Quantum-safe Postgres

How to achieve it

Tim Steward
Principal Data
Enterprise Architect

Quantum safe – why is it important?

FUJITSU

Normal encryption

Attacks may take **weeks/months**

Quantum computing

Attacks may take **hours/days**

Encryption from Press to Rest

3 stages of data

Data in use

From Press of a key until it reaches the destination

Data in transit

Between two nodes (traffic)

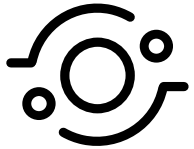
Data at rest

Where the data is generated and stored

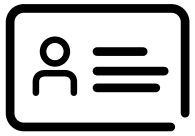
Cyber security and Postgres

FUJITSU

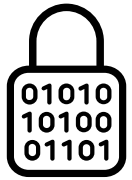
Postgres, as the leading open source database, provides a variety of tools and ways to ensure security compliant with industry best practices



Access control



Authentication



Encryption
in transit and at rest

Audit logs

Best practices need to go beyond just the database

OS

Key management

Backups

Encryption at rest

FUJITSU

Practice of protecting data stored in a device, usually a hard drive, using **encryption algorithms**

Symmetric

- AES
- DES
- 3DES

Asymmetric

- RSA
- ECC

In Postgres, the most common **types of encryption** are:

Column-level encryption

using pgcrypto

Data partition encryption

using OS filesystem encryption options – *i.e.*, dm-crypt + LUKS

Very good options, but...

It was all good... until it wasn't

FUJITSU

It's a weird, weird quantum world

In MIT's 2023 Killian Lecture, Peter Shor shares a brief history of quantum computing from a personal viewpoint.

Jennifer Chu | MIT News Office
March 10, 2023

Chinese scientists claim they broke RSA encryption with a quantum computer — but there's a catch

News By Peter Ray Allison published October 22, 2024

Researchers claim to have broken RSA encryption using a quantum computer, but what really happened?

Debunking Hype: China Hasn't Broken Military Encryption With Quantum

Craig S. Smith Contributor ©
Craig S. Smith, Eye on AI host and former NYT writer, covers AI.

Recent headlines have proclaimed that Chinese scientists have hacked "military-grade encryption" using quantum computers, sparking concern and speculation about the future of cybersecurity. The claims, largely stemming from a recent South China Morning Post article about a Chinese academic paper published in May, was picked up by many more serious publications.

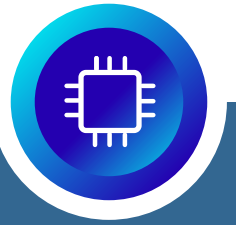
However, a closer examination reveals that while Chinese researchers have made incremental advances in quantum computing, the news

Quantum compute

FUJITSU

Quantum computing is a type of nonclassical computing that operates on the quantum state of subatomic particles.

Gartner



Quantum computing is an emergent field of cutting-edge computer science harnessing the unique qualities of quantum mechanics to solve problems beyond the ability of even the most powerful classical computers.

IBM

Quantum computers harness some of the almost-mystical phenomena of quantum mechanics to deliver huge leaps forward in processing power. Quantum machines promise to outstrip even the most capable of today's—and tomorrow's—supercomputers.

MIT Technology Review

Quantum compute

FUJITSU

Quantum bit or qubit

The unit of information that can be stored

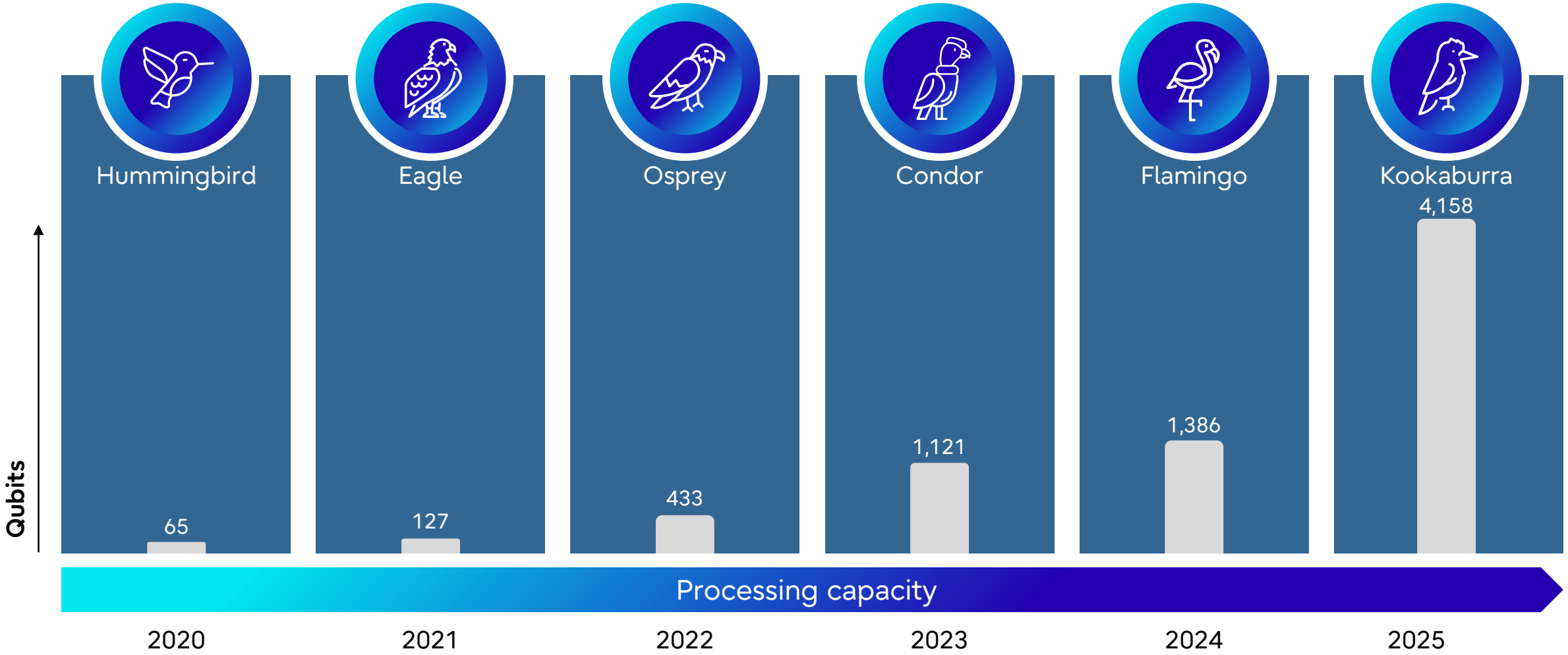
10 qubits

1024 combinations of numbers it can encode simultaneously

IBM Quantum Roadmap

FUJITSU

Technology for the quantum future | Development roadmap



Source: https://www.ibm.com/quantum/assets/IBM_Quantum_Developmen_&_Innovation_Roadmap_Explainer_2024-Update.pdf

Quantum compute applications

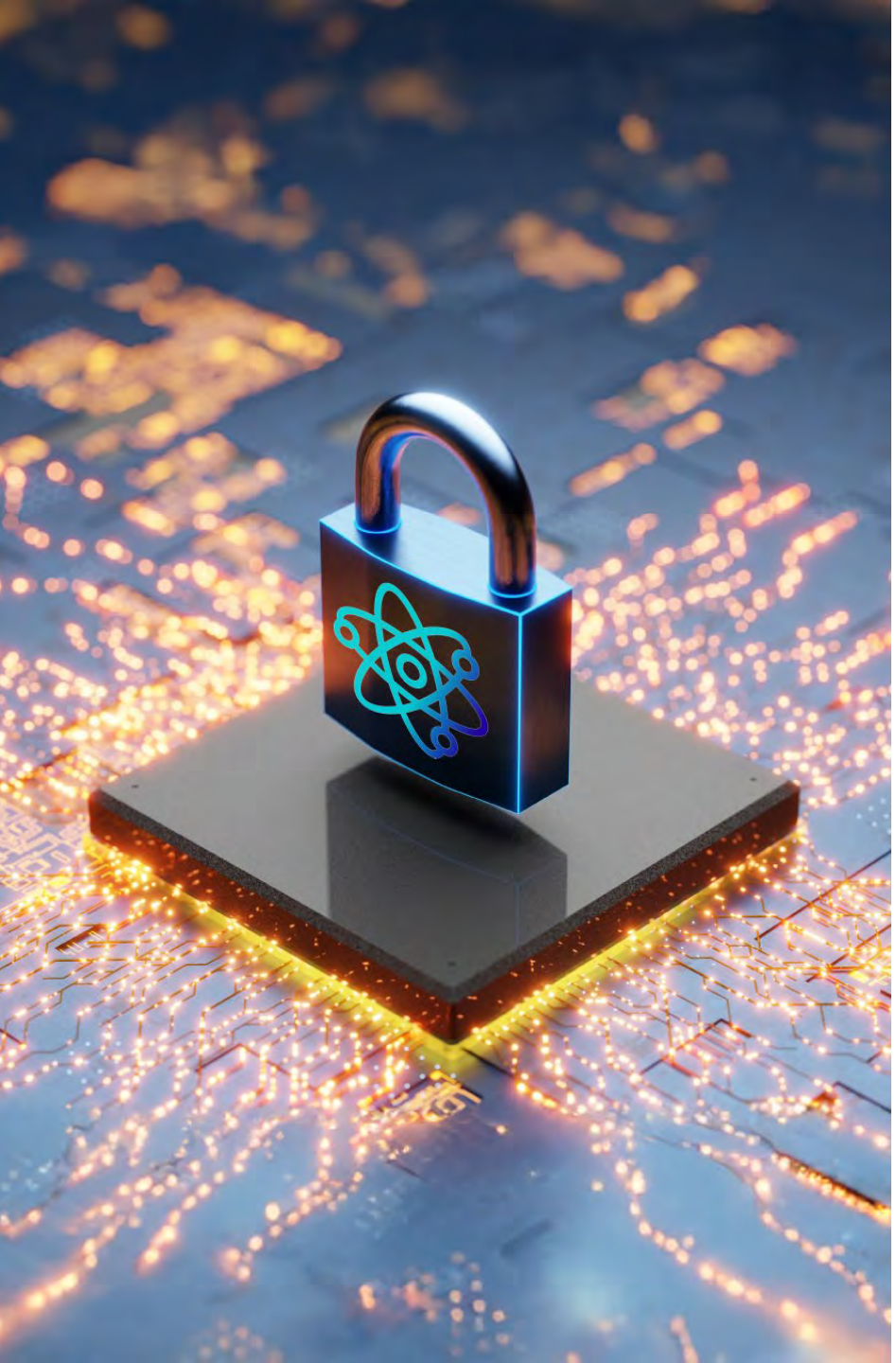
FUJITSU

- Cyber security
  - Quantum random number generation, quantum key distribution, post-quantum cryptography
- Drug development and materials science
  - More efficient simulation of molecular interactions accelerates discovery/development of new drugs
  - Logistics and supply chain optimization
  - Optimization of complex logistics networks leads to more efficient transportation, warehousing, and delivery systems
- Financial modelling
  - Optimization of complex financial models leads to better investment strategies
- Artificial intelligence
  - Enhanced machine learning algorithms and data pattern recognition
- Weather forecasting
  - Improved accuracy of weather forecasts and climate model

Encryption in a quantum world

FUJITSU

- Vulnerability of existing algorithms
  - AES256 safe until 2050; vulnerable with quantum computing
- Quantum-safe algorithms
  - Algorithms like SIKE (Supersingular Isogeny Key Encapsulation) and others being standardized by NIST for post-quantum cryptography
- Quantum-resistant encryption
  - Techniques designed to withstand quantum attacks, ensuring long-term data security
- Quantum cryptography
  - Tasks such as quantum key distribution offers an information-theoretically secure solution to the key exchange problem



Encryption in a quantum world

FUJITSU

Take action now

Size of key	Hack crack attack time
56-bit	399 seconds
128-bit	1.02 x 10^{18} years
192-bit	1.872 x 10^{37} years
256-bit	3.31 x 10^{56} years

Postgres security

FUJITSU

Transitioning to Post-Quantum Cryptography (PQC)

PQC algorithms resist attacks from quantum computers.
Current cryptographic primitives (like RSA and ECC) will need to be replaced with quantum-resistant alternatives

Algorithm selection and standardization

NIST post-quantum cryptography standardization process provides guidance on suitable algorithms for different cryptographic tasks

Hybrid cryptographic approaches

Combining current and post-quantum algorithms might be necessary during transition to ensure smooth migration without compromising security

Database schema and application changes

Integrating PQC might require changes to DB schema and application code to accommodate new cryptographic primitives and key management processes

Quantum cryptography – Risks and opportunities

FUJITSU

In 1994, Peter Shor proved quantum computers could theoretically break our current public key encryption algorithms. For that, massive-scale quantum computers would be necessary.

Neven's Law says that quantum computing power is experiencing doubly exponential growth (i.e., growth by powers of powers of two) relative to conventional computing (i.e., doubling processing power every two years per Moore's Law.) Thus, it's only a matter of time until we see quantum computers with sufficient power to break public key encryption

Grover's algorithm is a quantum algorithm for unstructured data that provides a quadratic speedup in the computation over classical computing. This can result in AES-128 being feasible to crack, but AES-256 is still considered quantum-resistant—at least until 2050, (as referenced throughout ETSI GR QSC 006 V1.1.1)

Disk vs File System vs Database Encryption

FUJITSU

Disk encryption	File system encryption	Database encryption
Strongest protection against physical theft or unauthorized access; Simple to implement	Granular control over encrypted file scope; Less overhead than full-disk encryption	Granular control over encrypted data scope; Can be transparent; Safe even if file system or disk is compromised
Performance overhead; Does not protect data in transit; Requires full disk decryption before access	Vulnerable if OS or file system is compromised; Does not protect data in transit; Moderate complexity to manage	Performance overhead depending on encryption method and data volume; Does not protect data in transit; Requires careful planning to avoid performance impact
Can use quantum-resistant algorithms for encryption key	**Can use quantum-resistant algorithms for file encryption keys**	**Can use quantum-resistant algorithms with pgcrypto**

Database encryption - not all the same

FUJITSU

- Open source advantage
  - PostgreSQL's open-source nature allows for greater transparency and community scrutiny of its encryption mechanisms, leading to more secure solution and also allows for independent verification of security claims
- Compliance-ready
  - PostgreSQL's robust encryption features help organizations meet stringent security compliance standards like PCI DSS, ensuring data protection and reducing the risk of non-compliance penalties
- Extensibility and flexibility
  - PostgreSQL can integrate with various encryption tools and libraries so you can choose the best encryption methods, allowing for easier adoption of future quantum-safe algorithms
  - Performance optimization
  - PostgreSQL offers various performance optimization techniques for database encryption, minimizing the impact on application performance
- Integration with existing tools
  - PostgreSQL integrates seamlessly with existing security tools and infrastructure

Database encryption management

FUJITSU

Best practices for key management

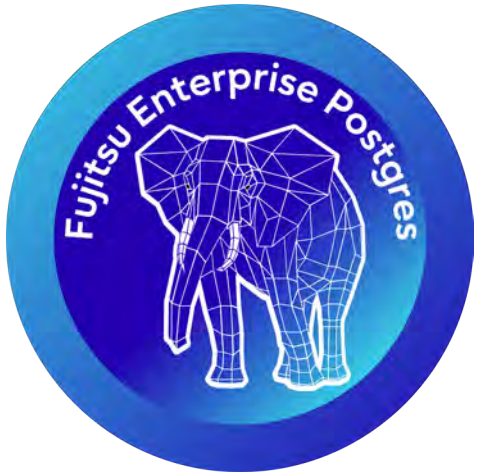
- Type of key – e.g., private signature key, symmetric data encryption key
- Key format – e.g., TLS/SSL server certificate, TLS/SSL client certificate, code signing certificate, email certificate, ASN.1, and Tag-Length-Value (TLV) encoding for symmetric keys
- Key length – e.g., 2048 bits, 256 bits
- Algorithm with which the key is used – e.g., AES, ECDSA, RSA

NIST SP 800-57 PT. 2 REV. 1

https://doi.org/10.6028/NIST.SP.800-57pt2r1

Quantum-safe Postgres - Fujitsu Enterprise Postgres

FUJITSU



- Support for Post-Quantum Cryptography (PQC) algorithms
  - Fujitsu's future-proofing of Fujitsu Enterprise Postgres means support of post-quantum cryptographic algorithms as they become available
- Enhanced key management
  - Fujitsu Enterprise Postgres enhances key management to better support longer and more complex keys, required for PQC algorithms
- Proactive security updates
  - Fujitsu provides security updates and patches to address vulnerabilities, and will continue doing so when threats to quantum computing emerge
- Consulting services and database expertise
  - Fujitsu's proven expertise in database security and ability to provide consulting services positions Fujitsu as a partner in the transition to quantum-safe systems
- Platform optimization
  - Fujitsu Enterprise Postgres is optimized for performance and scalability, two crucial factors for mitigating the potential performance impact of implementing PQC algorithms.

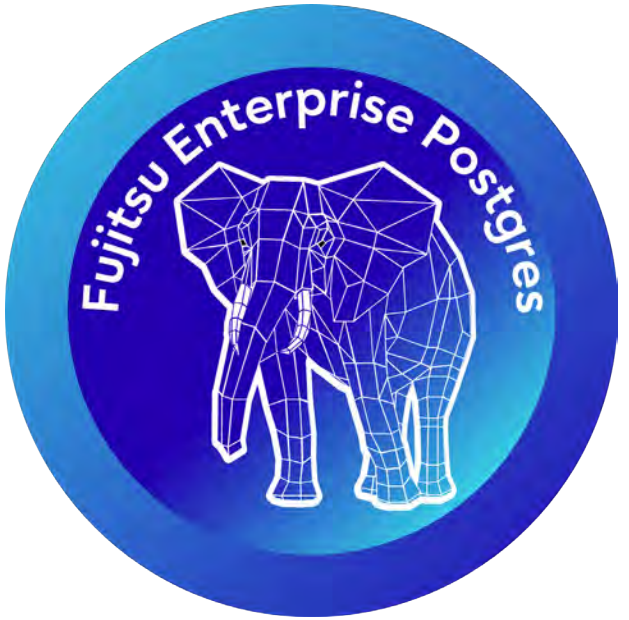
Interesting Fact

- Mathematician: Alan Turing
- Movie: The imitation game - 2014
- Fact: Breaking of Germany’s Enigma machine

Quantum-safe Postgres - Fujitsu Enterprise Postgres

FUJITSU

"You don't just need encryption, you need the right encryption"



Tim Steward

Principal Data Enterprise Architect

If you would like to continue this conversation, feel free to reach out

fast.fujitsu.com/tim-steward

linkedin.com/in/tsteward1