

IBM

- (NIST),



2024 8 14, – IBM (NIST) (PQC, post-quantum cryptography)IBM 2 .

3 ML-KEM<sup>[1]</sup> ML-DSA<sup>[2]</sup> IBM , SLH-DSA<sup>[3]</sup> IBM IBM . , IBM FN-DSA<sup>[4]</sup>

‘ (cryptographic relevancy)’ . ‘ ’ .

(Jay Gambetta) IBM " IBM . , . " . NIST " .

IBM . , IBM 2029 .

. IBM 2033 10 . IBM , , , , . (Utility

Scale)<sup>[5]</sup> .

RSA . IBM

NIST .

2016 NIST . 2022 69 ‘ - ’, ‘ - ’, ‘ ’, ‘ +’ 4 .

NIST , IBM . IBM , N

IBM IBM z16 IBM . 2023 , , 3 IBM (IBM

Quantum Safe) . IBM IBM IBM (CBOM

Cryptography Bill of Materials) .

IBM <https://www.ibm.com/quantum/quantum-safe> .

###

---

[1] - (CRYSTALS-KYBER) .

[2] - (CRYSTALS-DILITHIUM) .

[3] (SPHINCS+) .

[4] (FALCON) .

[5] (Utility Scale, ) : , ,

---

<https://kr.newsroom.ibm.com/announcements?item=122786>