

KR Maritime Cyber Safety News & Report



Vol. 053
Sep. 2022



CONTENTS

KR Activities

- KR, Cyber Security Presentation in Digital@sea Conference

Maritime Cyber Safety News

- UK increases maritime cyber focus with new 5-year strategy
- Does Failure to Communicate Undercut Your Cyber Resilience Strategy?

Maritime Cyber Security Project Series

- 5G's Effects and Cyber Threats on the Maritime

KR Cyber Security Column

- Seokjun Lee, Gachon University : Cryptography Evolving with Quantum Technologies

Advertisement

- KR Cyber Security Training Tool & E-LEARNING

KR, Cyber Security Presentation in Digital@sea Conference

Editor : AHN Jongwoo, Korean Register



The Ministry of Oceans and Fisheries held the 6th Asia-Pacific Regional Marine Digital International Conference for two days from September 15 to 16. The Asia-Pacific Conference has been held every year since 2017, and is an international consultative body that promotes cooperation related to marine digital technologies such as autonomous ships, beyond technical cooperation related to E-Nav.

6th Asia-Pacific Conference was attended by more than 100 experts, including international organizations such as the International Maritime Organization(IMO), International Association of Marine Aids to Navigation and Lighthouse Authorities(IALA), and the International Hydrographic Organization(IHO), government agencies and academia from 20 European and Asia-Pacific countries, including Denmark and Australia. The conference consisted of five sessions, with presentations and questions and answers under the themes of 'The role of maritime digitalization for De-Carbonization,' 'International standards of maritime digitalization and Sharing platforms,' 'Harmonious maritime digital transformation,' 'Maritime cyber security,' and 'Digital@Sea Conference and Promotion of e-Navigation.'

In Session 4 Maritime Cyber Security, PARK Kaemyoung, General Manager of Cyber Certification Team in Korean Register, presented about the cyber security in MASS System. "The cyber security threat is gradually increasing due to the digitization, automation, and networking of ships, and especially autonomous ships demand enhanced cyber security. In this environment, maritime industry stakeholders announced a number of cyber security guidelines for ships, and the demand for establishing and operating a cyber security system for ships is increasing." "In particular, shipyards and equipment companies should prepare to apply cyber security systems under the two URs, as IACS UR E26(Cyber Resilience for Ships) and E27(Cyber Resilience for onboard systems and equipment) will be applied to the ships contracted for construction after January 1, 2024.

UK increases maritime cyber focus with new 5-year strategy

Editor : AHN Jongwoo, Korean Register

Source : Smart Maritime Network

The UK government has set out a new 5-year maritime security strategy with a particular emphasis on cyber security, as the country looks to update its capabilities in protecting the industry and responding to threats.

“Alongside the robust protection of our physical assets, government continues to support the maritime sector to build resilience against a range of cyber threats including cyber espionage, cyber-crime, hacktivism, and ransomware,” the document says.

“In some areas, the UK maritime sector is already making the most of technological advances. In the management of ports, logistics, supply chains, the rollout of 5G networks and the consideration of autonomous shipping, the UK has made great progress.”

“As a consequence of a spike in the volume of incidents globally, the maritime sector has experienced a growth in ransomware attacks. Improvements in understanding the threat and taking appropriate mitigations will reduce the impact of successful cyber-attacks.”

The UK has pledged to support maritime organisations to build their resilience by providing advice and guidance on cyber best practice, in line with its recently published National Cyber Strategy, which sets out broader plans to strengthen cyber security and resilience across the country.

The Department for Transport has adopted the National Cyber Security Centre’s (NCSC) Cyber Assessment Framework (CAF) to guide operators on how to manage the security of their network and information systems to ensure continuity of essential services, based on Network and Information Systems Regulations that came into effect in 2018.

The UK government says it will also update its 2017 Cyber Security Code of Practice for Ships and work with the International Maritime Organization (IMO) to agree international standards and agreements.

Does Failure to Communicate Undercut Your Cyber Resilience Strategy?

Editor : AHN Jongwoo, Korean Register

Source : Cyberstar

Achieving effective communication between the various stakeholders in a business can be challenging under any circumstance. But it can become a real nightmare when you're in the midst of a severe crisis, such as a cyber attack that disrupts normal business operations. That's why establishing a crisis communication plan is essential to your cyber resilience plan, especially for the maritime and logistics industry where the complex infrastructures and geographical dispersion of stakeholders adds an extra layer of difficulty.

☐ The challenges of crisis communication during maritime cyber security incidents

When a crisis strikes, you're likely to run into a variety of sticky communication issues.

There is the obvious problem that normal communications platforms may be impacted and rendered non-operational during an attack. Beyond this it can be a real challenge to simply determine which parties to loop in using alternative communications channels. You need to know which stakeholders – executive team, managers, employees, partners, investors and customers need to be part of the conversation as the crisis response unfolds, before you can begin effective communications.

Deciding which information to share publicly, and which to restrict to internal communications channels, is another common challenge in times of crisis. In order to make these decisions, you must first assess the situation to understand the impact: was sensitive data accessed and downloaded? This can greatly affect the urgency and the nature of the communication needed.

In addition, you must take into account regulatory compliance; relevant regulations around cyber crisis communication, pertaining to your specific company under local or international law. This is usually under the jurisdiction of the legal department and must be considered before moving ahead with any form of crisis communication.

Once all this has been taken into account, you must also determine how to share information publicly:

- Which social media channels to post to
- Whether and how to send emails
- Where and how to release information to the press

Controlling the narrative is essential during crisis management and requires to be on top of all these elements, otherwise there is a risk of major reputation harm. However, it is also important to keep in mind that the cybercriminals can choose to leverage communication channels, by publishing details of the attack on social media, or by approaching customers.

And then there is the issue of making promises you can't keep during crisis communications. For instance, organizations have a tendency to say things like, "we'll provide daily updates as the situation unfolds," but fulfilling that promise can become challenging if there ends up not being something new to say every day. They may also fall into the trap of "communicating just to communicate," meaning that they release information that is not actually meaningful.

There are several overall concepts to consider in your communications, here are our recommendations:

1. Own it, accept responsibility for the situation
2. Avoid blaming others for the situation (even the cybercriminals...)
3. Downplaying the situation is usually not the answer. Instead consider demonstrating that you are taking it very seriously – stakeholders will appreciate this much more
4. Clearly address the main concerns of your stakeholders, in particular your customers
5. Decide how you will communicate any updates; provide ad-hoc solutions, offer compensation, etc.

☐ Principles for effective crisis communication and cyber resiliency

mitigate these risks, developing a communication response plan is vital. Your plan should identify:

- **Communications stakeholders:** First, decide who will handle communications during a crisis. It is important to decide who manages the internal communication (within the organization) and ensure that it is clearly coordinated with the external messaging. You may choose to rely on an in-house communications team, a third-party agency or both. You should also decide which C-level leaders, board members, legal representatives or regulatory consultants will need to be available to help prepare statements, decide which information to release and so on.
- **Communications channels:** Determine which channels you'll use to share information. Be sure to address both internal communication channels (such as those used by your teams to achieve business continuity) and external channels (where you'll reach customers, investors, partners and other stakeholders from outside your business). In addition, you can consider other contingencies including a dedicated landing page, FAQ page, or setting up a hotline for customers,
- **Communications workflows:** Establish who will prepare information, how it will be reviewed and how it will be released. Since these processes may vary between different types of communications (for instance, large customers might receive notifications directly from C-level executives, while smaller customers will be notified in a more generic manner), you should plan a different workflow for each type of information you may need to release during a crisis. Each of these workflows should be outlined into a written plan, to avoid any possible confusion.
- **Communication system contingencies:** It is important to prepare an alternative communication channel, in case normal communications systems (like email servers) are brought down by a cyber attack. Your communications plan should therefore identify which alternative systems you'll use to share information internally and externally during a crisis.

Develop a proper communication plan based on this information, which will serve as your formal crisis communications plan. Implement and test the plan on a routine basis. You can include these tests as part of your cyber drills, which are an opportunity to practice and enhance how stakeholders will respond during a crisis.

☐ Communication is a pillar of cyber resilience

Surviving a cyber attack hinges, in part, on maintaining effective communications during the crisis. Plan ahead by deciding which stakeholders to include in communication operations, how they'll share information and how you'll maintain communication channels in the event that key systems are brought down during an attack.

5G`s Effects and Cyber Threats on the Maritime

Editor : YOO Jinho, Korean Register

series news



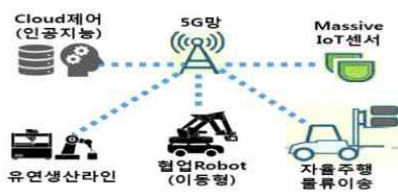
① What is 5G?

- ② 5G Network architecture, Network Slicing technology, and Affects on the maritime Industry
- ③ Comparison between LTE centralized network and 5G distributed network
- ④ Role of wireless backhaul technology and 5G satellites in 5G standards
- ⑤ The private network reference model in 5G standard for effective use in ships and ports

What is 5G?

5G guarantees data transmission and reception capacity and speed in mobile communication environment, no difference between wired and wireless. Also, the 5G guarantees service stability even in IoT communication environments where many devices are connected and low power in device use. we inquire to a new communication technology “seconds to download movies”. However, 5G is not just a technology that aims to improve communication data rates, but an ICT convergence technology that is based on the requirements of a wide range of industries such as automobiles, railways, cities, and factories.

Core Performance		4G	5G	More than 4G
Speed	Maximum transmission speed	1 Gbps	20 Gbps	20 times
Latency	Transmission latency	1 sec / 100 min	1 sec / 1,000 min	1/10
Connectivity	Maximum device connection	100,000/km ²	1,000,000/km ²	10 times

[Speed] Real time Media	[Latency] V2X	[Connectivity] Smart Factory
360° wireless hologram 	Full Autonomous Driving(Level 4) 	Wireless production system 

Source : http://www.gokea.org/bbs/down.php?file_no=20262

What is 5G?(Continue page)

It wants to find out how 5G will be applied to the maritime environment in ships, Maritime IoT and Smart ports. This newsletter will briefly introduce some features of the 5G and explain them in more detail in the next newsletter issue.

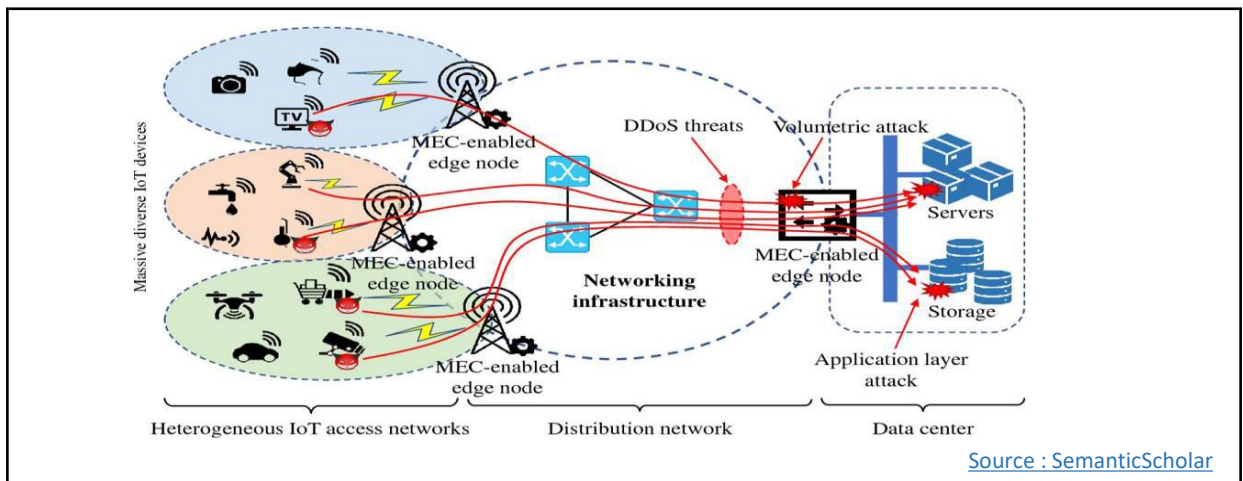
- **Network Slicing** : It is possible to virtualize on the same physical network infrastructure, to diversify independent logical networks, and to have 5G communication requirements suitable for the marine environment, such as ships and marine IoT devices, through network slicing.
- **Mission Critical Service** : 5G's low latency and high reliability (URLLC) technology is used for disaster communication, autonomous driving, railroad communication, and can be used for services for preventing ship collisions.

Source : <https://www.3gpp.org/DynaReport/22819.htm>

5G's Cyber Security risks - Possibility of DDOS attacks

Unlike traditional communication networks, which are closed to each industry and use, 5G is designed to be open and distributed according to use. This is called network slicing, where a network is divided into virtual dedicated networks such as communication, IoT, VR, and autonomous driving. However, because all devices are physically connected to 5G, malware can spread at a very rapid rate, and the base station is likely to be attacked by DDoS attacks from a large number of infected devices.

The market demand for new security technologies such as blockchain and quantum cryptography will spread, to provide a defence against cyberattacks while using 5G's ultra-fast and high-density features.





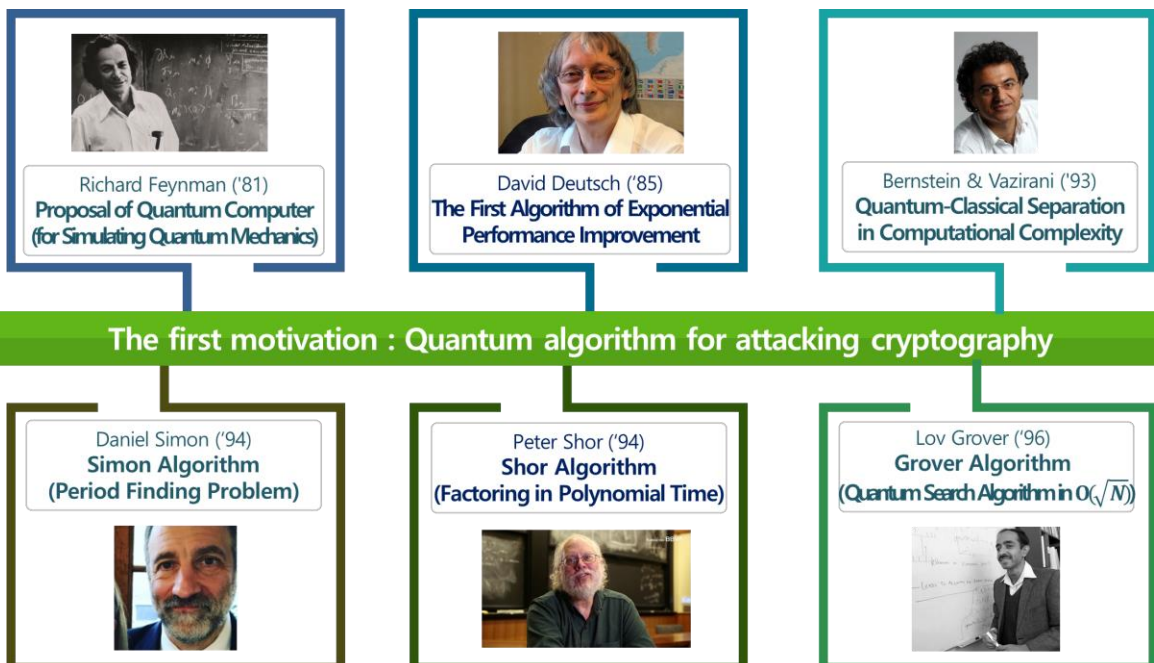
Cryptography Evolving with Quantum Technologies

Editor : Prof. Seokjun Lee, Gachon University

● Advances in quantum computing and its threats to the cryptosystems

Currently, one of the most noteworthy technologies related to next-generation cryptography is related to quantum computing. Quantum mechanics, which was born from Max Planck's energy quantization hypothesis in the early 1900s, was gradually completed in the Copenhagen interpretation in the late 1920s and in the controversy among physicists. It was combined with ICT technology in the early 1980s and began to have a great influence on cryptography.

In the early 1980s, a quantum computer was conceptually proposed by R. Feynman. Prof. Feynman, who was simulating quantum mechanics with a computer at that time, argued that a much more efficient simulation would be possible if a computer using quantum phenomena was developed. Quantum computers, which were discussed at the level of ideas, began to attract



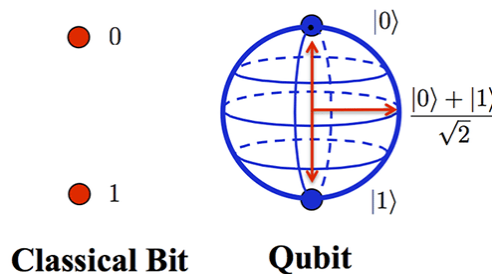
<The first motivation for quantum computer development>

many scholars when D. Deutsch proposed the first quantum algorithm with exponential performance improvement compared to classical computers in 1985.

Afterwards, in 1994, P. Shor theoretically proved that public key cryptography based on discrete logarithmic or factorization problems can be attacked by quantum computers. There is currently no quantum hardware technology capable of attacking RSA, DH, or ECC, but it will pose a significant threat to the existing cryptographic system.

Why is quantum computer faster than classical computer?

Quantum computers utilize the properties of quantum states, such as superconducting elements, ion traps, photons, and so on. It uses qubit or quantum bit that can have superposition states of 0 and 1 instead of classical bit that can store information of 0 or 1. The operations on N-qubit with superposition state is equivalent to performing 2^N classical operations simultaneously, showing that parallel computation is possible with exponential performance improvement.



<Classical bit and Qubit>

(Source: <https://www.autodesk.com/products/eagle/blog/future-computing-quantum-qubits/>)

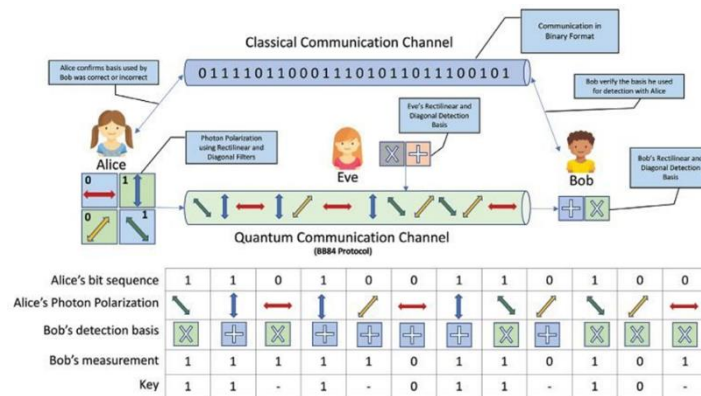
However, it is impossible to accurately read the superposition state from qubit. Since it collapses into a single state of 0 or 1 when reading the data (or measuring the qubit), it is impossible to show exponential performance improvement for all computational problems. Quantum computer can solve only some problems such as factorization quickly with high probability.

In 2019, Google, with UCSB, published a research result in the Nature that, for the first time, they solved a problem in 200 seconds on its 54-qubit quantum processor Sycamore, with arguing that the problem took 10,000 years with a supercomputer. Furthermore, global companies and governments are investing heavily in the development of quantum computers. For example, IBM announced the quantum processor Eagle with 127 qubits and also opened the quantum roadmap to develop more than 4,000 qubits by 2025.

Advances in Quantum Cryptography Technology

The literal meaning of quantum cryptography can be seen as a field of cryptography that utilizes the features of quantum mechanics for cryptographic work or secure transmission of data. In other words, it includes not only encryption/decryption to simply support the confidentiality of data, but also the cryptographic functions such as key generation, key distribution, random number generation, or digital signature. All of the cryptographic fields exploiting quantum technologies can be said to be quantum cryptography.

The start of quantum cryptography is considered to be a quantum key distribution technology proposed by C. Bennett and G. Brassard in 1984. Although it has been developed independently of the quantum computer, it is believed to have quantum safety.



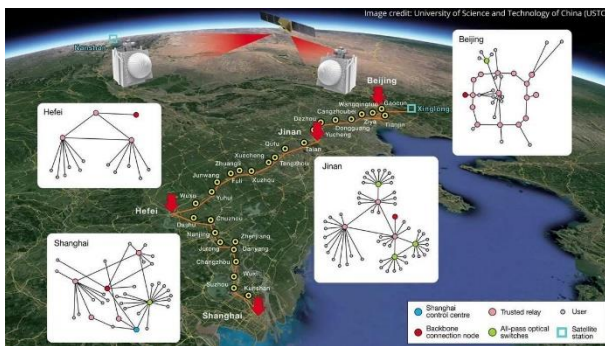
<Quantum key distribution protocol by C. Bennett and G. Brassard (1984)>

Quantum key distribution process proposed by C. Bennett and G. Brassard

- ① Alice creates a random bit stream that she wants to send to Bob
- ② She randomly select the basis (rectilinear or diagonal) for each bit in the above bit stream
- ③ Alice transmits a random bit string 0 or 1 by polarizing the photon according to the selected basis.
- ④ Bob receives to observe a photon using a random basis. If the basis selected by Alice and Bob are the same, the same bit value is observed, otherwise the probability with equal bit value is 1/2)
- ⑤ When all bit streams are transmitted, Alice and Bob exchange randomly selected base information through the authenticated classical channel and extract only the bit stream corresponding to the same base (the same value should be extracted if there is no eavesdropper)
- ⑥ After measuring the error rate (QBER, Quantum Bit Error Rate) by exchanging some of the extracted bit strings, if the error rate does not exceed a certain level, it is determined that there was no eavesdropping and the remaining part of bit stream is used as the key.

Trends in Quantum Cryptography Technology

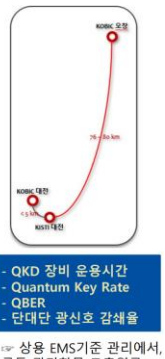
The European OpenQKD project (<https://openqkd.eu/>) is being conducted through 38 partners in 13 countries through the quantum key distribution testbed of the H2020 program, with various use-cases. In 2017, China succeeded in quantum cryptography communication between Beijing and Vienna over a distance of 7,600 km between Beijing and Vienna through the quantum communication satellite Micius, and built a 4,600 km fiber optic network that integrates two satellite-terrestrial communicators and 700 QKD links. In Korea, SKT has constructed a quantum cryptography network that connects Bundang, Seongnam, Suwon, Yongin, and Yangpyeong, and KISTI has built a quantum cryptography test network that can test the QKD system and security service utilizing QKD in KREONET.



<QKD networks in China>



<KISTI Quantum cryptography-based experimental network >



Disadvantages of quantum key distribution

Quantum cryptography including quantum key distribution (QKD) technology is not a technology that has been developed to counter the threat of quantum computers from the beginning, and has the following limitations. However, despite of these limitations, there is a possibility that it can be used in some applications where absolute safety is important.

- It can be applied and implemented only in the physical layer, and expensive equipment is required.
- Since it is a point-to-point protocol, it is difficult to satisfy the end-to-end security of the conventional application layer.
- Presumably susceptible to denial-of-service attacks, especially in relation to receivers
- It requires the sharing of authenticated information through classical communication.
- It is difficult to replace all the various data security functions (user/message authentication, signature, etc.) provided by the existing public key cryptography.

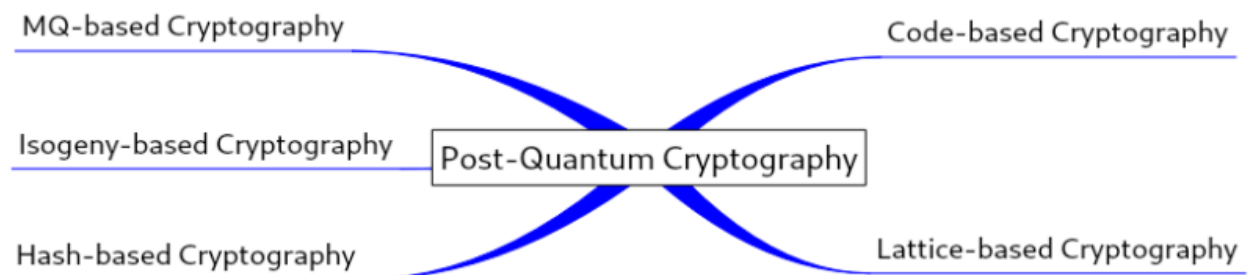
● The research in post-quantum cryptography area

The lattice-based cryptography proposed by M. Ajtai in 1996 stands on the SVP (Shortest Vector Problem) that it is difficult to find the shortest vector in polynomial time when basis vectors are given in a specific lattice, and CVP(Closest Vector Problem) that it is difficult to find the vector closest to a specific point. Until now, this shows the best performance in terms of the performance and size of public/private key and encrypted/signed text, compared to other techniques. LWE (Learning with Error) and LWR (Learning with Rounding) techniques, which are variants of the SVP or CVP problem, make it difficult to find the secret value by applying error or rounding to the matrix equation formed by the vector, respectively.

The multivariate quadratic (MQ)-based cryptography was proposed by T. Matsumoto and H. Imai in 1988. Many optimization techniques have appeared to solve the drawbacks caused by a large key size. But they could make security vulnerabilities in many cases.

Code-based cryptography, which started from the code theory to handle errors in communication, was proposed by R. McEliece in 1978. this has been well evaluated in terms of security, not showing any significant attack points, but there are disadvantages due to the large key.

In addition, numerous algorithms inherently resistant to the threat of quantum computers, such as hash-based signature technology and elliptic curve Isogeny-based cryptography, have been studied so far.



<The types of PQC>

● The standardization in post-quantum cryptography

NIST (National Institute of Standards and Technology) in the United States, which standardized major cryptographic algorithms such as AES, SHA, and ECC through a public procedure, has been preparing for standardization of quantum-resistant cryptography since 2015. PQC standardization by NIST was divided into PKE (public key encryption)/KEM (key encapsulation method) algorithm and digital signature algorithm (DS) tracks. After Round 1/2/3 in 2017/2019/2020, 4 draft standard algorithms (1 lattice-based PKE/KEM, 2 lattice-based digital signatures, and 1 hash-based digital signatures) were announced in July 2022. Round 4 process was announced additionally for 4 types of PKE/KEM. Among them, CRYSTALS-Kyber and CRYSTALS-Dilithium are recommended as primary algorithms and are expected to be used soon. Lattice-based cryptographic method was mainly selected based on the performance and safety analyzed so far. However, we should discuss other types of cryptography because there is no guarantee that the cryptography is completely secure. The era of PQC to prepare for quantum threats is coming in earnest.

PKE/KEM	Digital Signatures
CRYSTALS-KYBER (Lattice)	CRYSTALS-Dilithium (Lattice) FALCON (Lattice), SPHINCS ⁺ (Hash)
PKE/KEM 4 Round Candidates	
BIKE (Code), Classic McEliece (Code), HQC (Code), SIKE (Isogeny)	

<NIST PQC Standardization 3 Round Results>

Timeline	PQC Standard Processes
2015.08	NSA, "IAD will initiate a transition to quantum resistant algorithms ..."
2016.02	NIST Report on PQC (NISTIR 8105) and announcement for standardization
2016.08 ~ 2016.09	NIST, Draft submission requirements & evaluation criteria
2016.12	Final requirements and criteria in 3 areas (Digital signature, Encryption, Key Encapsulation)
2017.11	82 PQC candidates received from All around the world
2017.12	69 PQC Candidates accepted (Round 1)
2019.01	26 PQC Candidates announced (Round 2)
2020.07	7 Final PQC Candidates and 8 Alternative Candidates (Round 3)
2022.07	4 PQC Draft Standards and 4 additional candidates announced (Round 4)
2024	1st Standards will be published

<NIST PQC Standardization Timeline>

KR CS++



No.	Titles
1	Understanding of Maritime Cyber Security
2	Practice of Maritime Cyber Security
3	Administrative Security
4	Cyber Asset, Threat and Technical Security
5	KR Cyber Security Type Approval
6	Understanding of Maritime Cyber Security Risk Assessment
7	KR Remote Cyber Survey

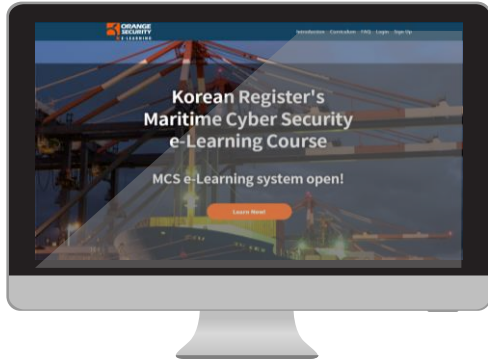
KR launched KR CS++, maritime cybersecurity training tool.

KR CS++ was produced in USB type and tablet type for effective cybersecurity training of seafarers in an environment where cybersecurity training is difficult due to the unstable Internet environment on ships. In addition, KR is striving for customer satisfaction by providing various types of services.

Currently, the same service is provided through cybersecurity e-learning education.

Online Training

KR Maritime Cybersecurity e-Learning Center training course



Q&A : <https://edu.orangecq.com/>

KR reorganized the cyber security e-learning training in cooperation with Orange Security, who is a maritime cyber security specialist. Through this reorganization of e-learning training, KR becomes to provide customized training for each customer.

New curriculum consists of Maritime cyber security Awareness, cyber security Practical Management, cyber security Officers and cyber security Type Approval. Maritime cyber security Awareness is a course to raise awareness of maritime cyber security for employees including crews, which includes two modules - Understanding of Maritime Cyber Security and Practice of Maritime Cyber Security. cyber security Practical Management is a course for ship officers and engineers, which includes KR Remote Cyber Survey as well as Maritime cyber security Awareness course. cyber security Officers is for the person in charge of managing cyber security system and responding classification cyber security survey. This course consists of Administrative Security, Cyber Asset, Threat and Technical Security, Understanding of Maritime Cyber Security Risk Assessment with all modules in cyber security Practical Management. Finally, KR Cyber Security Type Approval is a course for equipment company and provides introduction of international standard related to requirements of cyber security for equipment and materials required for obtaining KR cyber security type approval.



Providing the best services, Creating a better world

Cyber Certification Team, Korean Register
(46762) 36, Myeongji ocean city 9-ro, Gangseo-gu, Busan Republic of Korea
Tel +82 70 8799 8595
Fax +82 70 8799 8594
www.krs.co.kr

Copyright © 2022 ALL RIGHTS RESERVED BY KOREAN REGISTER