Beneficial Applications of Quantum Computing for International Security

BENJAMIN ANG
HEAD, CYBER HOMELAND DEFENCE,
CENTRE OF EXCELLENCE FOR NATIONAL SECURITY
S RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
NANYANG TECHNOLOGICAL UNIVERSITY, SINGAPORE

Key Concepts of Quantum Computing

CLASSICAL DIGITAL COMPUTERS

Use bits (1 or 0)

Work step by step

Need lots of them to model complex questions (chem, bio)

8 bit computer can store 2^8 (i.e. 256) states of data

QUANTUM COMPUTERS

Use qubits (anything between)

Work in parallel (faster!)

Naturally suited to model complex questions

8 qubit computer can store 10^{77} states of data

Key Concepts

QUANTUM SUPREMACY

- When quantum computers can surpass classical digital computers
- Estimated 5 years time

QUANTUM COMPETITION

- USA vs China
- Google, IBM
- Singapore?

Some projects from Singapore – AI algorithms

Quantum algorithm to crunch numbers on commodities pricing, social networks and chemical structures, and find correlations.

Saving memory from simulations

Using quantum to store computer models of a city's traffic flow or neural firing in the brain, (continuous-time stochastic processes)

Problem: Encryption and Cybersecurity Apple vs FBI

SUPPORTING UNBREAKABLE ENCRYPTION

It protects transactions from criminals

It protects privacy of citizens (human right)

If there are back doors for law enforcement / government, then criminals can find them too

AGAINST UNBREAKABLE ENCRYPTION

It protects criminals from investigation

It prevents citizens from accessing information

There must be another way – Ray Ozzie's highly criticized proposal

The power of quantum computing?

Case Western Reserve University and Microsoft's Quantum will use *quantum-inspired* algorithms to enhance detection of cancerous tumors.

Almost all current classical encryption (RSA, etc) could be broken by quantum computing by 2025

ENCRYPTED DATA CAN BE STOLEN NOW, DECRYPTED LATER

Use Case 1: Bank needs to protect customer banking data

Bank Servers

- Banking data

Data Recovery Centre

- Backup of banking data

Use Case 2: Government needs to protect counted votes data

Central ballot counting station

- Counted votes data

Government data centre

- Counted votes data

Use Case 3: Smart Factory needs to protect intellectual property

Automobile manufacturer

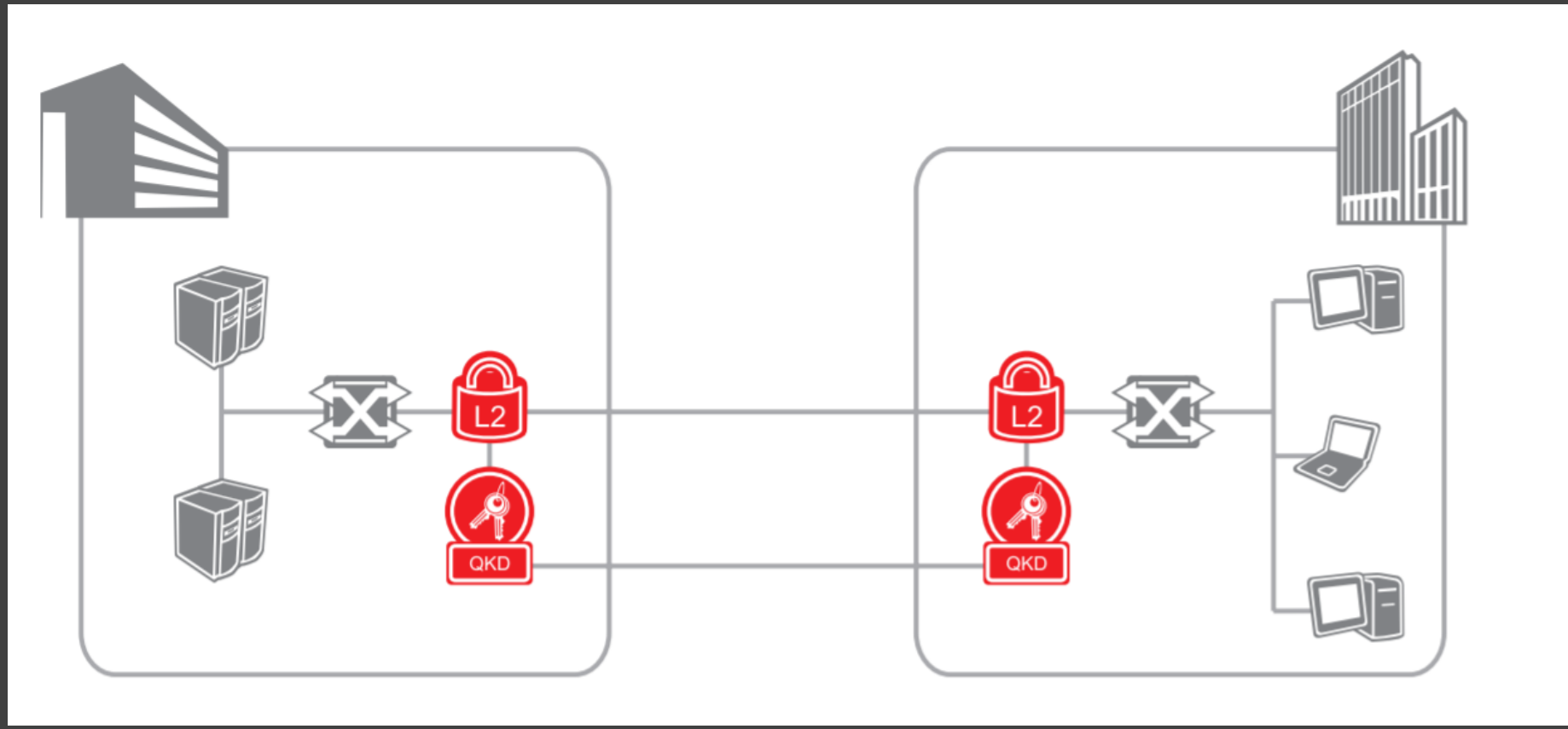
- Design documents

Smart Factory

- Robots and IOT devices

Solution (?): Quantum Key Distribution will not be compromised by increase in computing power

Quantum Key Distribution at work



Why Quantum Key Distribution works

Quantum Random Number Generation is truly random

Keys can be changed constantly

Eavesdropping is not possible without perturbation

Is there a way to protect data until it needs to be accessed for national security reasons?

Challenges

* Scale & distance

* Cost