QUANTUM COMPUTING RISKS TO EMENSCR+

SANPAWAT KANTABUTRA, PhD
CENTER OF EXCELLENCE IN QUANTUM TECHNOLOGY, CMU

WHAT IS QUANTUM COMPUTING?

- Classical computing is based on classical physics.
- Quantum computing is based on quantum physics.
  - Superposition
  - Entanglement
  - Interference

SOME MEANINGFUL NUMBERS

- The number of known stars in the Universe is 2^{76}.
- To solve a hard problem of the input size 30, a most powerful classical supercomputer takes 2^{106} time steps = **10 million years** to compute.
- One of such hard problems is to crack an encrypted message using a 2048-bit RSA key.

RSA CRYPTOGRAPHY

- Encryption based on multiplying two 2048-bit primes $p \times q = n$.
- Decryption based on factoring n into p and q.
- Given n, the most powerful classical supercomputer cannot find p and q in a reasonable time.
- A quantum computer with a sufficient number of qubits (4000-6000 logical qubits) can do it very quickly.

SHOR'S FACTORING ALGORITHM

Turn the problem of factoring into a different problem:

➡️ **Finding the period (or repeating pattern) of a function.**

$3 \rightarrow 9 \rightarrow 7 \rightarrow 3 \rightarrow 9 \rightarrow 7 \rightarrow \ldots$

If you can figure out **how often the pattern repeats**, you can use that to **crack the code** and **find the hidden prime factors** of a giant number.

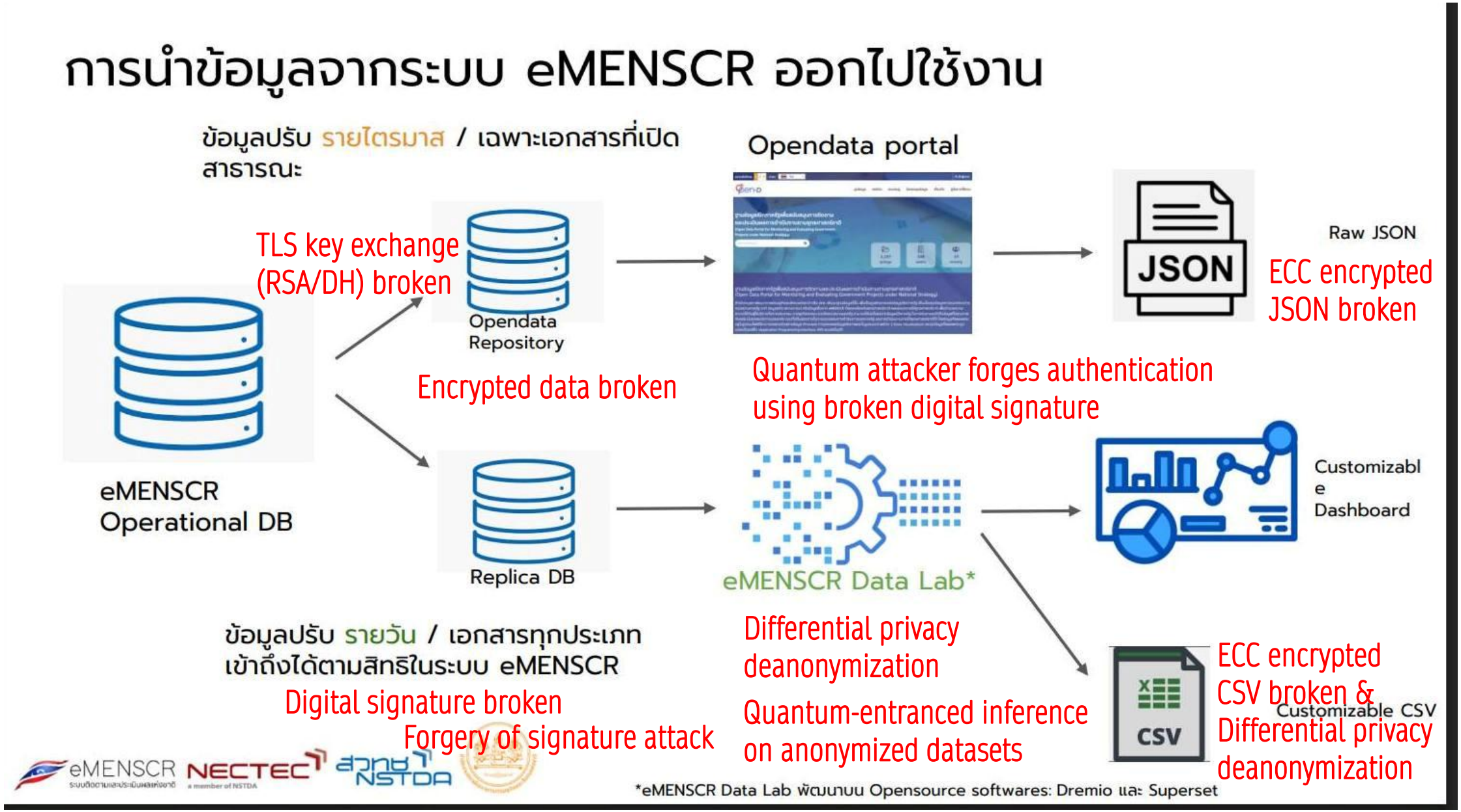
COMMON CRYPTOGRAPHIC SCHEMES

- **Symmetric-Key Cryptography** such as AES, ChaCha20, DES, 3DES.
  - Safe from quantum computer, given that you have a safe way to send a shared key.
- **Asymmetric-Key Cryptography** such as RSA, Diffie-Hellman, Elliptic Curve Crypto (ECC).
  - These schemes rely on **integer factorization** or **discrete logarithms** — both are efficiently solvable by **Shor's algorithm**.

HOW SOON WILL QUANTUM COMPUTER RENDER CURRENT CRYPTO USELESS?

Question	Answer
Can quantum computers break RSA/ECC today?	❌ No, not yet
When might they?	10–20 years
Can encrypted data now be vulnerable later?	✅ Yes (store-now-decrypt-later)
Should we migrate to post-quantum now?	✅ Yes — for long-term data
Is post-quantum crypto ready?	✅ Nearly — NIST standards in 2024–25

EXAMPLE OF POTENTIAL VULNERABILITIES



SYSTEM MIGRATION

Purpose	Classical	Post-Quantum Replacement
Key Exchange	RSA, DH	**Kyber** (ML-KEM)
Digital Signatures	RSA, ECC	**Dilithium**, **Falcon**, **SPHINCS+**

It requires **careful planning, compatibility testing, and staged rollout and could take 5 to 10 years to complete.**