PriMera Scientific Engineering
Volume 4 Issue 1 January 2024
ISSN: 2834-2550

PriMera Scientific Publications

Quantum Computational Paradigm, Elucidating the Potential Ramifications for Automotive Cyber Security

Type: Short Communication
Received: November 29, 2023
Published: December 28, 2023

Citation:
Maciej Nowak., et al. "Quantum Computational Paradigm, Elucidating the Potential Ramifications for Automotive Cyber Security". PriMera Scientific Engineering 4.1 (2024): 58-62.

Maciej Nowak[1]* and Michał Andrzejczak[2]

[1]*Security Architect, Argus Cyber Security*

[2]*Senior Cryptographer, ResQuant*

***Corresponding Author:** Maciej Nowak, Security Architect, Argus Cyber Security.

Introduction

The automotive industry faces many challenges caused by AI and is pursuing more ecological solutions. We can see a significant increase in articles announcing the implementation of the latest trends in the automotive industry. Buzzwords, including Artificial Intelligence, Machine Learning, Big Data, and blockchain, stand out among others. Although very promising, these technologies only sometimes match the needs of the automotive market, although they may have (narrow) applications. Quantum computing represents a revolution to transform the IT industry and extend to the automotive sector, posing a significant threat to automotive security in the coming decades.

What is Quantum Computing?

Quantum computing is a cutting-edge field of study that harnesses the principles of quantum mechanics to process information. Unlike classical computers, which use bits as the smallest data unit that can be either 0 or 1, quantum computers use quantum bits or qubits. Qubits can exist in a superposition of states, representing 0 and 1 simultaneously. This unique property and quantum entanglement and interference enable quantum computers to perform complex calculations at exponentially faster rates than their classical counterparts. The potential applications of quantum computing span various domains, including cryptography, optimization, and drug discovery, promising revolutionary advancements in science and technology.

As companies and governments push more and more funds into quantum computer development, quantum computers are growing every year, expanding their functionalities and ability to solve more complex problems.

2023 marks a shift in the world of quantum computing research. Rather than focusing solely on increasing qubit count, the emphasis is now on practical applications. IBM's new Heron processor, featuring 133 qubits, is a prime example of this trend. Despite its relatively low qubit count, the Heron processor boasts impressive quality and can connect with other processors. This represents a shift towards "modular" quantum computers with the potential for scalable computing power. Additionally, there is a growing interest in quantum communication, which aims to transfer coherent qubits over vast distances. As global competition intensifies, the importance of quantum computing for the future of science and technology cannot be overstated.

Quantum Computers - Opportunities and Risks for the Automotive Industry

The advent of quantum computing could revolutionize several industries, including the automotive sector. As we explore this technology's potential applications and challenges, it is clear that the road ahead is exciting and complex. There are several areas where quantum computing can bring about significant improvements in the automotive industry. For instance:

Opportunities:

- Improved Simulations: Quantum computers can execute intricate simulations at unprecedented speeds, aiding in the creation of more efficient engine designs, enhanced fuel consumption, and advanced aerodynamics.
- Material Innovation: Quantum mechanics can help discover new materials with desired properties, leading to the creation of lighter, more robust, and more sustainable vehicles.
- Streamlined Supply Chains: Quantum algorithms can solve complex optimization problems, streamlining supply chains and reducing production costs.

However, some potential risks are associated with adopting quantum computing in the automotive industry. These include:

- Economic Disruption: As with any technological advancement, there is a risk of job displacement in areas that quantum computing can automate or optimize more efficiently.
- Implementation Challenges: Integrating quantum solutions into existing automotive systems will require significant time, expertise, and investment.
- Cyber security Concerns: Quantum computers have the potential to break many of the current encryption methods, necessitating the development of quantum-resistant cryptographic solutions to protect automotive software. In the 1990s, P. Shor published a method to break currently used cryptographic algorithms using potential quantum computers, posing a significant risk to the security of products like cars that have been on the market for many years.

What is Post-Quantum Cryptography?

Post-quantum cryptography, also known as quantum-resistant cryptography, is an exciting and rapidly evolving field that focuses on creating cryptographic algorithms that can withstand the immense computing power of quantum computers.

Traditional cryptographic systems such as RSA and ECC rely on complex mathematical problems that would take a classical computer an impractically long time to solve. However, these problems can be solved efficiently with the advent of quantum computers. Shor's algorithm could compromise RSA and ECC.

Therefore, Post-quantum cryptography is crucial to developing secure communication systems and data protection in a world where quantum computers are becoming increasingly powerful. By developing new cryptographic schemes based on mathematical problems that are believed to be resistant to quantum attacks, researchers in this field aim to ensure data confidentiality, integrity, and authenticity in a post-quantum computing era.

NIST: Announcing the Quantum Resistant Digital Signature Standard

To mitigate the quantum threat in 2016, the U.S. NIST called for proposals for quantum secure algorithms for new upcoming standards. In August 2023, after years of development, NIST published draft versions of new standards, including two algorithms for digital signatures and key encapsulation for key exchange protocols.

In the first quarter of 2024, NIST will announce the standards' final version. The new standards will be general-purpose ones without limitations, able to directly replace elliptic curves and RSA/DSA ancestors.

It should be noted that standardized quantum secure signatures have been available since 2020 when NIST announced their stan-

dards for stateful hash-based signatures.

Their biggest drawback is updating private keys after every signing operation. The number of signatures is also limited.

On the other hand, these algorithms are believed to be the most secure ones, and due to their properties, they are dedicated to signing software and firmware.

EU Perspective

NIST is not the only agency concerned about quantum security. Security agencies from France and Germany (ANSSI and BSI) have also emphasized the future need for quantum resistance. They also highlight the importance of a hybrid approach, combining classical algorithms with post-quantum ones to prevent attacks on immature PQC that are currently unknown.

NSA and Commercial National Security Algorithms Suite 2.0

In 2022, the U.S. NSA published their Commercial National Security Algorithms Suite 2.0, pointing out that products must be quantum secure:

- Software and firmware signing in 2030,
- Network equipment in 2033,
- Operating systems in 2033,
- Web and cloud services in 2033.

Considering vehicle lifecycle, estimated at 12 years, and product development, which is an additional 2-4 years, we can easily forecast that currently developing cars will need to face quantum computer threats, and hopefully, they will be quantum-resistant.

Automotive & Cyber Security Today

The current state of PQC development and the recommendations from cyber security agencies allow us to start working on adjusting the new algorithms for the automotive industry.

With the rapid growth of quantum technology and the emergence of post-quantum cryptography, it is becoming increasingly urgent to adjust new algorithms for the automotive industry. Cyber security agencies recommend adopting post-quantum cryptographic standards as a proactive measure against the “store now, decrypt later” threat posed by cyber espionage and data breaches.

Store Now, Decrypt Later

In the world of cyber espionage and data breaches, the “store now, decrypt later” strategy has emerged as a looming threat. This strategy involves capturing and storing encrypted data today, intending to decrypt it in the future when more powerful decryption tools become available.

The advent of quantum computing amplifies this threat, as traditional encryption methods such as RSA and ECC may easily be decrypted by quantum computers in the future.

Post-quantum cryptographic methods are designed to be secure against classical and quantum computer threats, making them a reliable solution to ensure that data remains secure today and in a future dominated by quantum computing. It is essential to consider the estimated vehicle lifetime when implementing these measures.

PQC in Automotive

The automotive industry heavily relies on cryptography to ensure the security and integrity of vehicular communications and systems.

Symmetric cryptography, which uses the same key for encryption and decryption, is well-suited for real-time operations such as vehicle-to-vehicle communications. It is considered less vulnerable to quantum computing as it only requires doubling the key length to maintain security.

However, the same cannot be said for asymmetric cryptography, which uses a public and private key pair. Also known as public-key cryptography, it is more susceptible to quantum threats, especially in the context of digital signatures.

This has increased the emphasis on post-quantum cryptography (PQC) for asymmetric methods within the automotive sector. Prioritizing PQC in asymmetric cryptography and digital signatures is essential to develop encryption techniques resistant to potential quantum attacks, ensuring long-term security for next-generation vehicles.

PQC Automotive Use-Cases

Public key cryptography is used in many areas of automotive. The other use cases for the public key in the automotive industry are privilege verification for maintenance, counterfeit parts verification, vehicle-2-vehicle data exchange, vehicle-2-infrastructure authentication, key lifecycle management, and many others. The mentioned areas have other requirements and will likely require different PQC solutions.

Root of Trust

One of the key components of a trusted computing system is the Root of Trust. It is a set of functions that serves as the foundation for all subsequent security and cryptographic functions in the system. The Root of Trust is responsible for securely executing and authenticating software operations, from boot-up sequences to firmware updates, and deriving the system's security properties. In a vehicle, the Root of Trust ensures that these operations are performed safely, providing a solid foundation for the security of the entire system. In the automotive sector, the root of trust often relies on public key cryptography, making it vulnerable to quantum threats.

All the software and firmware used in vehicles are usually signed with the manufacturer's private key. The signature is always verified in a secure boot procedure to ensure that only the vehicle will use the certified and safe code.

The ability to run untrusted and modified firmware might be dangerous for road traffic and the environment. Thus, this is the first and most important area to work on.

Key Lifecycle Management

Key Lifecycle Management is an essential aspect of securing modern vehicles. As cryptographic keys may need updating or revoking throughout a vehicle's lifespan, public key mechanisms provide a secure way to manage these keys and ensure that obsolete or compromised keys are replaced without compromising the vehicle's security.

Over-the-Air (OTA) Updates

Manufacturers commonly employ over-the-air (OTA) updates to upgrade a vehicle's software wirelessly. However, security risks arise as malicious software may be installed. That is where public keys come in - they provide an extra layer of security by ensuring that only genuine OTA updates are installed.

Secure Diagnostics

Secure Diagnostics are critical in modern vehicles to ensure that maintenance tasks are performed only by authorized personnel. Public keys facilitate secure communication between the vehicle and diagnostic tools, ensuring that diagnostic data remains confidential and is only accessible to authorized entities. The public key infrastructure (PKI) also ensures that only technicians with the correct cryptographic credentials can access and modify specific vehicle systems, preventing unauthorized tampering.

Counterfeit Parts Verification

Counterfeit Parts Verification is essential in preventing safety and performance risks posed by counterfeit automotive parts. By embedding genuine parts with cryptographic signatures, public keys can verify the authenticity of installed components, ensuring they meet the manufacturer's standards.

Driver Authentication

Driver Authentication is necessary for securing personalized driver settings and usage-based insurance. Public keys can authenticate drivers based on cryptographic credentials, adding an extra layer of security to vehicle personalization.

Vehicle-2-Everything (V2X)

Vehicle-2-Vehicle (V2V) Data Exchange is becoming increasingly crucial as vehicles become more interconnected. Public keys facilitate encrypted V2V data exchanges, ensuring that messages like collision warnings and traffic updates are genuine and originate from trusted sources.

Vehicle-2-Infrastructure (V2I) Authentication is necessary for smart transportation systems where vehicles must communicate with infrastructure like traffic lights or toll booths. Public keys authenticate these communications, ensuring that instructions or data received by the vehicle come from legitimate infrastructure components.

Conclusion

The anticipated impact of quantum computing in the automotive industry presents opportunities for advancement and significant challenges that necessitate further research and development. The potential of quantum computing to revolutionize multiple aspects is clear; however, the accompanying challenges, particularly in cybersecurity, pose the most pressing concerns. The vulnerability of current cryptographic methods to quantum attacks highlights a critical area for future research, mainly since cryptography is used in most automotive use cases.

The evolution of post-quantum cryptography (PQC) is thus not only a response to these emerging threats but a vital field of ongoing study. Efforts by institutions such as NIST and European security agencies to standardize quantum-resistant algorithms underscore the global recognition of this issue. Preparing for the quantum revolution in the automotive industry is more than a technological upgrade—it is a necessary step to safeguard against a rapidly evolving digital landscape.

Therefore, the industry must embrace quantum-resistant technologies as we move forward. This pursuit is about maintaining security and integrity and shaping the future of automotive technology in a post-quantum world. The path ahead is complex and uncharted, demanding a collaborative and innovative approach to harness the benefits of quantum computing while overcoming its challenges.