6th ETSI/IQC Quantum-Safe Workshop
Beijing, November 6-8, 2018
Session 1: World Tour

# Post-Quantum Cryptography and Japan CRYPTREC

**Shiho Moriai**
Director
Security Fundamentals Laboratory
Cybersecurity Research Institute
NICT

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

# If Large-scale Quantum Computers are ever Built, …

» they will be able to break many of the public-key cryptosystems currently in use…

# But…

- Will people willingly accept transition to post-quantum cryptography?

- Transition takes time and effort.
  It is not easy.

**SHA-1** **SHA-3**

# The North wind and the Sun

**“If Large-scale Quantum Computers…”**

**“Privacy Preserving Data Analysis”**

**Which accelerates deployment of Post-Quantum Crypto?**

# Why Post-Quantum Crypto?

» **Long-term Security**

> Rather than “quantum-resistant” crypto

» **Promising Functionalities** e.g.

> Privacy preserving data analytics by lattice-based homomorphic encryption

# Big Data Integration :
# Key to the new growth strategy

# Security and Privacy: Key Issues for Datability

# To Promote Big Data Integration across Sectors


**Data Analytics**

Security and Privacy Enhancing Technologies

While Encrypted/ Preserving Privacy

Create Value across Sectors
Innovation, Productivity, Growth

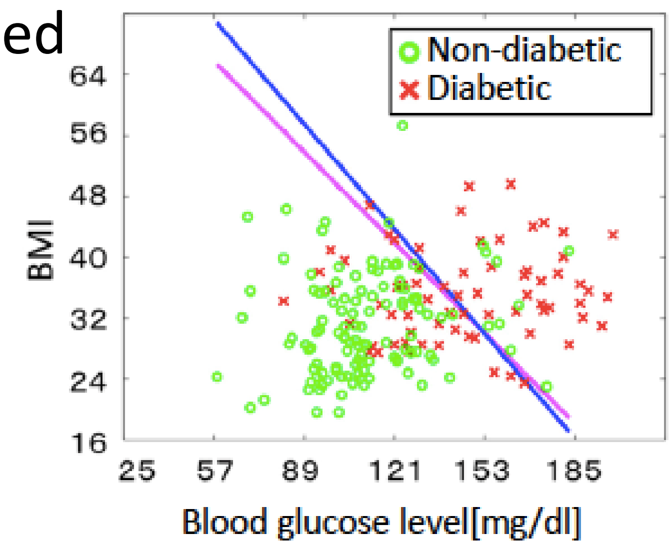
# Privacy Preserving Data Analytics

» **Privacy-Preserving Logistic Regression**

> powerful machine learning tool to classify confidential/ personal data

> Proposed a secure system for protecting both the training and predicting data in logistic regression using lattice-based homomorphic encryption.

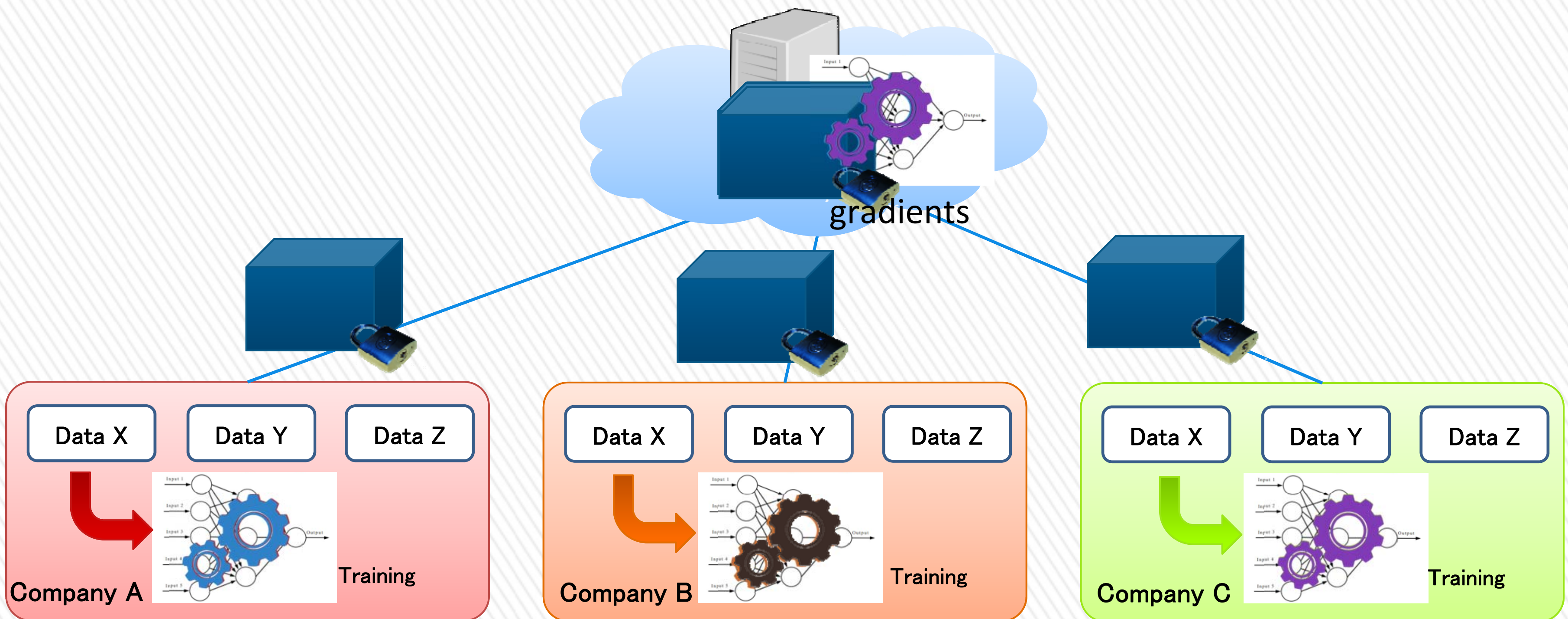
> Classify 100 million encrypted data in 30 min




Y. Aono, T. Hayashi, L.T. Phong, L. Wang, “Privacy-Preserving Logistic Regression with Distributed Data Sources via Homomorphic Encryption”, IEICE Trans. Inf. & Syst., VOL.E99-D, No.8 August 2016.

# Privacy Preserving Deep Learning

- » Many learning participants perform deep learning over a combined dataset of all, without revealing the participants' local data.
- » Using additively homomorphic encryption we improved the previous work by Shokri et al (ACM CCS 2015).



# Japan CRYPTREC

Cryptography Research and Evaluation Committees

- Project to evaluate and monitor the security of c ryptographic techniques used in Japanese e- Government systems

» Goal of the project

- To ensure the security of Japanese e-Government s ystems by using secure cryptographic techniques and t o realize a secure IT society.

# Three Lists in the CRYPTREC Ciphers List

**e-Government Recommended Ciphers List**

> Recommended ciphers approved by CRYPTREC in terms o f security and implementation aspects as well as current a nd future market deployment.

**Candidate Recommended Ciphers List**

> Candidate recommended ciphers approved by CRYPTREC in terms of security and implementation aspects.

**Monitored Ciphers List**

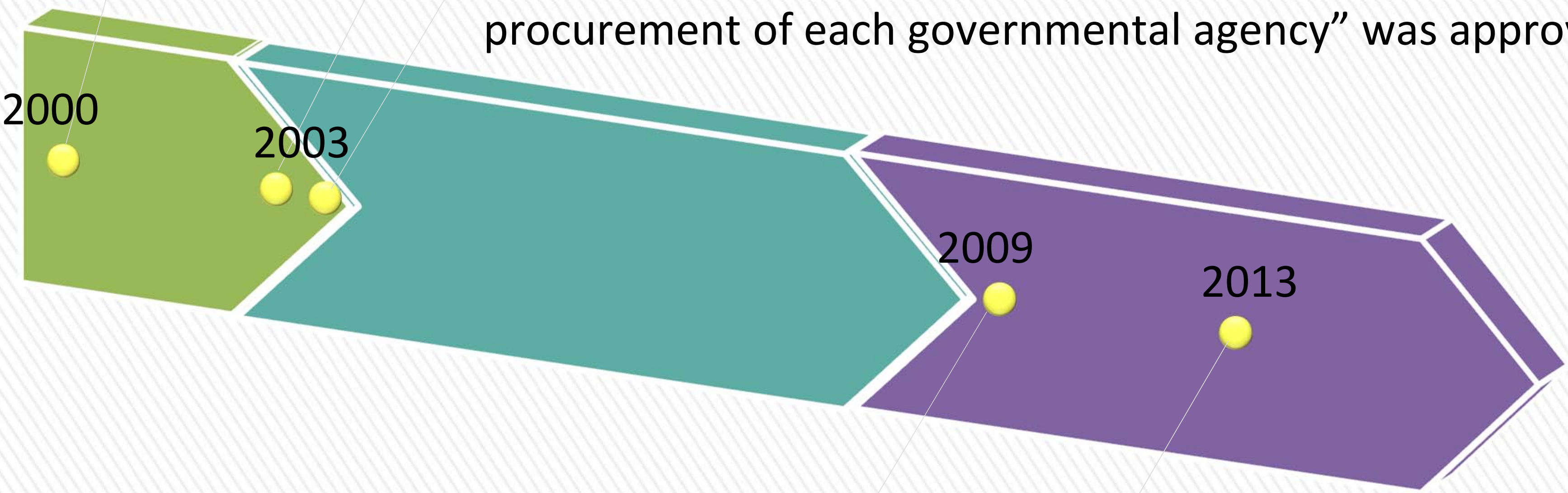
> The ciphers are not-recommended for use because of high risk of compromise while they are allowed to use only for interoperability with legacy systems.

# History of CRYPTREC

CRYPTREC launch, Call for cryptographic techniques

Publication of the e-Government Recommended Ciphers List

“Policy for the use of ciphers in information system procurement of each governmental agency” was approved




Call for cryptographic techniques for the revision of the e-Government Recommended Ciphers List

Publication of the CRYPTREC Ciphers List

# e-Government Recommended Ciphers List

| Classification | | Cipher |
|---|---|---|
| Public key ciphers | Signature | DSA |
| | | ECDSA |
| | | RSA-PSS |
| | | RSASSA-PKCS1-v1_5 |
| | Confidentiality | RSA-OAEP |
| | Key exchange | DH |
| | | ECDH |
| Symmetric key ciphers | 64-bit block ciphers | N/A |
| | 128-bit block ciphers | AES |
| | | Camellia |
| | Stream ciphers | KCipher-2 |
| Hash functions | | SHA-256 |
| | | SHA-384 |
| | | SHA-512 |
| Modes of operation | Encryption modes | CBC |
| | | CFB |
| | | CTR |
| | | OFB |
| | Authenticated encryption modes | CCM |
| | | GCM |
| Message authentication codes | | CMAC |
| | | HMAC |
| Authenticated encryption | | N/A |
| Entity authentication | | ISO/IEC 9798-2 |
| | | ISO/IEC 9798-3 |

# CRYPTREC Organization

NISC National center of Incident readiness and Strategy for Cybersecurity

Management Standards for
Information Security Measures
for the Central Government Computer Systems

総務省 MIC Ministry of Internal Affairs and Communications

**Advisory Board for Cryptographic Technology (Secretariat:MIC,METI)**

経済産業省 Ministry of Economy, Trade and Industry

NICT 国立研究開発法人 情報通信研究機構 National Institute of Information and Communications Technology

IPA 独立行政法人 情報処理推進機構 Information-technology Promotion Agency, Japan

## Cryptographic Technology Evaluation Committee (Secretariat:NICT,IPA)

(1) Monitoring and evaluation of the security and implementation properties of the cryptographic technology
(2) Research on new-generation cryptographic technology
(3) Research on secure utilization of cryptographic technology

**Cryptanalysis Evaluation WG**

## Cryptographic Technology Promotion Committee (Secretariat:NICT,IPA)

(1) Research on the promotion of cryptographic technologies and the strengthening of IT security industries
(2) Research on the utilization status of cryptographic technologies and research of their promotion strategy
(3) Research on the strategy of cryptographic policy from mid-and-long term viewpoints

# Cryptanalysis Evaluation WG

» Goal

> Survey and research on the security of public-key crypto- systems for current and future uses

» Recent Activities

> Survey and research on post-quantum cryptography

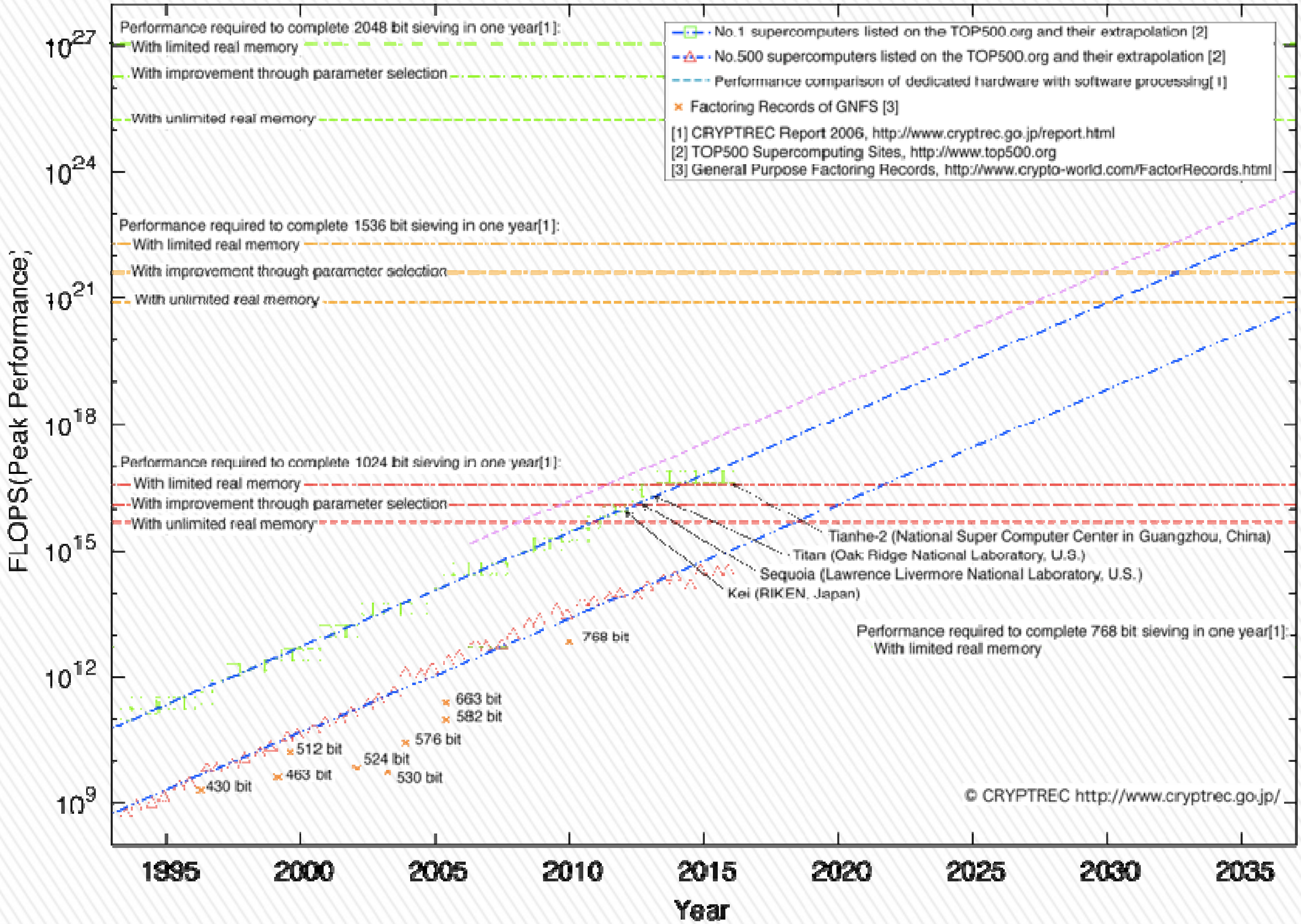
+ A report on PQC will be published in FY 2018.

> Update of the complexity required for Integer Factoring

» Chair

> Prof. Tsuyoshi Takagi (Univ. of Tokyo)

# Complexity required for Integer Factoring



# PQC Standardization Plan