Development

Continued research and development efforts are essential for creating and standardizing quantum-safe solutions. These efforts could focus, for example, on discovering and developing new quantum algorithms and protocols that are resilient against attacks from quantum computers.

Collaboration and Standardization

International collaboration and standardization efforts are also imperative for the successful adoption of robust and interoperable quantum-resistant data security standards. We are talking, for instance, about collaborative initiatives among governments, industry leaders, and research institutions to ensure the development of universally accepted standards.

Risk Assessment and Transition Planning

Assessing current systems and planning for the transition to quantum computers will also be essential for ensuring long-term data security. This can involve, for example, evaluating the existing infrastructure, identifying vulnerabilities, and understanding the potential impact of quantum threats. Organizations will need to devise comprehensive transition plans that encompass upgrading systems, training personnel, and implementing new security measures.

Continuous Monitoring and Adaptation

The landscape of cybersecurity and quantum computing is continuously evolving. So, we will need monitoring and adaptation to new technological advancements and emerging threats, too. Organizations should remain agile and adaptive in their strategies for implementing and maintaining data security for quantum computing.

PHYSICAL DESTRUCTION DATA SECURITY SOLUTIONS

Physical destruction is a data security method that renders stored information on physical storage media irrecoverable by destroying the media itself. This method is commonly used when data is no longer needed and there's a need to prevent any potential recovery or access to sensitive information.

There are two main methods commonly used for physical destruction when it comes to our current media:

- **Shredding:** Physical documents, optical media (such as CDs or DVDs), hard drives, or solid-state drives can be shredded using specialized equipment to turn them into very small pieces. The particle size is a critical factor in data destruction. Some standards, like DIN 66399, specify different security levels based on particle size, ensuring that the resulting fragments are small enough to prevent data reconstruction.

- **Degaussing:** This method uses a strong magnetic field to disrupt the magnetic structure of certain storage media, erasing the data and making it unrecoverable. Degaussing is particularly effective for media that relies on magnetic properties for data storage. However, it is not applicable to non-magnetic media like optical discs or solid-state drives, which use different technologies for data storage.

Physical destruction ensures that the data cannot be retrieved, providing a high level of security against unauthorized access. This method is also often a part of an overall data security strategy. For example, it is combined with other security measures like data encryption, access control, and secure data disposal policies to ensure comprehensive data protection.

Most industries dealing with sensitive information, such as healthcare or finance, have specific regulations mandating the secure disposal of data, and physical destruction helps meet compliance standards. The regulations are designed to protect the confidentiality, integrity, and privacy of sensitive data, ensuring it is handled and disposed of in a manner that prevents unauthorized access or breaches.

PHYSICAL DESTRUCTION AND COMPLIANCE

Industries dealing with sensitive information, including healthcare and finance, are subject to stringent regulations and compliance standards that mandate secure disposal methods for data. For example:

- In the United States, healthcare organizations covered by **HIPAA regulations** are required to implement secure data disposal practices. This includes the secure destruction of electronic health records (EHR) and other sensitive patient information to prevent unauthorized access.

- The **Payment Card Industry Data Security Standard** (or PCI DSS) also established that entities dealing with cardholder information must comply with PCI DSS, which includes guidelines for secure data disposal, particularly for expired or invalid credit card data.

- The **GLBA** imposes data security and privacy regulations on financial institutions, requiring them to safeguard customers' personal financial information. Secure disposal methods are necessary to prevent identity theft or financial fraud.

What's important to remember is that regulatory bodies impose legal requirements for data protection, making compliance mandatory. Failure to comply can, in fact, lead to severe penalties, fines, or legal actions against organizations that mishandle sensitive data.

Physical destruction methods like shredding or degaussing can help make the data stored on physical media get eradicated - but only provided degaussing is high enough and the shred particle is small enough to ensure irretrievability and can meet the requirement of irretrievability.

DEGAUSSING AND QUANTUM COMPUTING

Degaussing is primarily effective for magnetic storage media such as hard drives and magnetic tapes. However, quantum data storage does not rely on magnetism for encoding information. Quantum information is typically stored in physical systems like trapped ions, superconducting circuits, or photons - none of which rely on magnetic principles.

So, while this method might be useful for secure data disposal in classical computing contexts, it lacks relevance to the unique data storage principles of quantum computing.

DATA DESTRUCTION AND QUANTUM COMPUTING

Traditional data security methods like shredding and degaussing, commonly used for the physical destruction of data on storage media, can also be applicable to quantum computing. However, there are a few things to keep in mind due to the unique nature of quantum information.

As we have established above, quantum information is fundamentally different from classical data in how it's stored and processed.

We know that quantum data, stored in qubits, relies on principles like superposition and entanglement, making it highly sensitive and fragile. The information is often stored in physical systems like trapped ions, superconducting circuits, or photons, and the storage mechanism doesn't directly correspond to classical storage media. Due to the nature of quantum states and entanglement, traditional data destruction methods might not effectively erase quantum information.

DATA ERASURE AND QUANTUM COMPUTING

Data erasure, also known as data wiping or data sanitization, is the process of permanently removing data from storage devices to prevent any possibility of recovery. The goal of this method is to completely eliminate all traces of data on storage devices. Usually, this is done by overwriting existing data with random or predefined patterns.

Data erasure encounters significant challenges and limitations in the context of quantum computers because qubits behave very differently from classical bits. For example, the fundamental characteristic of superposition in qubits means that quantum information exists in multiple states simultaneously until measured. Erasing this information in a classical sense might not work, as the information can exist in multiple states at once!

The no-clone theorem in quantum mechanics, in fact, states that it's impossible to create an exact copy of an arbitrary unknown quantum state. This principle complicates the erasure process because copying and deleting quantum information in the classical sense might not be possible.

So, in short:

- You **cannot effectively overwrite data** because of superposition and entanglement.
- You **cannot completely erase data** (via wiping) without disrupting the underlying quantum system or causing unintended consequences.
- You **cannot securely verify all data has been erased.**

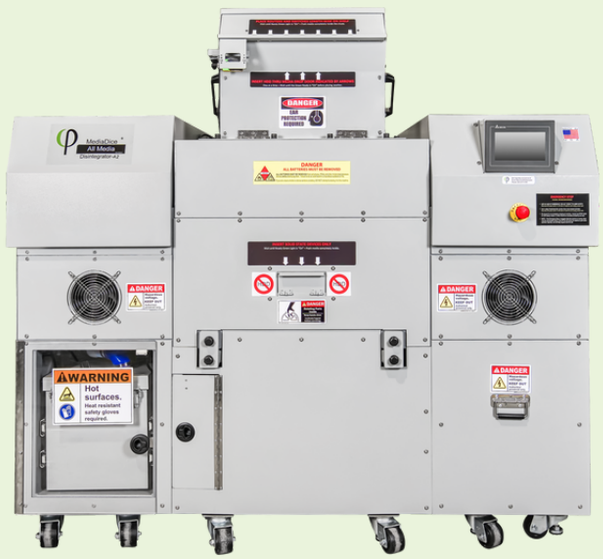
In other words, the traditional data erasure methods designed for classical computing are not directly applicable to quantum computing due to the distinctive properties and behaviors of quantum information.

PHYSICAL DESTRUCTION AND QUANTUM COMPUTING

The methods used for quantum data storage are also different from traditional storage media like hard drives or tapes used in classical computing. So, shredding or physically destroying the storage medium might not effectively erase quantum data without disrupting the underlying quantum system.

However, if your intention is not to erase the data but actually destroy the devices completely, then methods like using a disintegrator or destroyer can be effective for quantum computers, too.

Looking to the future, physical destruction to the appropriate particle size will be vital for complete data security and irretrievability of information in a quantum computing world. For example, the MediaDice® All Media Disintegrator A2 is a solution that can effectively disintegrate hard drives, switches, solid state drives, and even laptops - all while meeting the NSA/CSS standard of 2 mm nominal edge length or less. This machine is not just capable of destroying these devices but also includes a built-in magnetic metal separator that classifies e-waste so it can be recycled more easily - making it an ideal choice for the more environmentally conscious teams.



THE FUTURE OF DATA DESTRUCTION

THE FUTURE OF QUANTUM COMPUTING

CONCLUSION

Quantum computing has the potential to significantly impact fields like cryptography, optimization problems, drug discovery, materials science, and artificial intelligence. However, the technology is still in its early stages, so there are still several challenges (like maintaining qubits' stability, as they are highly sensitive to environmental interference) we will have to face on the path to wider adoption.

Researchers and scientists are continually working on developing and improving quantum hardware and algorithms to make quantum computing more practical and widely applicable. One thing is certain, though. Quantum computers, just like regular ones, have chips and circuits. So, there is a physical foundation in common. In terms of data security, this can, in fact, be advantageous.

Phiston Solutions specializes in end-of-life media destruction. Our disintegrators, destroyers, and degaussers are used by some of the largest tech companies around the world and are engineered to deal with the rise of data breaches, no matter the industry.

Sensitive data can't be just thrown away. It needs to be disposed of properly to safeguard it from malicious actors. All of our products are designed to ensure the data is made 100% unrecoverable and fully automated for ease of use and safety. Don't hesitate to contact us today to learn more about our range!