WHITE PAPER

CypherEye™
TRUSTED TRANSACTIONS

Cypher Shield

Agile Quantum Resistant Crypto Shield

Summary

The US intelligence agencies have put quantum computing and AI on the list of top potential threats to national security, along with nuclear weapons, terrorism, and climate change.

With classical computing becoming stronger as defined by Moore's law and the looming threat of Quantum Computing, current encryption models are under threat by ever increasing computing power. Most security and encryption standards over various transport protocols such as TCP/IP, Bluetooth, NFC and RFID thus, can be subject to various kinds of cyber-attacks.

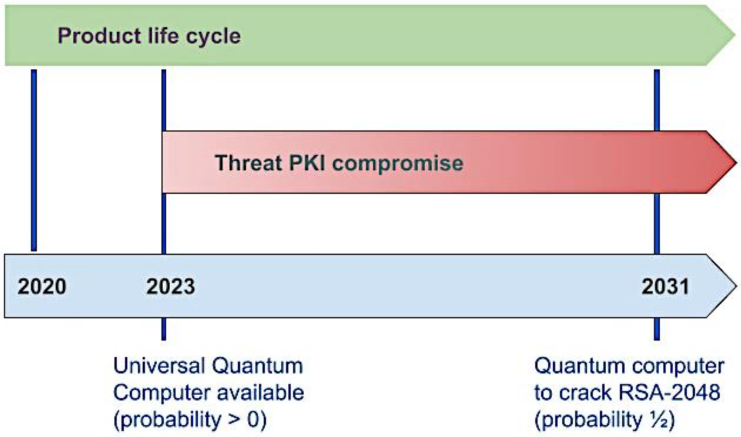
While several standardization efforts are under way to prevent this, these processes will take up to several years thus creating a vulnerability to our security infrastructure.

To solve this inevitably, impending crises, Cypher Shield has developed a very light weight and low latency shielding system based on a new set of mathematical algorithms that are not vulnerable to quantum computers.

Emerging Paradigm of Quantum Computing

Quantum computers promise huge advantages in many areas, such as faster data analysis and the search for unstructured data thus enabling us to solve problems that are very difficult or even impossible to solve using traditional computers.

In recent years there have been several significant and remarkable advances in the development of quantum computers. Technology giants in the US such as IBM, Microsoft and Google, as well as in other countries are heavily involved in the implementation of quantum computing and its applications.


Product life cycle
Threat PKI compromise
2020
2023
2031
Universal Quantum Computer available (probability > 0)
Quantum computer to crack RSA-2048 (probability ½)

Security Threats Posed by Quantum Computers

The powerful capabilities of quantum computers also pose an existential risk to our current encryption technologies. Many of the protocols used in mobile phones, credit cards, instant messengers, e-mail, wireless payment systems, banking payment systems, corporate information systems, unmanned vehicles, airplanes and other transport and power management information systems are under threat.

Modern public-key cryptosystems, such as RSA or elliptic curves, will become unsafe. Shore's algorithm shows how, using a quantum computer, the primary factorization of a large number and the calculation of discrete logarithms can be performed in polynomial time.

Symmetric key cryptography, such as Advanced Encryption Scheme (AES) or Secure Hash Algorithm (SHA) -2 and -3, will not be completely compromised, but the time need to compromise a symmetric scheme or hash function by means of a brute force attack is almost halved.

Post-Quantum Cryptography

Post-quantum cryptography leverages various mathematical schemes that move away from current industry standards that are based on mathematical problems like integer factorization or discrete logarithms. Currently, the industry recognizes the following five types of cryptosystems as promising candidates to replace the current systems:

- Hash-based
- Code-based
- Lattice-based
- Multivariate
- Super-singular isogeny-based

Each category focuses on a different set of mathematical problems, and for most of these proposals further research is needed in order to gain more confidence in their security and to improve their performance.

Action Needs to Be Taken Now

In determining when to take action, two important factors must be considered: the duration during which safety is required; and the time required to upgrade the system to a quantum-safe state.

Sophisticated software solutions and products usually have lengthy and difficult development processes. Also, many industries today develop products that have long lead times and so the security technology has to have a similarly long shelf life. This applies to the automotive, aerospace, transportation, critical infrastructure and other industries.

It also takes considerable time to transfer existing encryption methods to a new foundation.

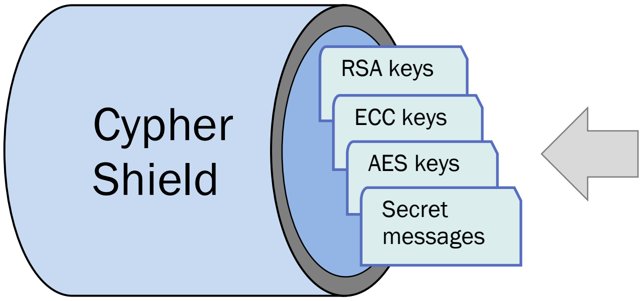
Data that needs to be kept secure for the next 10 years needs to use encryption algorithms that will be secure for the coming 10 years as well. Therefore, it is necessary to ensure that all sensitive data at risk is protected from such attacks by PQC methods.

Table: Comparing cryptosystem features

Features	Signatures	Encryption or Key Exchange	No protocol substitution	Fast computation	Low powered IoT devices	PKI secure, publishable
Multivariate Quadratic-based	●	○	○	○	○	○
Hash-based	●	○	○	○	○	○
Code-based	○	●	○	○	○	○
Isogeny-based	○	●	○	○	○	○
Lattice-based	●	●	○	○	○	○
Cypher Shield	●	●	●	●	●	●

Introducing Cypher Shield

Cypher Shield is an innovative platform based on an Agile Quantum Resistant Crypto Shield (AQRCS) technology to protect existing encryption protocols.



- The AQRCS method is not a symmetric or an asymmetric key exchange process in the traditional sense. It is a new concept of exchanging secret information, which can be conditionally called the "private-private keys" scheme without public key distribution.
- AQRCS does not replace or erase existing protocols, methods or algorithms. It creates an added level of quantum security that protects traditional key exchange algorithms (for instance RSA, ECC, AES, etc.) from quantum computer attacks.
- Or simply sends the secret information without ciphering (e.g. without encryption key use).

AQRCS does not rely on public keys. Only private keys are used, that are never shared in public space. The proprietary three-pass transaction algorithm exchanges information without disclosing any information about the users' private keys.

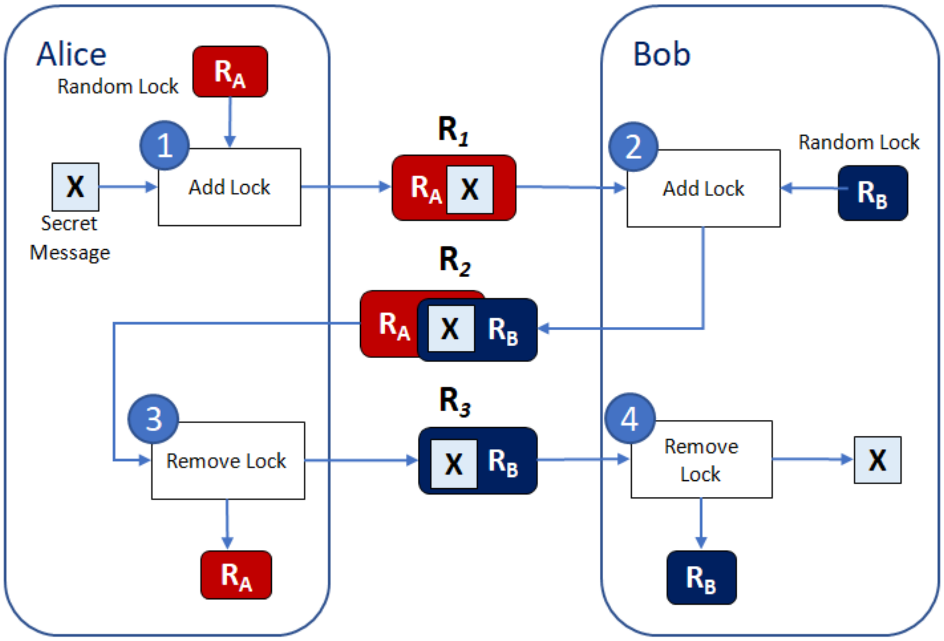
Every user uses his own private key, which is never shared with anybody. That is why there is no algorithms that can potentially decrypt the exchanged information.

The authentication system does not use public keys either. Even the reading of servers with an authentication system by hackers does not give any information about the private keys and information exchange. Therefore, the authentication system can be implemented in the form of a blockchain.

The mathematical resistance is based on the absence of preliminary public key distribution as well as any other information that relates to encryption method.

The developed cryptographic system is based on Underdetermined System of Equations and Uniform distribution of variables (white noise) that are used in multidimensional polynomial functions.

AQRCS is mathematically resistant to standard and quantum attack techniques thus robustly securing communications, messaging data, applications and devices.


Alice
Random Lock
R_A
1
X
Add Lock
Secret Message
R_1
R_A X
R_2
R_A X R_B
3
Remove Lock
R_A
R_3
X R_B
Bob
2
Random Lock
Add Lock
R_B
4
Remove Lock
X
R_B