Activities on PQC in Japan

Keita Xagawa (NTT Social Informatics Laboratories)

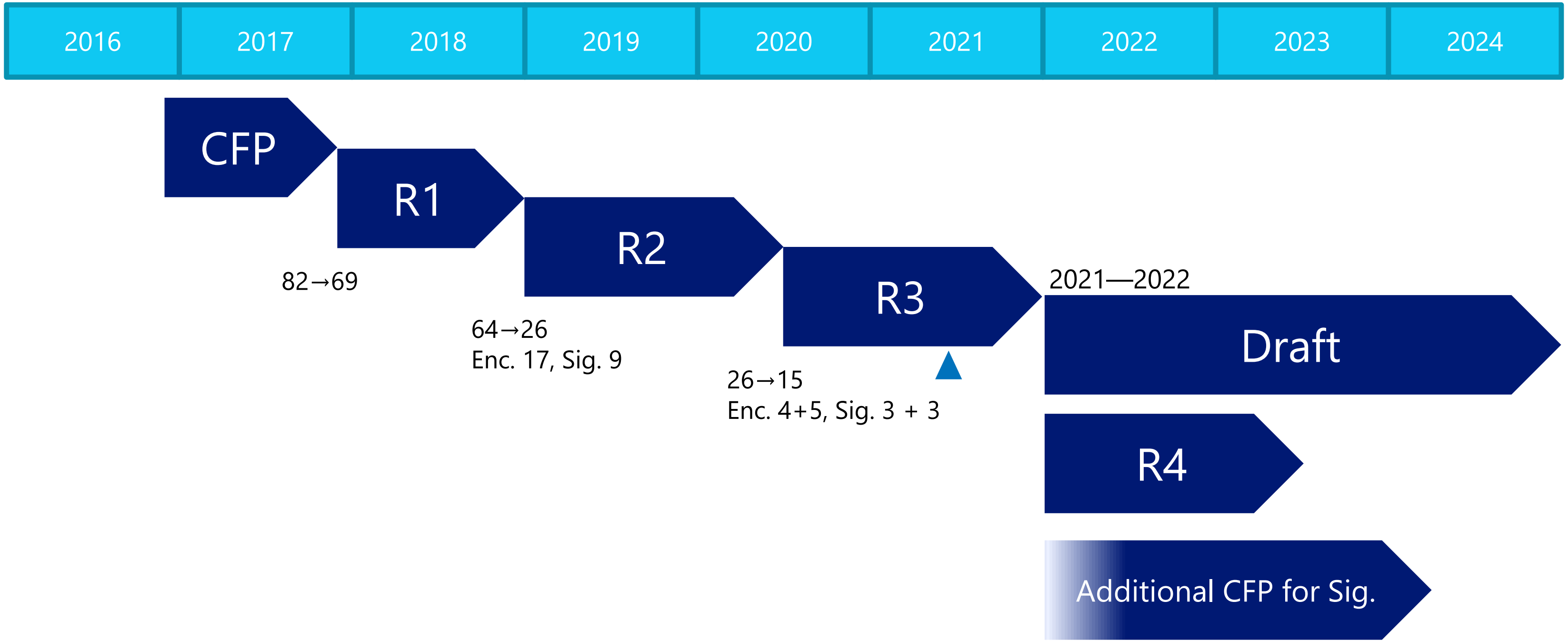
2021/07/16 @PQCRYPTO 2021

Contents

- NIST-PQC Activities from Japan
- PQC Transition in CRYPTREC
- Other activities

NIST-PQC Activities from Japan

NIST PQC Timeline



2016 2017 2018 2019 2020 2021 2022 2023 2024

CFP

R1

82→69

R2

64→26
Enc. 17, Sig. 9

R3

26→15
Enc. 4+5, Sig. 3 + 3

2021—2022

Draft

R4

Additional CFP for Sig.

NIST PQC Round1 69 Candidates

BIG QUAKE, BIKE, CFPKM, Classic McEliece, Compact LWE, CRYSTALS-Dilithium, CRYSTALS-Kyber, DAGS, Ding Key Exchange, DME, DRS, DualModeMS, Edon-K, EMBLEM and R.EMBLEM, Falcon, FrodoKEM, GeMSS, Giophantus, Gravity-SPHINCS, GuessAgain, Gui, Hila5, HiMQ-3, HK17, HQC, KCL, KINDI, LAC, LAKE, LEDAkem, LEDApkc, Lepton, Lima, Lizard, LOCKER, LOTUS, LUOV, McNie, Mersenne-756839, MQDSS, NewHope, NTRUEncrypt, pqNTRUsign, NTRU-HRSS-KEM, NTRU Prime, NTS-KEM, Odd Manhattan, Ouroboros-R, Picnic, Post-Quantum RSA-Encryption, Post-Quantum RSA-Signature, pqsigRM, QC-MDPC KEM, qTESLA, RaCoSS, Rainbow, Ramstake, RankSign, RLCE-KEM, Round2, RQC, RVB, SABER, SIKE, SPHINCS+, SRTPI, Three Bears, Titanium, WalnutDSA

R1 Candidates inv. Japanese Org.

- **Classic McEliece:** incl. T. Chou (Osaka U.)
- **Ding Key Exchange:** incl. T. Takagi, Y. Wang (UT, Kyushu U.)
- **Giophantus:** K. Akiyama, H. Shimizu (Toshiba) , Y. Goto (HUE), S. Okumura (Osaka U.), T. Takagi, Y. Ikematsu (Kyushu U.), K. Nuida, G. Hanaoka (AIST)
- **LOTUS:** L. T. Phong, T. Hayashi, Y. Aono, S. Moriai (NICT)
- **RaCoSS:** incl. K. Fukushima, P.S. Roy, R. Xu, S. Kiyomoto (KDDI), T. Takagi (UT)

R2 Candidates inv. Japanese Org.

- **Classic McEliece:** incl. T. Chou (Osaka U.)
- ~~**Ding Key Exchange:** incl. T. Takagi, Y. Wang (UT, Kyushu U.)~~
- ~~**Giophantus:** K. Akiyama, H. Shimizu (Toshiba) , Y. Goto (HUE), S. Okumura (Osaka U.), T. Takagi, Y. Ikematsu (Kyushu U.), K. Nuida, G. Hanaoka (AIST)~~
- ~~**LOTUS:** L. T. Phong, T. Hayashi, Y. Aono, S. Moriai (NICT)~~
- ~~**RaCoSS:** incl. K. Fukushima, P.S. Roy, R. Xu, S. Kiyomoto (KDDI), T. Takagi (UT)~~

R3 Candidates inv. Japanese Org.

- **NTRU:** incl. T. Saito, K. Xagawa, T. Yamakawa (NTT)
- **Classic McEliece?:** incl. T. Chou (Osaka U.→Academia Sinica)
- ~~**Ding Key Exchange:** incl. T. Takagi, Y. Wang (UT, Kyushu U.)~~
- ~~**Giophantus:** K. Akiyama, H. Shimizu (Toshiba) , Y. Goto (HUE), S. Okumura (Osaka U.), T. Takagi, Y. Ikematsu (Kyushu U.), K. Nuida, G. Hanaoka (AIST)~~
- ~~**LOTUS:** L. T. Phong, T. Hayashi, Y. Aono, S. Moriai (NICT)~~
- ~~**RaCoSS:** incl. K. Fukushima, P.S. Roy, R. Xu, S. Kiyomoto (KDDI), T. Takagi (UT)~~

Other activities

- Cryptanalysis and Improvement of Algorithms
- Side-channel/Fault-Injection analysis
- Implementation
- More functional primitives/protocols

PQC in CRYPTREC

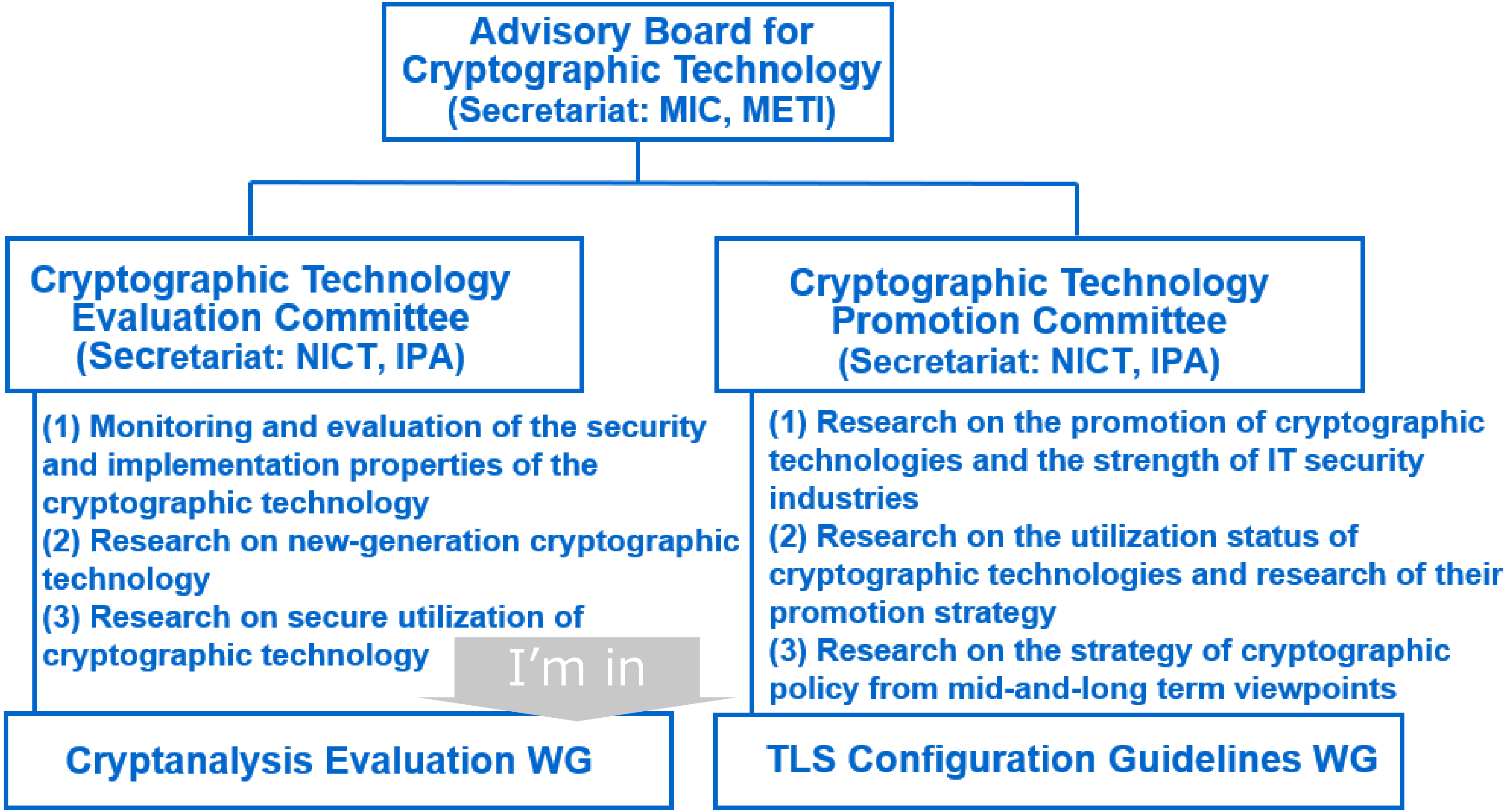
What's CRYPTREC?

CRYPTREC=Cryptography Research and Evaluation Committees

https://www.cryptrec.go.jp/en/index.html

- to evaluate and monitor the security of e-Government recommended ciphers
- to examine the establishment of evaluation criteria for cryptographic modules

Organization of CRYPTREC



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

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

Cryptographic Technology Promotion Committee (Secretariat: NICT, IPA)

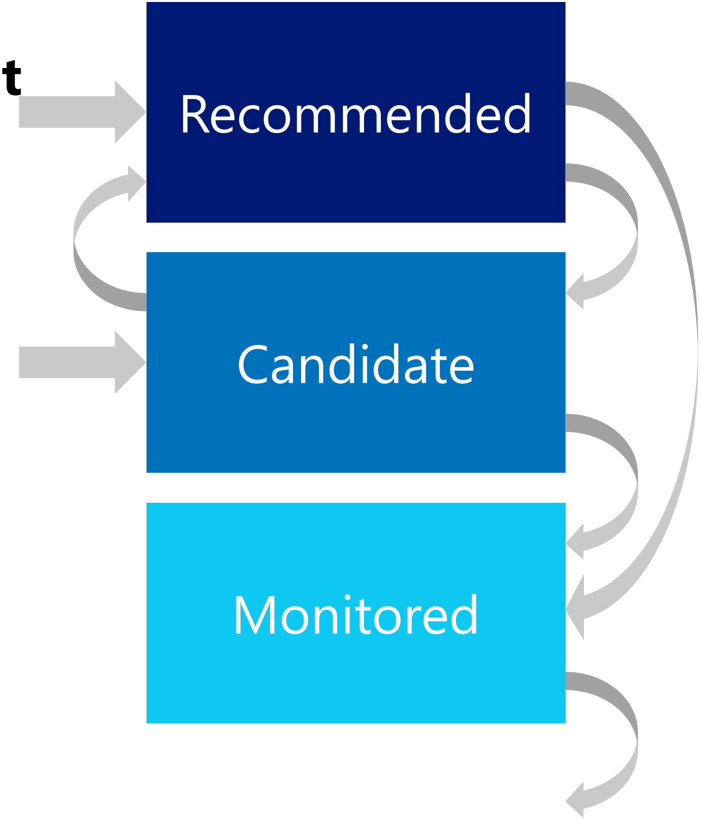
(1) Research on the promotion of cryptographic technologies and the strength of IT security industries
(2) Research on the utilization status of cryptographic technologies and research of their promotion strategy
(3) Research on the strategy of cryptographic policy from mid-and-long term viewpoints

Cryptanalysis Evaluation WG

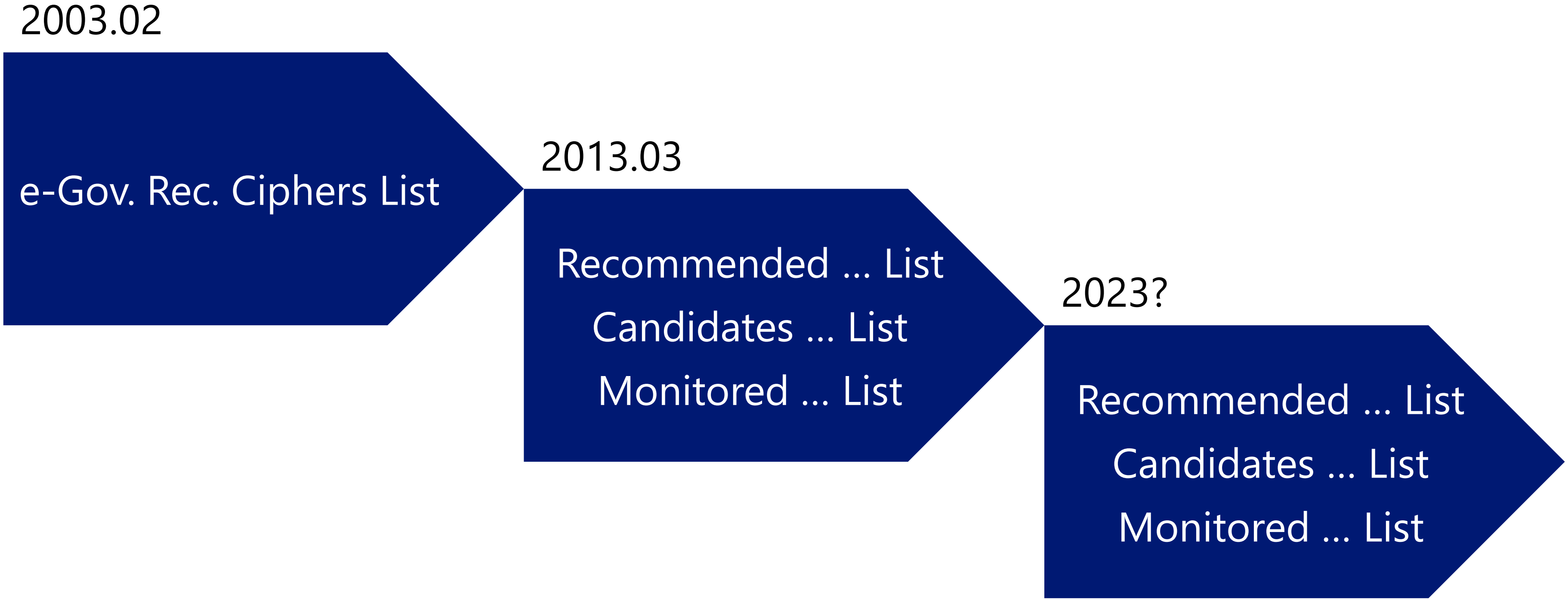
TLS Configuration Guidelines WG

Three Lists

- **e-Government Recommended Ciphers List**
  incl. (EC)DSA, (EC)DH, AES, SHA2, HMAC,…
- **Candidate Recommended Ciphers List**
  incl. MISTY1, SHA3, ChaCha20-Poly1305, …
- **Monitored Ciphers List**
  incl. 3-key TDES, SHA-1, CBC-MAC, …



(Big) Revision of Lists



2003.02

e-Gov. Rec. Ciphers List

2013.03

Recommended … List

Candidates … List

Monitored … List

2023?

Recommended … List

Candidates … List

Monitored … List

e-Gov. Recommended Ciphers List

Sig.	DSA, ECDSA, RSA-PSS, RSASSA-PKCS1-v1_5
Enc.	RSA-OAEP
KE	DH, ECDH
128 Block Cipher	AES, Camellia
Stream Cipher	KCipher-2
Hash	SHA-256/384/512
Mode	CBC, CFB, CTR, OFB
Auth.Mode	CCM, GCM
MAC	CMAC, HMAC
AEAD	N/A
Auth.	ISO/IEC 9788-2/3

None of them are PQC!

Reports on PQC

- Publish reports (in Japanese)
- 2015.03: WG ‘Report on LWE, LPN, ACD’
- 2019.03: WG ‘Report on PQC’
- 2020.02: WG ‘Effects of QC on Cryptography’
  https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html
- 2020.03: A. Hosoyamada ‘Report on PQ SKE’
- 2021.03: Lepidum ‘Report on Hybrid Modes’
- 2021.03: A. Takayasu ‘Report on Imple. of Shor’s Alg.’

Experimental Estimation!

NICT/Keio Univ./MUFJ/Mizuho – Dec. 2020

https://www.ieice.org/ken/paper/20201211zC19/eng/

First experiment on DL on IBM Q

OK: $2^z = 1 \bmod 3$

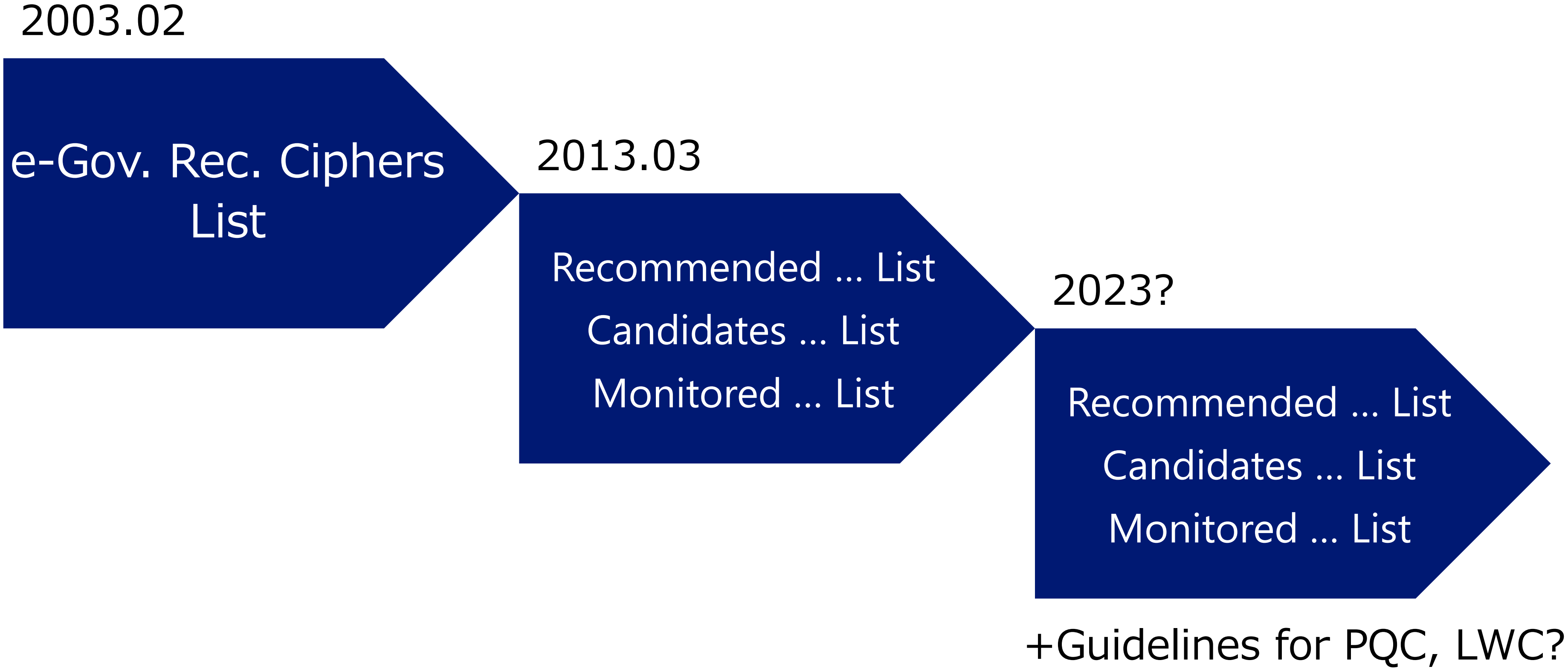
NG: $2^z = 2 \bmod 3$

NG: $4^z = 2 \bmod 7$

Task Force for PQC etc.

- Reports in Japanese are available
- #1 2019.06: QC, PQC
- #2 2019.09: PQC, LWC
- #3 2019.12: How to handle the lists
- #4 2021.03: QC, PQC, how to handle the lists
- They would start WG on a *guideline* for PQCs
- PQC may be not in the list but in a *guideline*

(Big) Revision of Lists



2003.02

e-Gov. Rec. Ciphers List

2013.03

Recommended … List

Candidates … List

Monitored … List

2023?

Recommended … List

Candidates … List

Monitored … List

+Guidelines for PQC, LWC?

Other PQC Activities in Japan

Other activities on transition

- **IMES BOJ (Institute for Monetary and Economic Studies, Bank of Japan)**
  - K. Kan, M. Une: Recent Trends on Research and Development of Quantum Computers and Standardization of Post-Quantum Cryptography
    - › https://www.imes.boj.or.jp/research/abstracts/english/21-E-05.html
  - T. Ito, M. Une, T. Seito: On mitigation to PQCs (in Japanese)
    - › https://www.imes.boj.or.jp/research/abstracts/japanese/19-J-15.html
  - J. Shikata: Recent Trends on Standardization of PQC: NIST (in Japanese)
    - › https://www.imes.boj.or.jp/research/abstracts/japanese/19-J-04.html
- **SECOM**
  - Performance Comparisons and Migration Analyses of Lattice-based Cryptosystems on Hardware Security Module
    - › https://ia.cr/2020/990

Wrap up

Wrap up

- Japanese activities on NIST PQC
- PQC Transition of CRYPTREC
  - They may write a guideline for PQC
- Other reports on PQC transition