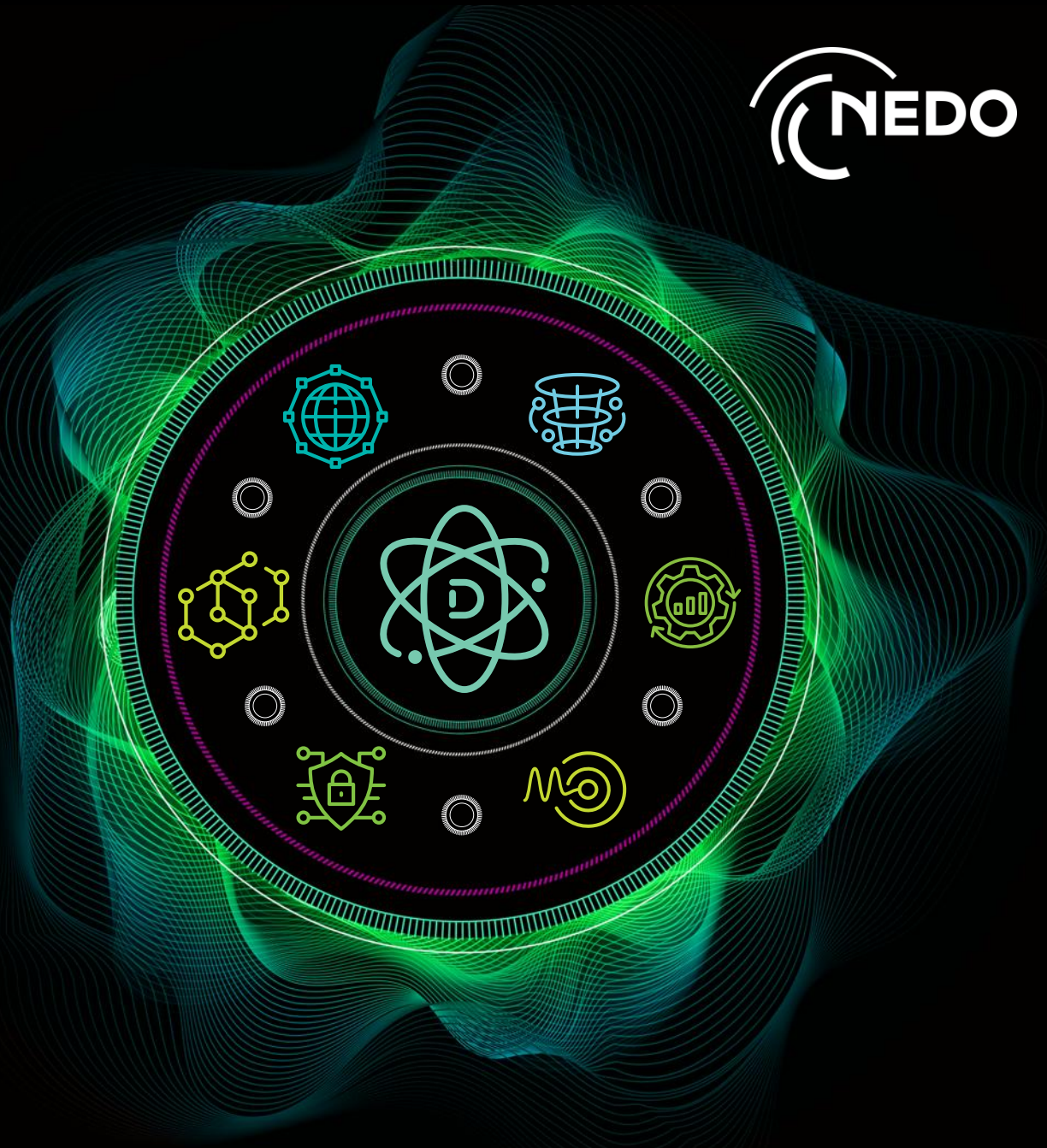
Quantum Computing Use Cases

Evaluation of RSA Cryptanalysis

Fujitsu



New Energy and Industrial Technology Development Organization (NEDO)

Fujitsu: Evaluation of RSA Cryptanalysis [2023/01] 1/2

Validation

Industry	Other
Method	cryptanalysis
Process	–
Category	Gate*

Background

- Based on **the security of public key cryptography (RSA cryptography, etc.) is the difficulty of the prime factorization problem**, 2,048 bit composite numbers are widely used.
  - ✓ *1 because the number of combinations that can be deciphered by classical computers is 829 bits.
  - ✓ The composite number of prime factorizations N=p x q(p and q are different prime numbers)
- **Although studies have been carried out to efficiently solve the prime factorization by classical computers, the number-field sieve method, which is the most asymptotically fast algorithm at present, requires quasi-exponential time for the digit length of the composite number N and is difficult to decipher.**
  - ✓ Even if a supercomputer is used by applying the number field sieve method to the prime factorization of 2,048 bit composite numbers, *2 is estimated to be required for several decades or more even for the fastest supercomputer (Linpack performance of 1018FLOPS).
- But **with the advent of quantum computers and the fast computable Shor algorithm, the RSA cipher has been shown to be breakable in a realistic amount of time,** and is now theoretically cracked.
  - ✓ **The complexity of the Shor algorithm is a polynomial of N digits in length** time, **exponentially accelerated from the computation time of a classical computer**

Issues and motivation to be solved

- **The advent of quantum computers threatens the security of cryptography, but there are few experimental cases to verify how much computational resources of quantum computers are actually required to decrypt RSA cryptography, making it difficult to estimate.**
- Thus, **Fujitsu has utilized a quantum simulator to demonstrate prime factorization to assess the security of a 2,048 bit RSA cipher.**

*1:「[Cado-nfs-discuss] Factorization of RSA-250」(https://web.archive.org/web/20200228234716/https:/lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html)
*IEICE "Security in the Age of Quantum Computers: Trends in Quantum-Resistant Computer Cryptography " (https://app.journal.ieice.org/trial/106_11/k106_11_966/index.html)
Fujitsu Limited, "Successful Security Assessment of RSA Cryptography with Quantum Simulator" (https://pr.fujitsu.com/jp/news/2023/01/23.html)
*Gate（gate-based）: A computing approach in which operations are applied sequentially to qubits to perform calculations. Similar in concept to logic circuits in classical computers, it can address a wide range of problems.

Fujitsu: Evaluation of RSA Cryptanalysis [2023/01] 2/2

Validation

Industry	Other
Method	cryptanalysis
Process	–
Category	Gate*

Problem setting as a quantum computer

- **Resource evaluation of quantum computer required to decode 2048 bit RSA cipher** generally used at present was carried out.
- In the computer experiments, **a general-purpose program for generating a quantum circuit that factorizes input composite numbers was implemented in a quantum simulator using Shor's algorithm,** and **a quantum circuit that factorizes several composite numbers from 10 bits to 25 bits was actually generated.**
- **Estimation of the computational resources of the quantum circuit required for factoring 2,048 bit composite numbers was performed from the computational resources required at that time.**
- Using our in-house developed **39 qubit quantum simulator** to perform prime factorization
  - ✓ The quantum simulator takes advantage of the high speed of the Fugaku supercomputer's A64FX CPU and Fujitsu's massively parallel computing technology

Expected business benefits

- **They** successfully factorized 96 prime numbers from N=15 to N=511, confirming that a general-purpose program can generate the correct quantum circuit.
- From the calculation resources required for a quantum circuit that factorizes several composite numbers from 10 bits to 25 bits, it was shown that **104 days of computation is required even if a quantum circuit with the following specifications is used** to factorize a 2,048 bit composite number.
  - ✓ Number of qubits: Approximately 10,000 qubits
  - ✓ Number of gates: approximately 2.23 trillion
  - ✓ Quantum computation steps: about 1.8 trillion
- However, because it is **difficult to develop a stable FTQC in the short term** at large scales and for long periods of time (104 days of keeping qubits intact), **the 2,048 bit RSA cipher is safe against the Shor algorithm**.

Fujitsu Limited, "Successful Security Assessment of RSA Cryptography with Quantum Simulator" (https://pr.fujitsu.com/jp/news/2023/01/23.html)
*Gate（gate-based）: A computing approach in which operations are applied sequentially to qubits to perform calculations. Similar in concept to logic circuits in classical computers, it can address a wide range of problems.

More use cases are available on our website. We invite you to explore them.
https://www.quantum-computing-use-cases.nedo.go.jp/english/

More Use Cases

New Energy and Industrial Technology Development Organization (NEDO)
AI and Robotics Department (e-mail: quantum_ai@ml.nedo.go.jp)

This collection of use cases was obtained as a result of the work commissioned by the New Energy and Industrial Technology Development Organization (NEDO) "Cyber-Physical Development Business of Quantum/Classical Hybrid Technology/Study of Use Case of Quantum Technology" and the "Post-5G Information and Communications System Infrastructure Reinforcement R & D Project (Quantum Industrialization)/Comprehensive Study for Promoting the Industrialization of Quantum Computers".