IBM Research

Quantum Safe Future

CIONET Oktober CyberFest

Zygmunt A. Łoziński, IBM Research 03 October 2024

IBM

Bring useful quantum computing to the world

Make the world quantum safe

Bring useful quantum computing to the world

Make the world quantum safe

IBM **Quantum** Safe Roadmap

● First generation available ◔ On target ○ Planned

	2022	2023	2024	2025	2026+
Regulatory milestones	NIST selects algorithms for standardization	Federal agencies plan for PQC adoption	NIST publishes PQC standards	CNSA 2.0: preference to PQC-compliant vendors	Vendors complete transition to PQC
Consortia	● Open Quantum Safe (OQS) ● Post-Quantum Telco Network	● NCCoE ● PQC Coalition (MITRE)	◔ Payments (EPAA, NACHA) ◔ PQC Alliance (Linux Foundation)	○ Critical Infrastructure Protection Coalition	
IBM services		● Quantum-safe preparation & advisory	◔ Application modernization ◔ Platform modernization	○ Security platform modernization	○ Quantum-safe talent transformation
IBM Quantum Safe technology			**IBM Quantum Safe Remediator** — *Transform* ◔ Adaptive proxy ◔ TLS, VPN, SSL ◔ Performance benchmarking	◔ Crypto-agility framework ◔ Encryption ◔ Key/certificate management	○ Automated remediation ○ LLM-based recommendation
			Quantum Safe Posture Management — *Observe* ◔ Dynamic scan ◔ Cryptographic inventory ◔ Cryptographic posture mgmt	◔ Risk-based prioritization ◔ Enriched metadata	○ AI-driven risk analysis
		IBM Quantum Safe Explorer — *Discover* ● Static scan ● CBOM generation ● CI/CD integration	◔ Custom library support ◔ Remediation recommendation	○ LLM-assisted scanning	
Algorithms, protocols, standards, libraries	● Key encryption: CRYSTALS - Kyber ● Digital signature: CRYSTALS - Dilithium, FALCON	● Cryptography Bill of Materials (CBOM)	◔ MAYO, UOV, SQISign ◔ OpenSSL		
IBM infrastructure		● IBM z16, IBM Hyper Protect Crypto Services, IBM Tape Storage, Hardware Security Modules (HSM)	◔ IBM Cloud, IBM Software, Red Hat, IBM Storage, IBM Power		

IBM **Quantum**