

Cryptography Engineering



Jerry J. R. Shieh, PhD

CSIC 30040 Spring 2024

Cryptography engineering has a significant impact on the world!

1. The Last Line of Defense for Cyber Security.

- PRC's government hackers carry out cyber espionage as unconstrained warfare (超限战)
- Free World governmental institutions, critical facilities and military corporations have sustained such attacks.



Humvee (U.S. Army)



The U.S. Navy F-35 Joint Strike Fighter.



U.S. MQ-1 Predator



东风汽车公司 EQ2050



沈阳飞机工业集团公司 鹞鹰 歼31



彩虹4号CH4察打一体无人机



- PRC set **nuclear weapons, aerospace science and information security** as its **three primary national strategies goals**



http://www.project2049.net/documents/Stokes_PLA_General_Staff_Department_Unit_61398.pdf



SECRET//REL TO USA, JPN

U.S. Victims of Chinese Cyber Espionage over the past five years



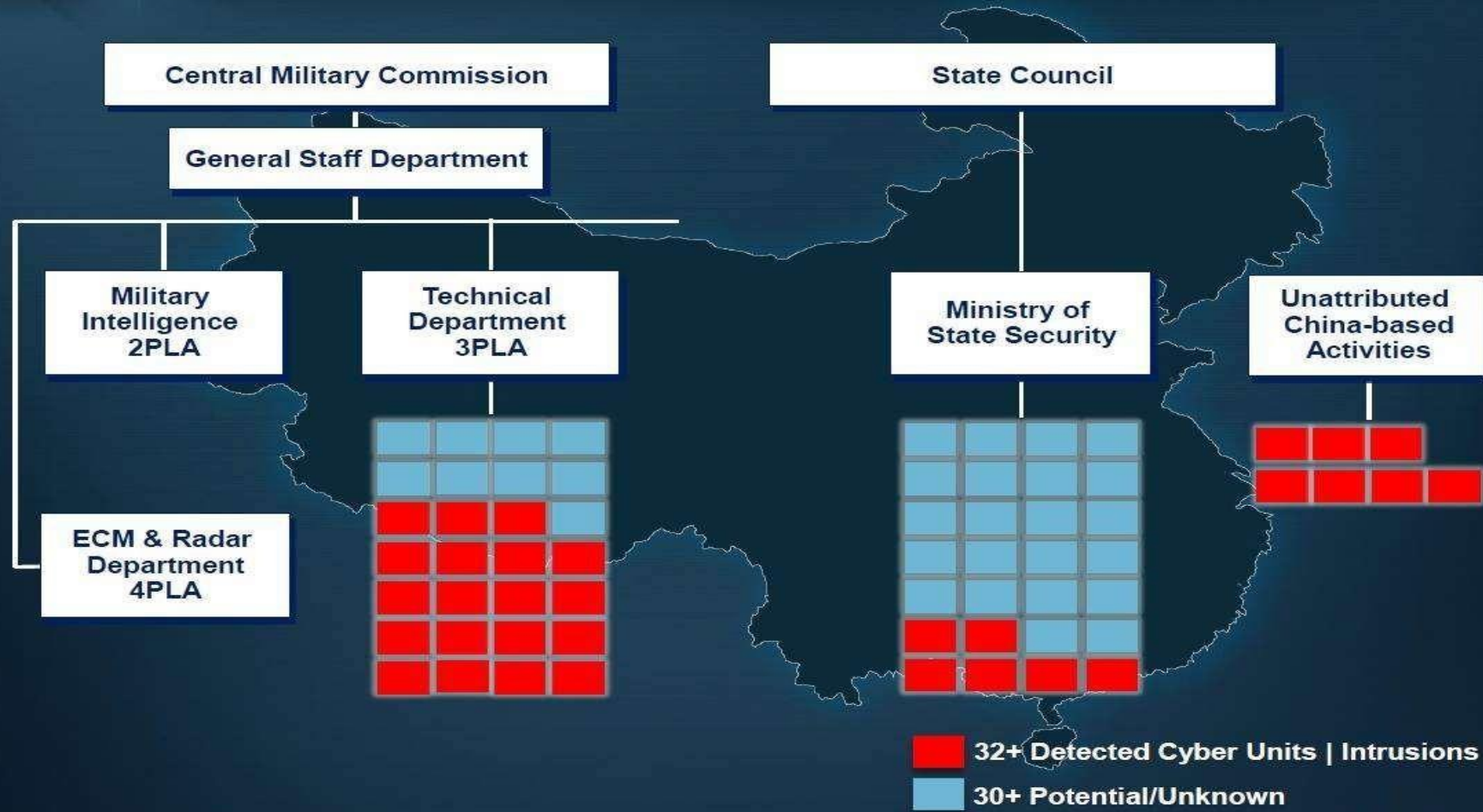
Each red dot is a unique corporate, private, or U.S. government victim.

SECRET//REL TO USA, JPN



SECRET//REL TO USA, JPN

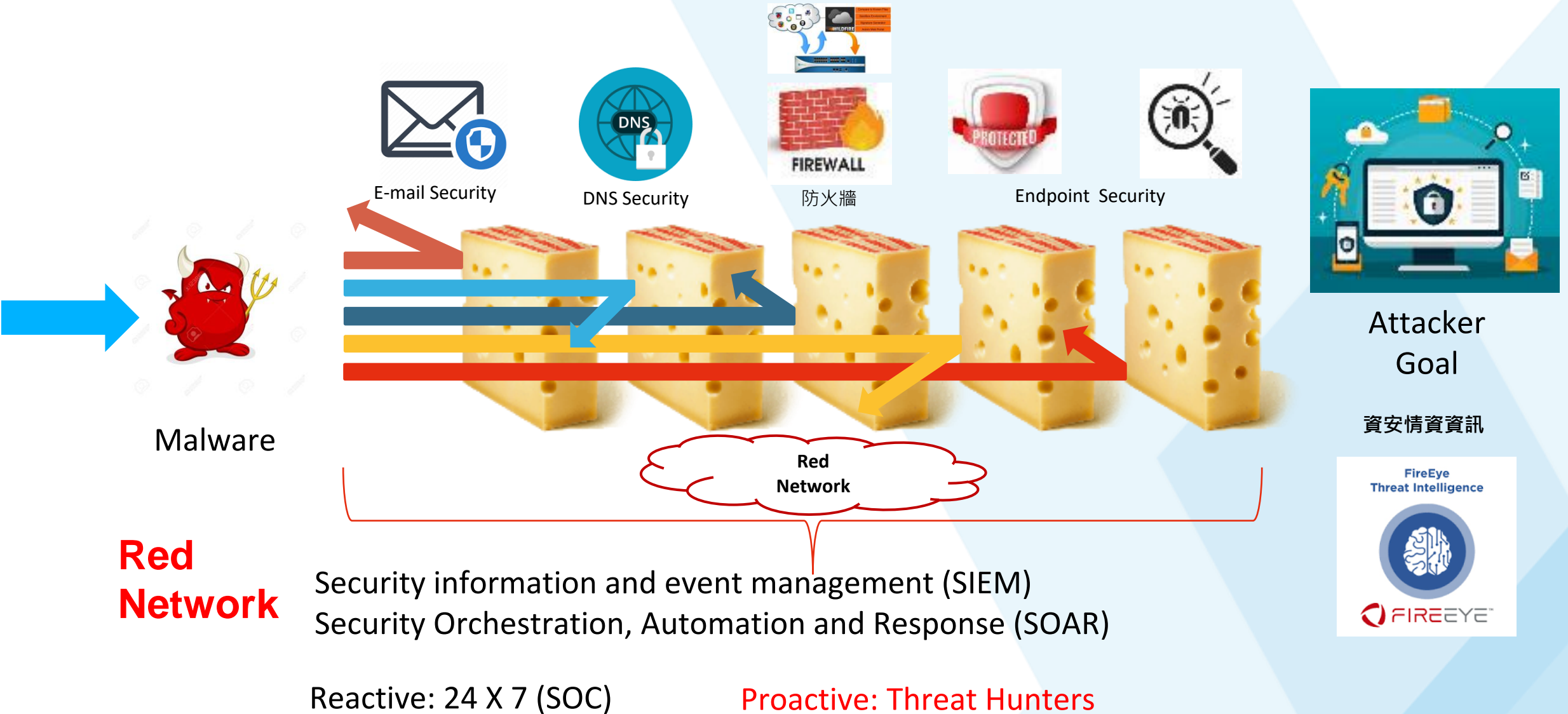
China: Cyber Exploitation *and* Attack Units



SECRET//REL TO USA, JPN

網路區隔 Red Data Network

Multi-Layered Defense Using Different Independent Solutions



zero trust = identity authentication + encryption

Encryption is the last line of defense for security.

Security experts agree that the biggest problem with the breach was not the failure to prevent remote break-ins, but the **absence of mechanisms to detect outside intrusion** and **the lack of proper encryption of sensitive data.**

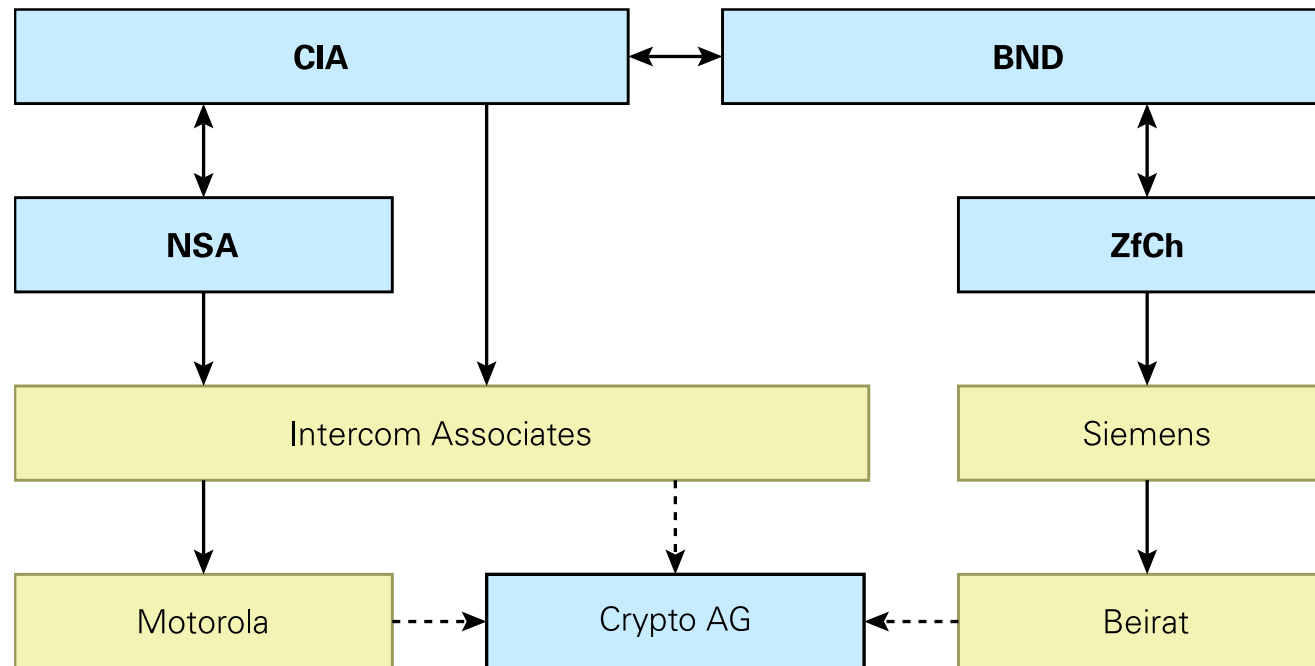
https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach

2. Using Encryption Backdoors and Vulnerabilities for International Espionage



<https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/>





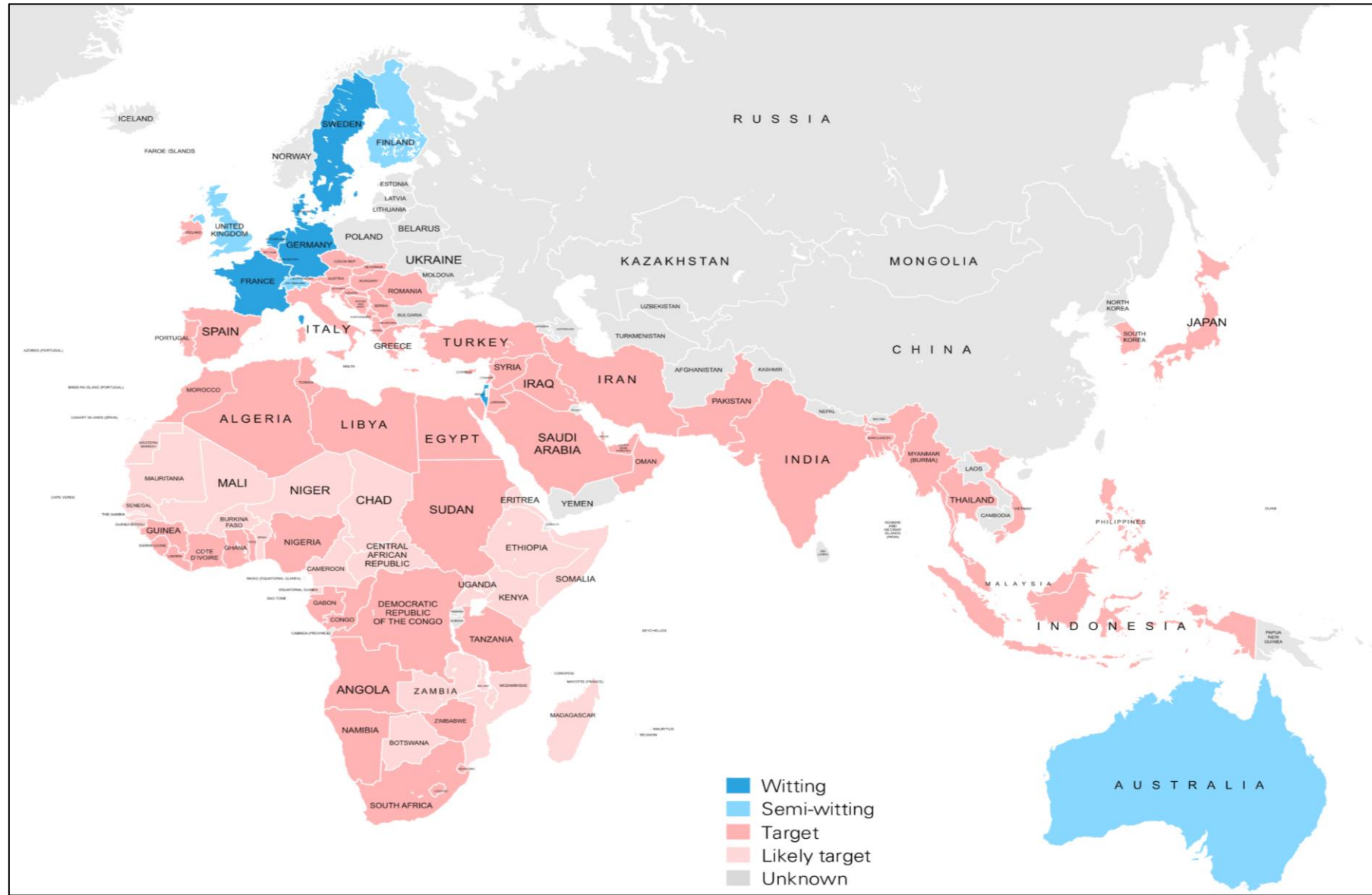
Influencing of the cryptographic algorithms

<https://www.cryptomuseum.com/intel/cia/rubicon.htm>

<https://www.cryptomuseum.com/intel/zfch/>

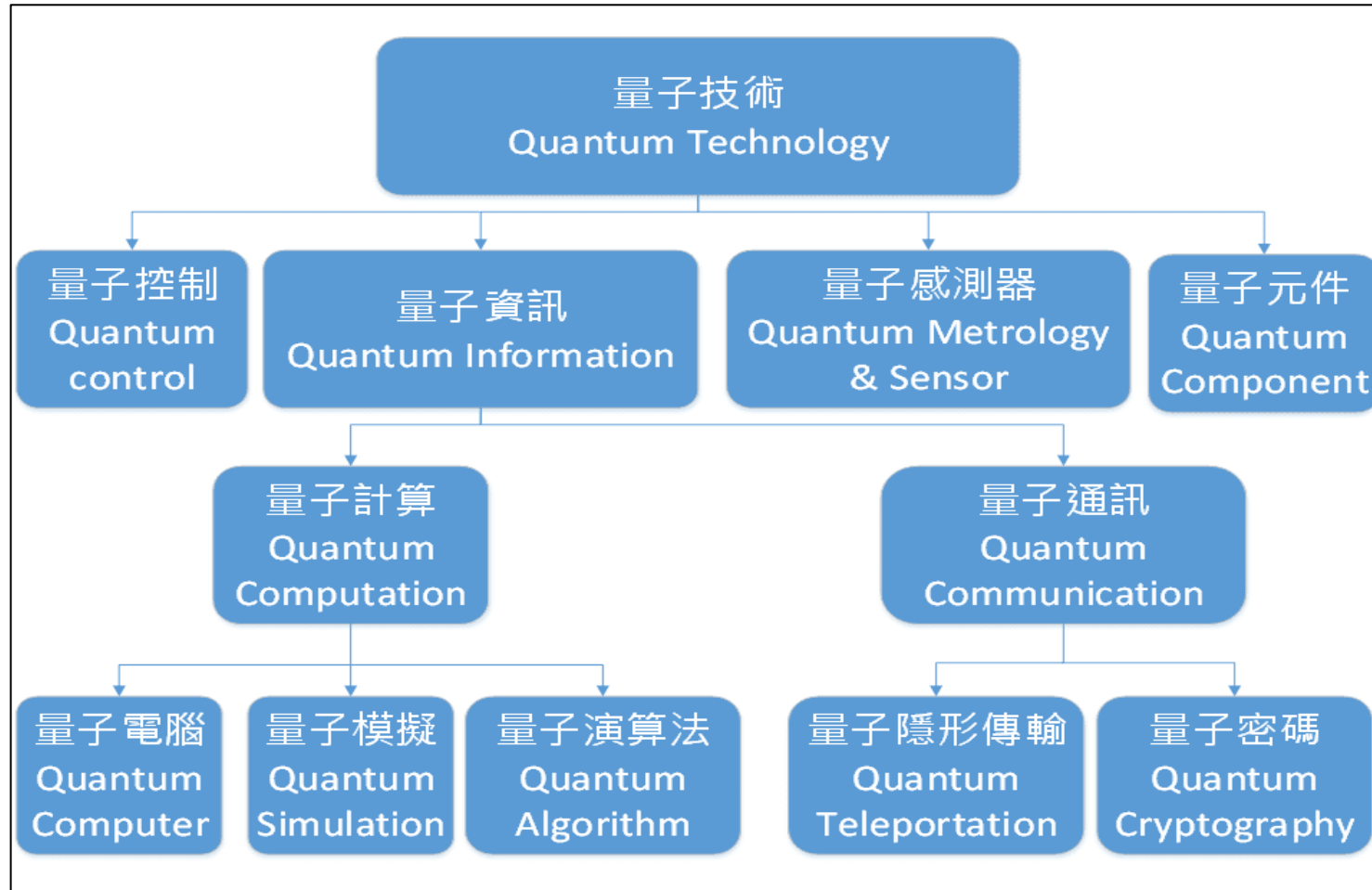
Swiss Crypto AG spying scandal shakes reputation for neutrality

- The Swiss government has ordered an inquiry into a global encryption company based in Zug following revelations it was owned and controlled for decades by US and German intelligence.
- **Encryption weaknesses added to products** sold by Crypto AG allowed the CIA and its German counterpart, the BND, to eavesdrop on adversaries and allies alike while earning million of dollars from the sales, according the Washington Post and the German public broadcaster ZDF, based on the agencies' internal histories of the intelligence operation



<https://www.cryptomuseum.com/intel/cia/rubicon.htm>

3. Facing the Emerge of Quantum Computing



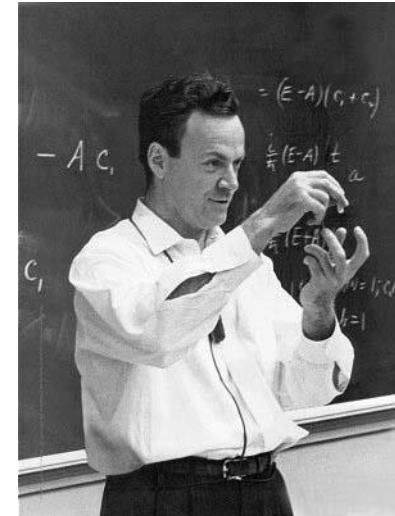


What is a quantum computer?

- A quantum computer is a machine that performs calculations based on the laws of quantum mechanics, which is the behavior of particles at the sub-atomic level.

Introduction

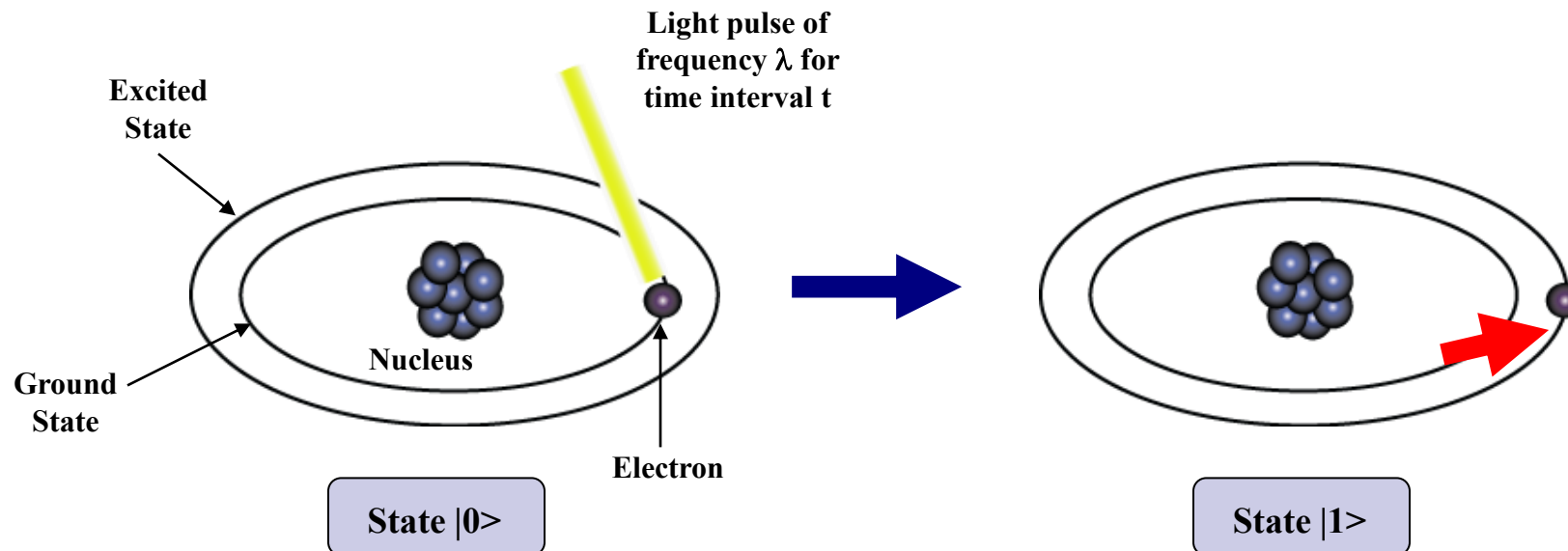
- “I think I can safely say that nobody understands quantum mechanics” - Feynman
- **1982 - Feynman proposed the idea of creating machines based on the laws of quantum mechanics instead of the laws of classical physics.**
- 1985 - David Deutsch developed the quantum turing machine, showing that quantum circuits are universal.
- **1994 - Peter Shor came up with a quantum algorithm to factor very large numbers in polynomial time.**
- **1997 - Lov Grover develops a quantum search algorithm with $O(\sqrt{N})$ complexity**



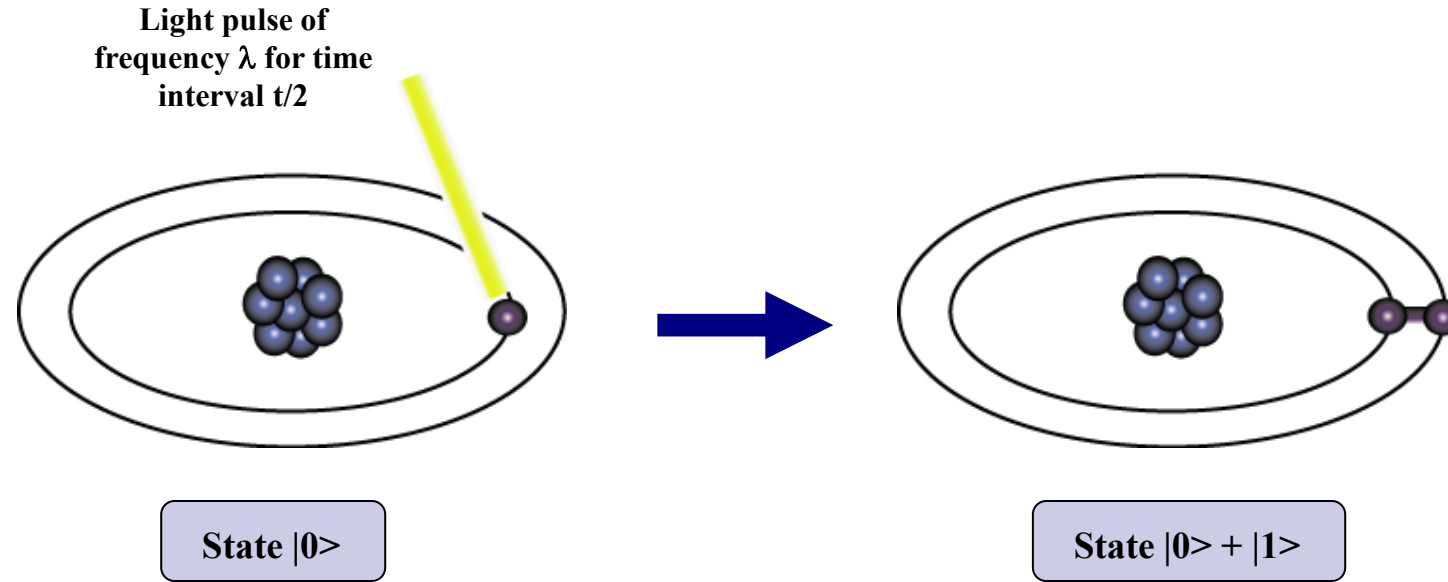
Representation of Data - Qubits

A bit of data is represented by a single atom that is in one of two states denoted by $|0\rangle$ and $|1\rangle$. A single bit of this form is known as a ***qubit***

A physical implementation of a qubit could use the two energy levels of an atom. An excited state representing $|1\rangle$ and a ground state representing $|0\rangle$.



Representation of Data - Superposition



- Consider a 3 bit qubit register. An equally weighted superposition of all possible states would be denoted by:

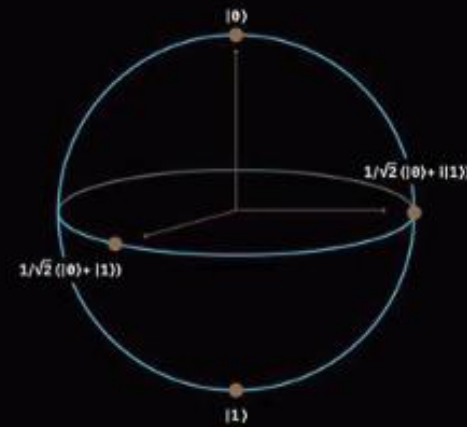
$$|\psi\rangle = \frac{1}{\sqrt{8}} |000\rangle + \frac{1}{\sqrt{8}} |001\rangle + \dots + \frac{1}{\sqrt{8}} |111\rangle$$

Why is quantum different?

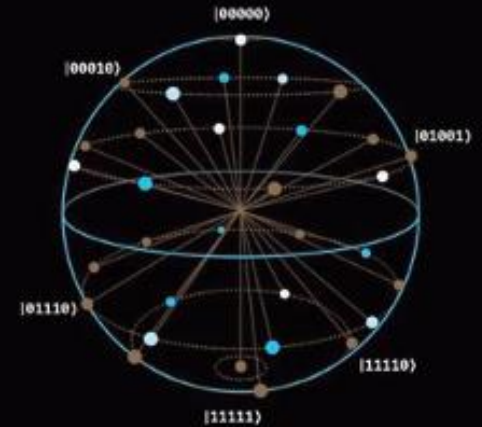
1. Superposition



Classical states



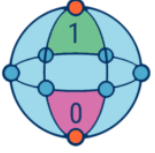



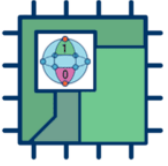



BLOCH SPHERE (1 QUBIT)



QSPHERE (5 QUBITS)

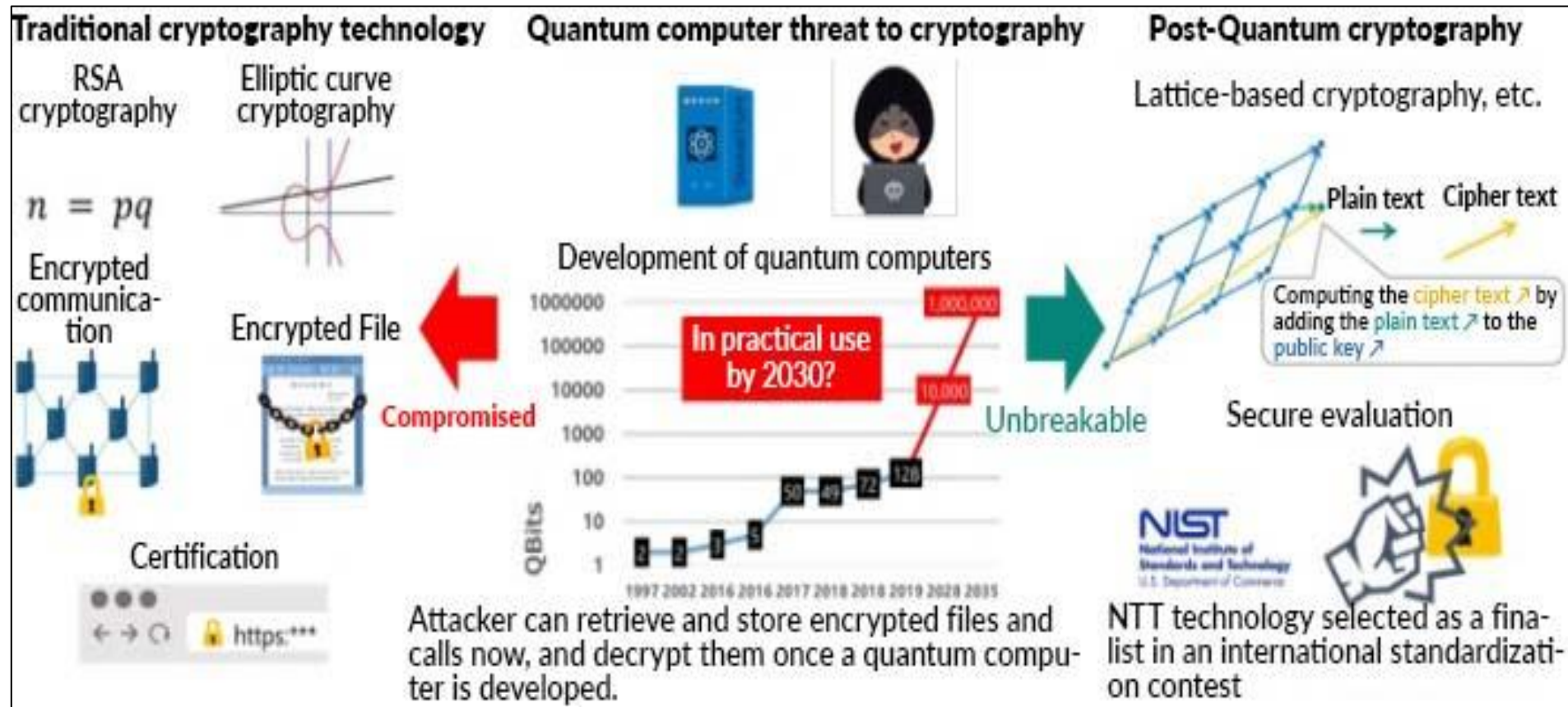
N qubits
 2^N paths

Quantum states

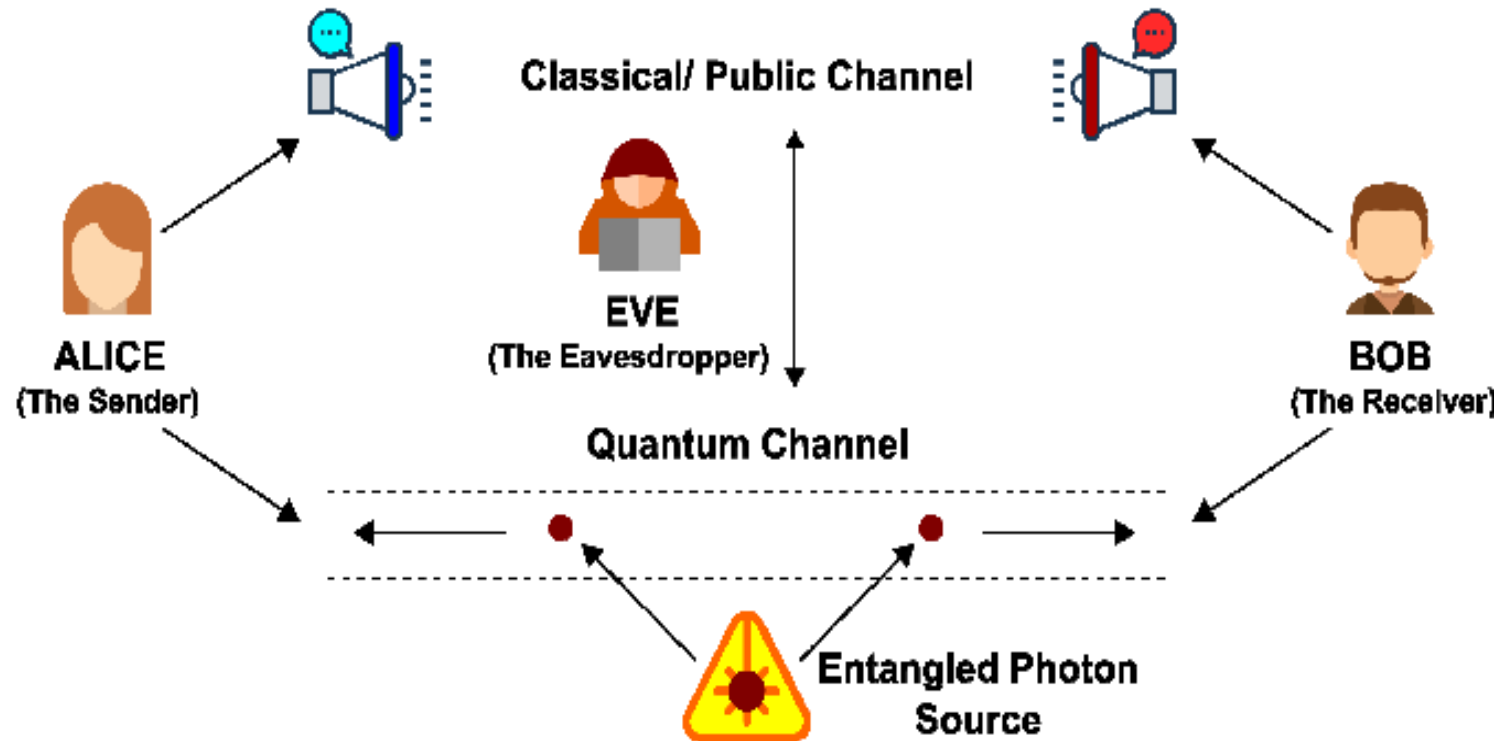
Quantum Computing	Vs. Classical Computing
 <p>Calculates with qubits, which can represent 0 and 1 at the same time</p>	<p>Calculates with transistors, which can represent either 0 or 1</p> 
 <p>Power increases exponentially in proportion to the number of qubits</p>	<p>Power increases in a 1:1 relationship with the number of transistors</p> 
 <p>Quantum computers have high error rates and need to be kept ultracold</p>	<p>Classical computers have low error rates and can operate at room temp</p> 
 <p>Well suited for tasks like optimization problems, data analysis, and simulations</p>	<p>Most everyday processing is best handled by classical computers</p> 

Classical Computing		Quantum Computing	
Subroutine	Complexity	Subroutine	Complexity
Matrix inversion: $Ax = b \rightarrow x = A^{-1}b$	$O(N \times \log(N)) \rightarrow O(N^2)^*$	Matrix inversion: $A x\rangle = b\rangle \rightarrow x\rangle = A^{-1} b\rangle$	$O((\log(N))^2)$
Eigenvectors and eigenvalues of sparse/low-rank matrices	$O(N^2)$	Q Phase	$O((\log(N))^2)$
FFT: Fast Fourier Transform	$O(N \times \log(N))$	QFT: Quantum Fourier Transform	$O((\log(N))^2)$

後量子密碼學 (Post-Quantum Cryptography, PQC)

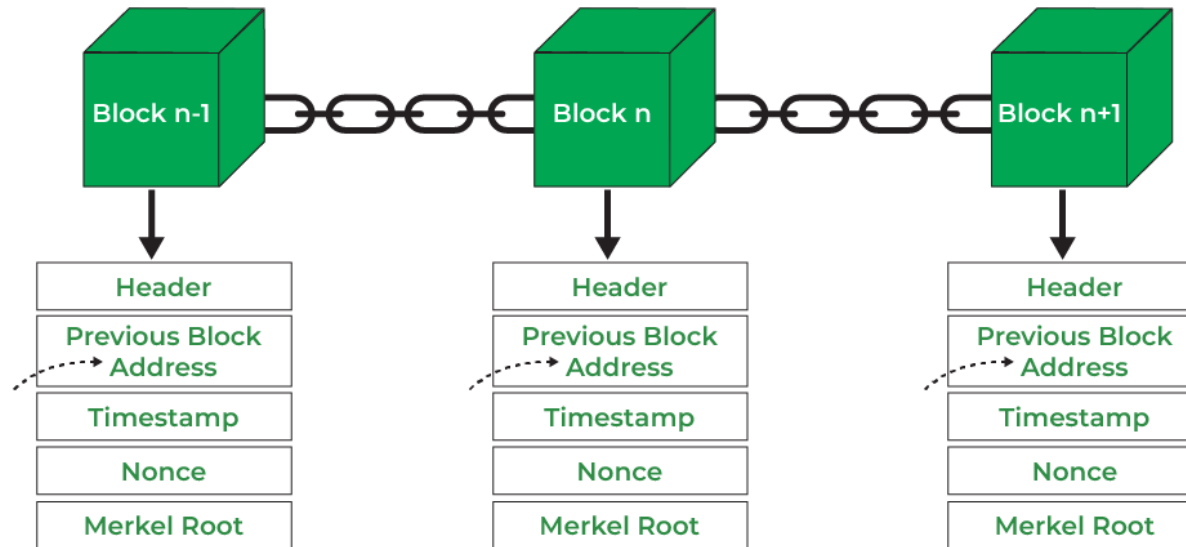


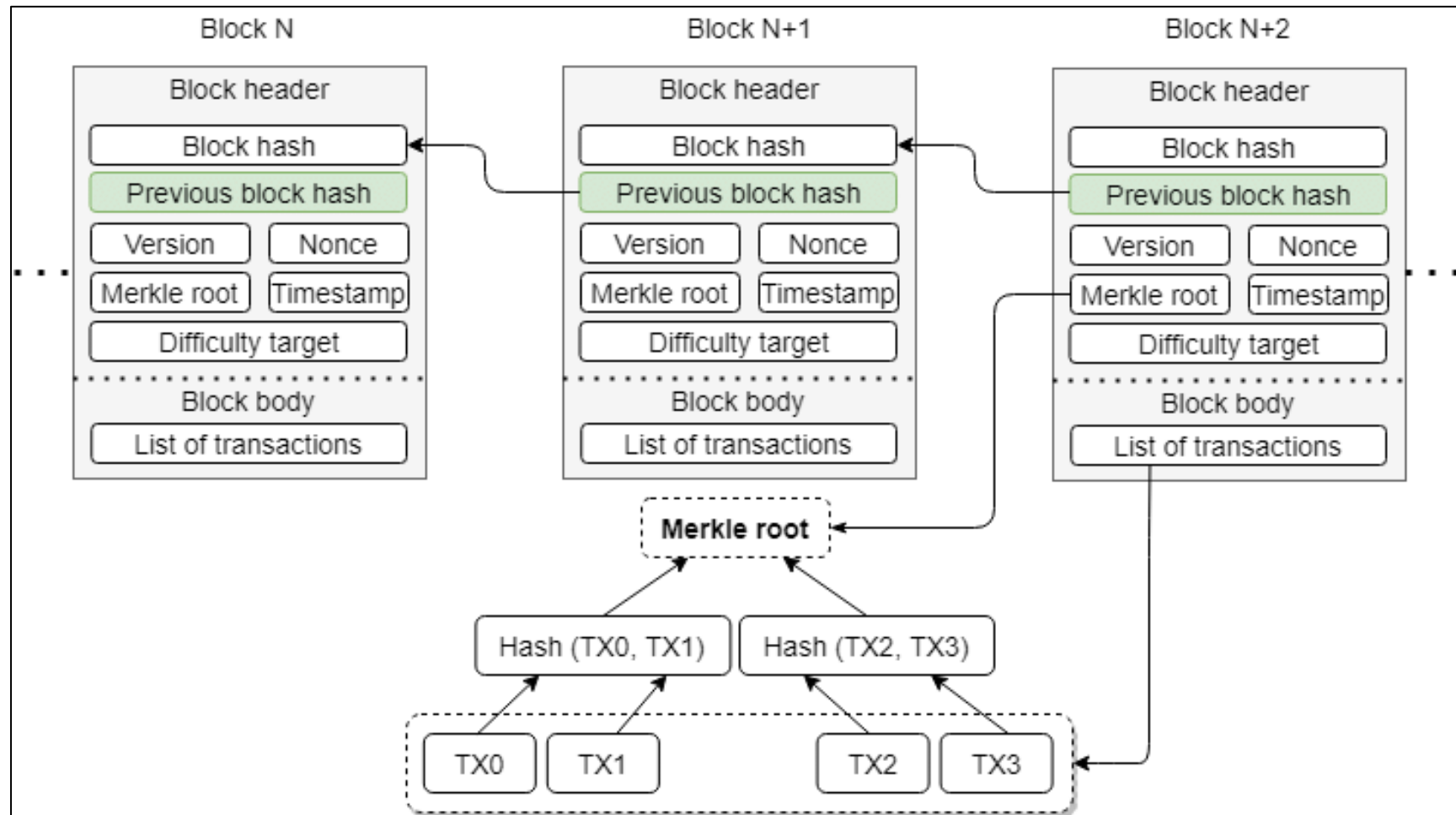
量子密鑰交換(Quantum Key Distribution, QKD)



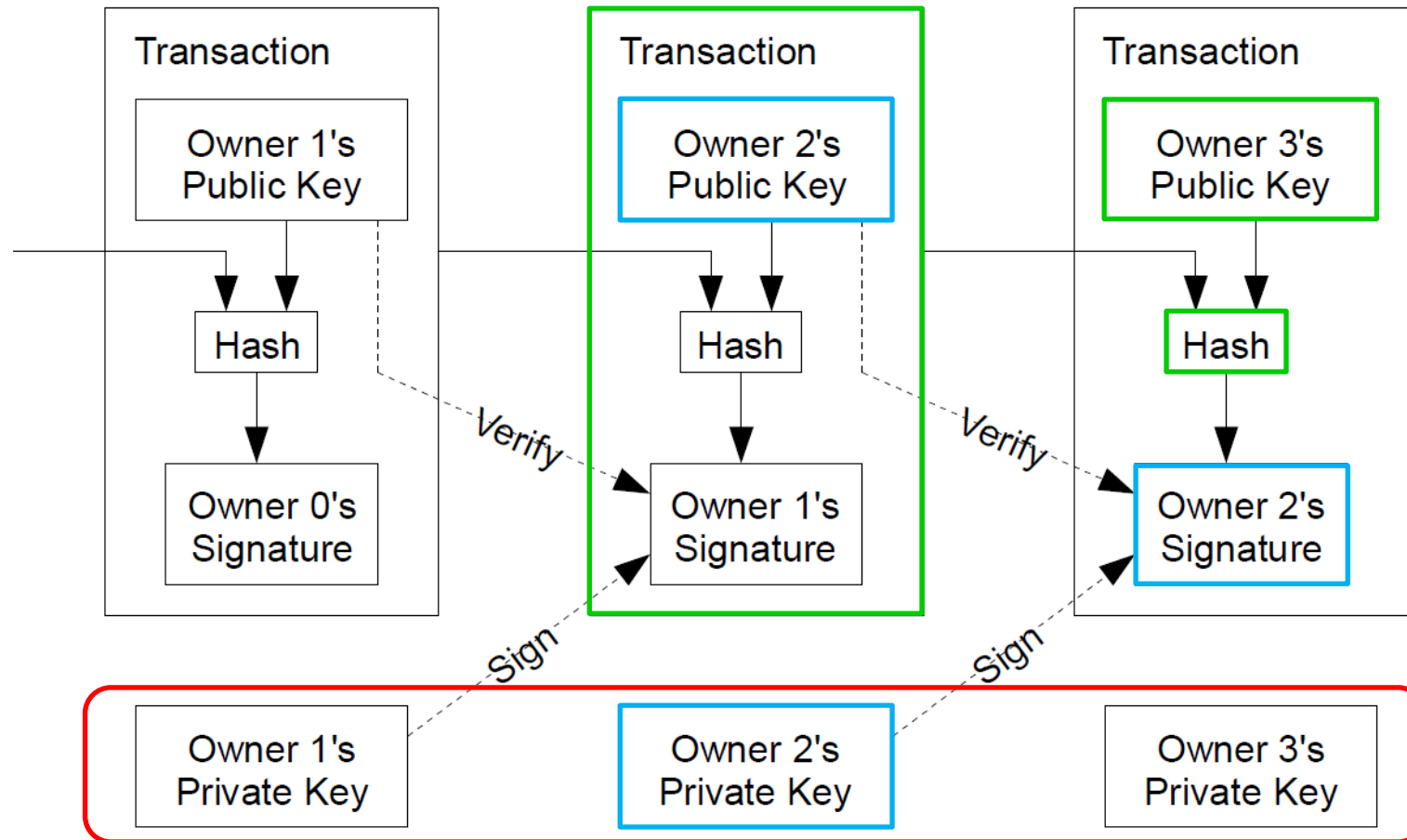
4. Blockchain and Cryptocurrencies:

- Blockchain, a decentralized and distributed ledger technology, relies heavily on cryptography. Cryptography is used to secure transactions, create **digital signatures**, and maintain the integrity of the blockchain.
- Cryptocurrencies, like Bitcoin, use **cryptographic principles to secure financial transactions and control the creation of new units.**





Bitcoin Transactions



Must be protected very well!!!

Encryption is a critical component of security.

You use strong encryption daily, and our Internet-laced world would be far riskier if you did not.

Encryption is the last line of defense for security.

Why is Cryptography Engineering essential, and why it matters?

Cryptography performs four important functions:

1. **Confidentiality:** Keeps the contents of the data secret
2. **Integrity:** Verifies the origin of the message or data
3. **Authentication:** The capability of a system to identify the sender of a message correctly
4. **Nonrepudiation:** Prevents the sender of the data or message from denying they were the origin

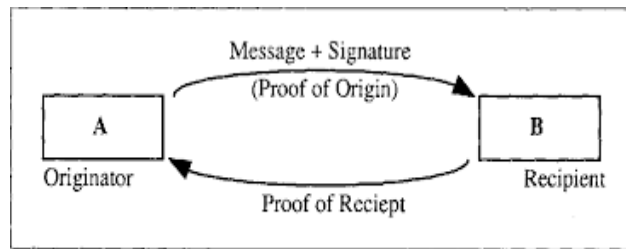


Figure 2 : Simple Non-Repudiation Scheme

When do we need Cryptography Engineering?

- **Security and Privacy:**

- **Confidentiality:** Cryptography ensures that sensitive information remains confidential and inaccessible to unauthorized parties. This protects user data, financial transactions, and other confidential information.
- **Integrity:** Cryptographic techniques help ensure data integrity, making it difficult for attackers to modify or tamper with information without detection.
- **Authentication:** Cryptography provides mechanisms for verifying the identity of parties involved in communication, essential for establishing trust in online transactions and communication.

Privacy relates to any rights you have to control your personal information and identity.

Security refers to how your personal information is protected.



Why do we need Cryptography Engineering?

- **Secure Communication:**

- In the digital age, secure communication is vital. Crypto engineering ensures that information transmitted over the network is encrypted, making it difficult for eavesdroppers to intercept and understand the content.

- **Data at Rest Protection:**

- Encrypting data at rest secures files and documents, ensuring only those with the key can access them. The files are useless to anyone else. This prevents data leakage, unauthorized access, and physical theft—unless attackers compromise the key management scheme and gain access.

- **Preventing Unauthorized Access:**

- Cryptography plays a crucial role in access control and authentication systems. Passwords are often stored using cryptographic hash functions, and cryptographic protocols are used to secure login sessions.

- **Digital Signatures:**

- Cryptographic techniques such as digital signatures help verify the authenticity and origin of digital messages. This is essential in applications *like secure communication, e-commerce, and digital contracts*.

Why do we need Cryptography Engineering?

- **Compliance and Regulations:**

- Many industries and applications are subject to regulatory requirements and compliance standards. Crypto engineering helps organizations meet these standards by implementing secure and privacy-preserving solutions.
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a US law that limits the use of protected health information (PHI) by healthcare organizations, which it refers to as covered entities.
- The General Data Protection Regulation, or GDPR, became law on May 25, 2018, and is one of the most stringent data privacy and security laws worldwide.

- **Defense Against Cyber Attacks:**

- With the increasing frequency and sophistication of cyber attacks, cryptographic techniques provide a strong line of defense. They help protect against various attacks, including man-in-the-middle attacks, data breaches, and ransomware.

- **Cutting-Edge Technologies:**

- As technology advances, new challenges and opportunities arise. Crypto engineering becomes crucial in addressing the security and privacy concerns associated with emerging technologies such as the Internet of Things (IoT), cloud computing, and artificial intelligence.

Challenge of Cryptography Engineering

1. Key Management:

- Generating, distributing, storing, and revoking encryption keys can be complex. Effective key management is essential for maintaining the security of encrypted data.
- If encryption keys are compromised, it can lead to a complete security breakdown. Regularly updating and rotating keys is important to minimize the risk.

2. Quantum Computing:

- The advent of quantum computing poses a potential threat to traditional encryption algorithms like RSA and ECC (Elliptic Curve Cryptography). Quantum computers could break these algorithms using Shor's algorithm, compromising the security of encrypted data.
- Developing quantum-resistant encryption methods is an ongoing challenge in cryptography.

3. Performance Overhead:

- Encryption and decryption processes can introduce computational overhead, impacting system performance. This is particularly relevant in resource-constrained environments like mobile devices or IoT (Internet of Things) devices.
- Striking a balance between security and performance is crucial, especially in scenarios where real-time processing is essential.

Challenge of Cryptography Engineering

4. **Backdoors and Vulnerabilities:**

- Creating intentional or unintentional backdoors in encryption systems can undermine their security. Governments, organizations, or malicious actors may attempt to exploit vulnerabilities for unauthorized access to encrypted data.
- Ensuring the integrity of encryption algorithms and protocols is vital to prevent the introduction of weaknesses.

5. **Social Engineering and User Behavior:**

- No matter how robust the encryption technology is, human factors remain a significant challenge. Users may inadvertently compromise security through weak passwords, sharing sensitive information, or falling victim to phishing attacks.
- Educating users on secure practices and implementing multi-factor authentication can help mitigate these risks.

LECTURE 0:

COURSE INFORMATION

Cryptography Engineering, Spring 2024

Agenda

- 老師介紹和聯絡方式
- 課程大綱
- 成績計算方式
- Ethics

- Level: **Elective** graduate-level course
- Time: Thursday 18:30-21:20
- Location: 工程四館 ED 117
- Email: jerry.shieh@nycu.edu.tw
- Knowledge and skills preferred
 - Computer Network concept
 - Basic knowledge of Discrete Math will be plus
 - Programming skills: Python, Java, C++

Teaching Team & Office Hours

謝致仁老師: Thursday 18:30 to 21:20 jerry.shieh@nycu.edu.tw

Line id: js590

助教: 古聖聰 kust.c@nycu.edu.tw

助教: 杜 峯 dufeng@nycu.edu.tw

助教: 單宇晟 syc910415.cs09@nycu.edu.tw

重要事項老師或助教會寄信至同學們的信箱，並在課程網站上公告

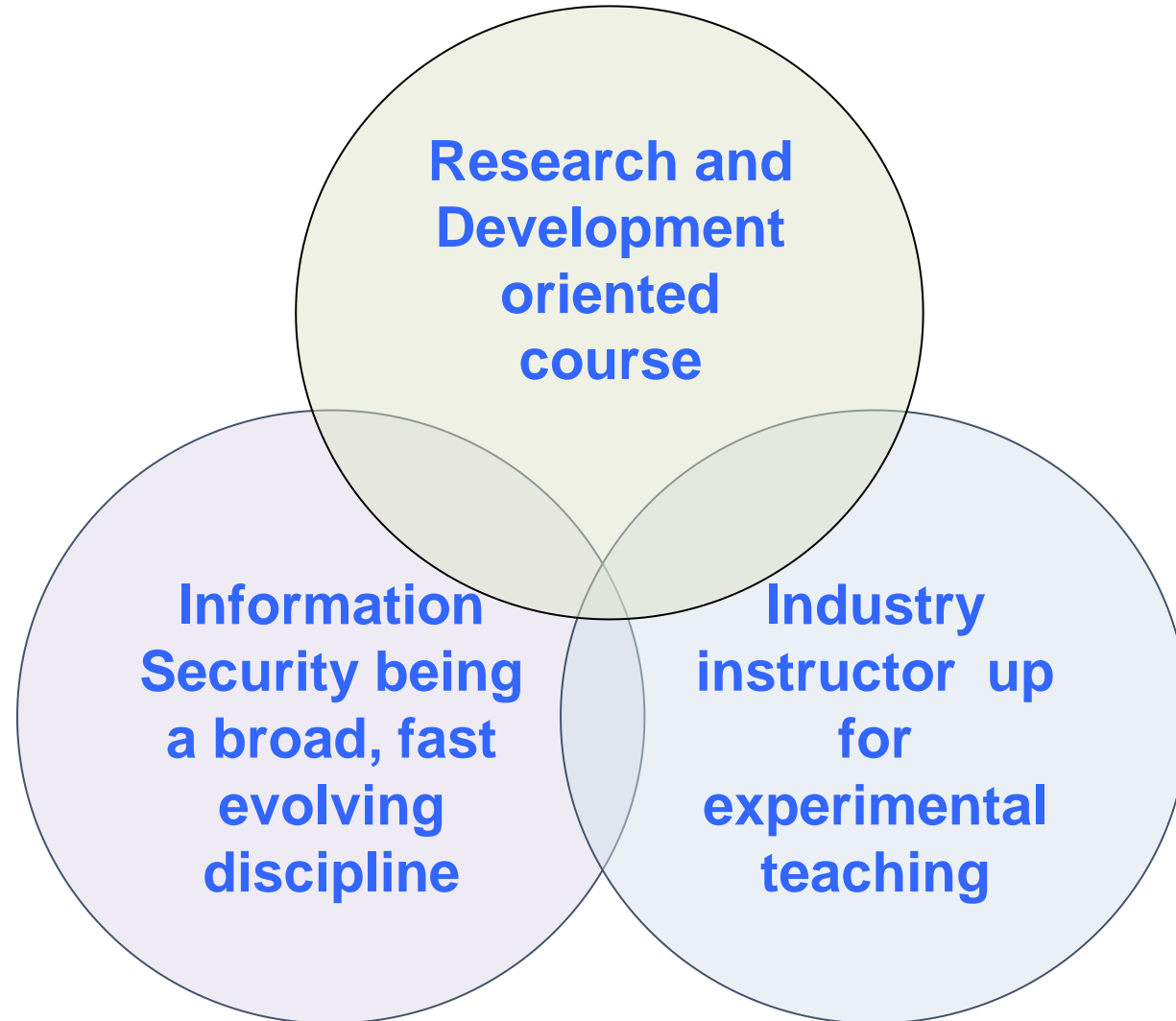
Lesson Objective

- After finishing the course and passing, you should be able to obtain the following capabilities:
 - Understand key concepts in building up an encryption system
 - Classic and modern cryptanalysis and attack skills
 - Identify and cryptosystem security threats
 - Potential mitigation and countermeasures
 - Build encryption mechanisms both software and hardware
 - Reason whether real-world security systems can achieve such desired goals

Learning Objective

- How to accomplish our objectives.
- We will practice the “security mindset” – **thinking like an attacker & thinking about how things can be made to fail.**
- We will learn a variety of **attack and defense techniques.**
- This course covers important concepts in security but is not meant to be comprehensive.
- You’re expected to search for answers and learn by yourself in this graduate-level course.

Our Course Design and Features



Our Course Scope: A metaphor

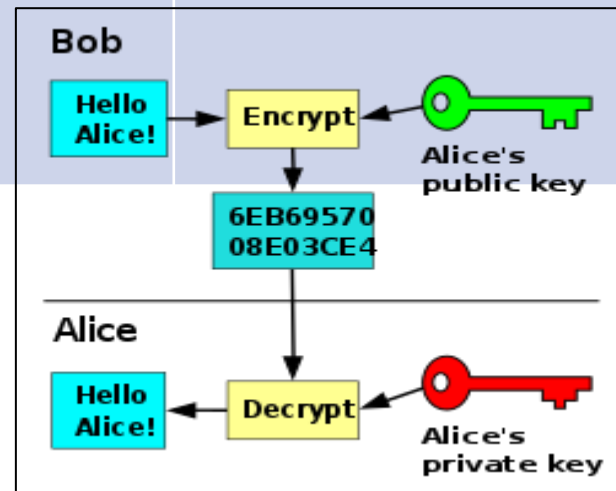
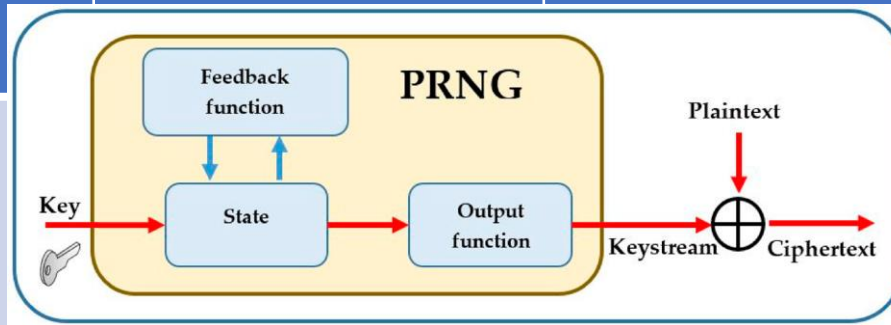
Elementary
Cryptography

Stream and Block
Cipher Engineering

Practical Public Key
Encryption

Authenticated
Encryption

Practical
Quantum
Cryptography



Tentative Class Schedule

Week	Date	Topics
1	2/22	What is cryptography?
2	2/29	Classic and modern cryptanalysis and One Time Pad
3	3/07	Stream cipher and True and pseudorandom generators
4	3/14	Attacks on stream cipher and PRNG
5	3/21	Real-world stream cipher and NIST SP-800-22 / 90
6	3/28	Block cipher attacks and its design
7	4/04	Spring off
8	4/11	AES-like system and S-box design
9	4/18	Block cipher mode operation attacks

Tentative Class Schedule

Week	Date	Topics
10	4/25	Message integrity and Public Key Encryption
11	5/02	Authenticated encryption
12	5/09	Take home exam
13	5/16	Secure crypto processor application
14	5/23	Public key encryption and its attacks
15	5/30	Final Projects I
16	6/06	Final Projects II
17	6/13	Final Projects III
18	6/20	Final Projects IV

Grading Components

- Quiz and homework assignments (6+*5%)
- Reading critiques (4*5%)
- Midterm exam (20%)
- Group project (20%)
 - Written proposal (5%)
 - Final oral presentation (5%)
 - Final report (10%)
- Class participation (10+%)



Grading Components 1:

Quiz and Homework Assignments

- 6+ Quiz and Homework assignments
- May contain programming labs
- Details will be announced soon
- Due policy: Due at the beginning of the next lesson.

Grading Components 2:

Critique should contain the following:

1. **Summary** – answering these four questions in your own words:

What problem is the paper trying to solve?

Why does the problem matter?

What is the approach used to solve the problem?

What is the conclusion drawn from this work?

2. **Strength(s) of the paper**

3. **Weakness(es) of the paper**

4. **Your own reflection, which can include but not limited to:**

What did you learn from this paper?

How would you improve or extend the work if you were the author?

What are the unsolved questions that you want to investigate?

What are the broader impacts of this proposed technology?

5. **Realization of a technical specification or algorithm as a program earn extra credit.**

Write a critique on one of the following papers:

- **Password Managers: Attacks and Defenses**

David Silver, Suman Jana, and Dan Boneh, Stanford University; Eric Chen and Collin Jackson, Carnegie Mellon University.

- Text-only, about 1000-1200 words
- With programming lab will earn extra credits.

Grading Component 3:

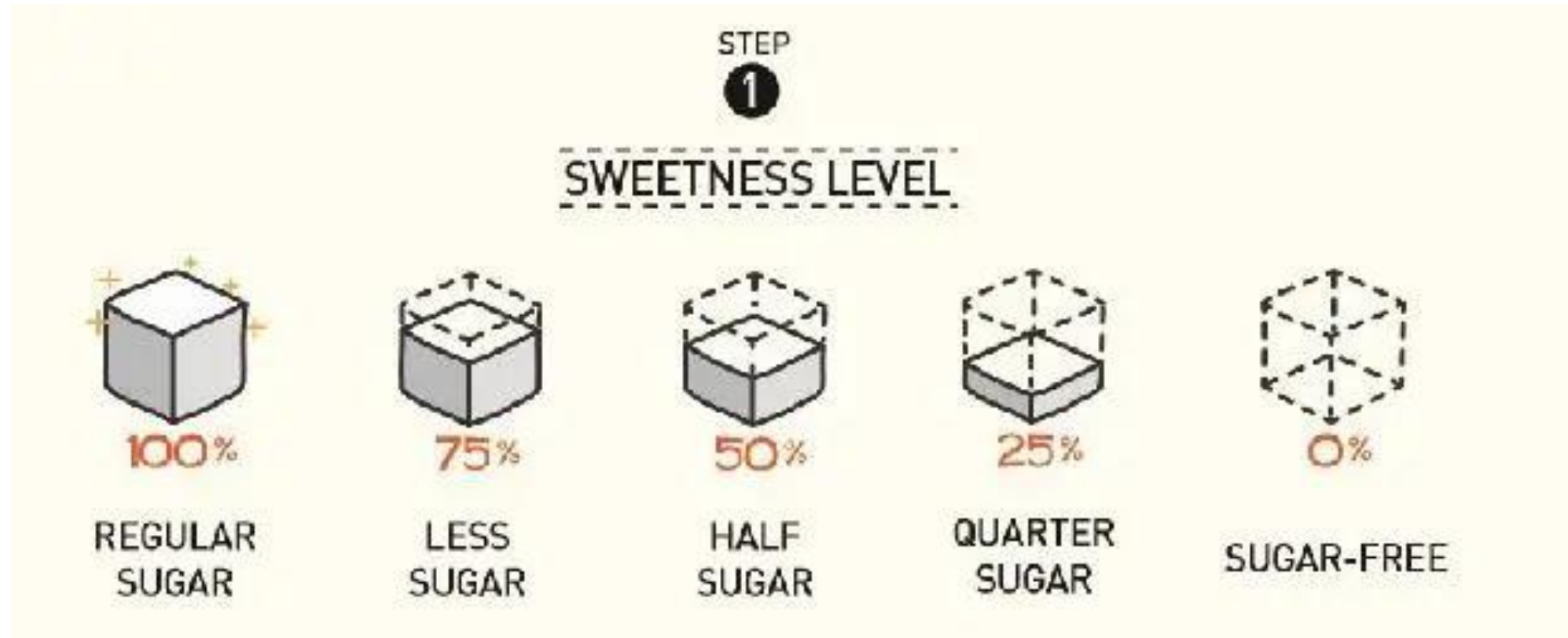
Group project

- 1-5人
- 時程
- 三月底前繳交分組名單和所選題目
- 四月底前繳交提案 (Proposal)
- 6/6 6/13 6/20 期末報告程式碼與展示，每一組約15~20分鐘(參考全班互評成績)
- 六月底前繳交期末書面報告及程式碼!
- Finding your project partners soon!

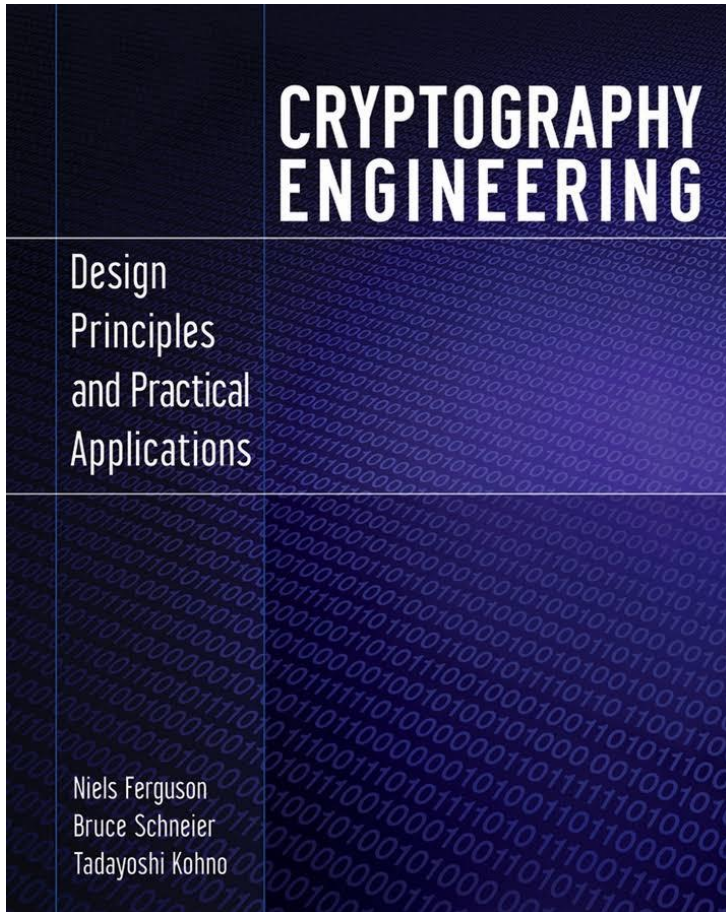
Course Policies

- 大原則：不要打擾別人或影響老師上課
- **Late submission policy**
 - **Critiques and quiz:** Late submission is allowed with the penalty.
 - **Project proposal and report:** Late submissions are not accepted.
 - It is very important to submit all class assignments.
- **Collaboration policy**
 - Discussion is encouraged, but you must acknowledge.

Consistent submission of assignments is crucial for passing my class.
Missing a submission may fail the entire course.



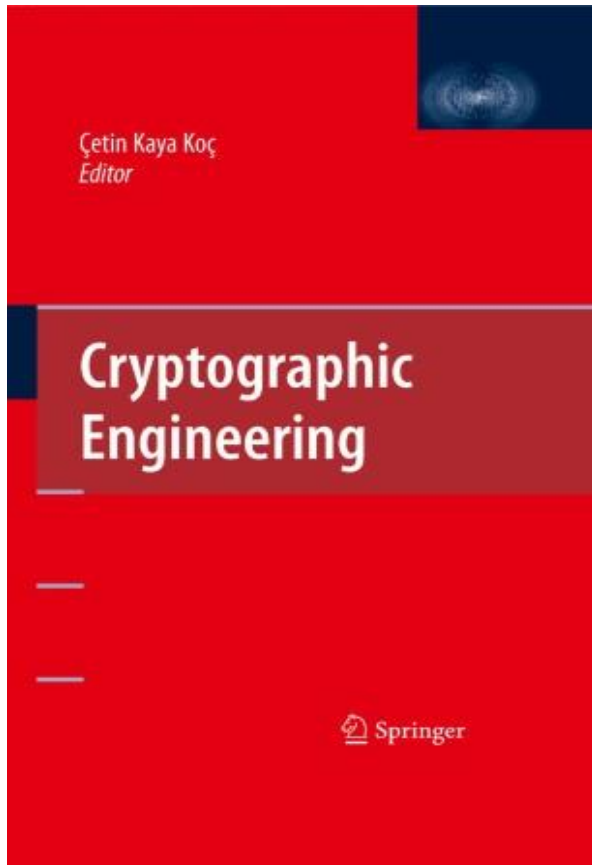
Optional textbooks (all available online)



Cryptography Engineering

Design Principles and Practical Applications

A book by Niels Ferguson,
Bruce Schneier, and Tadayoshi
Kohno



Cryptographic Engineering

Editor

Çetin Kaya Koç,

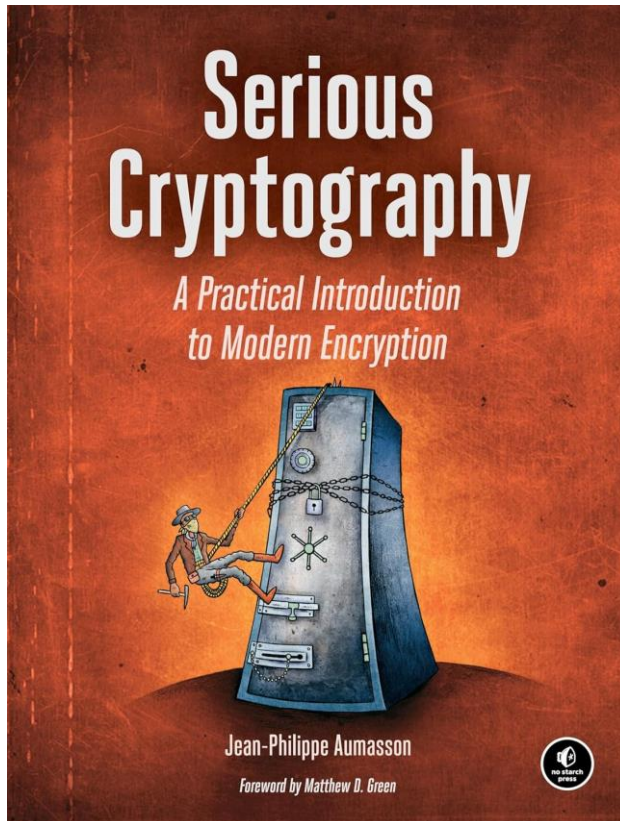
City University of Istanbul

Tophane, Istanbul Turkey

and University of California Santa Barbara

Santa Barbara, CA, USA

<https://helix.stormhub.org/data/Advanced%20Topics%20in%20Security/Books/Cryptographic%20Engineering.pdf>



Serious Cryptography:

A Practical Introduction to Modern Encryption

Jean-Philippe Aumasson
ISBN 978-1593278267

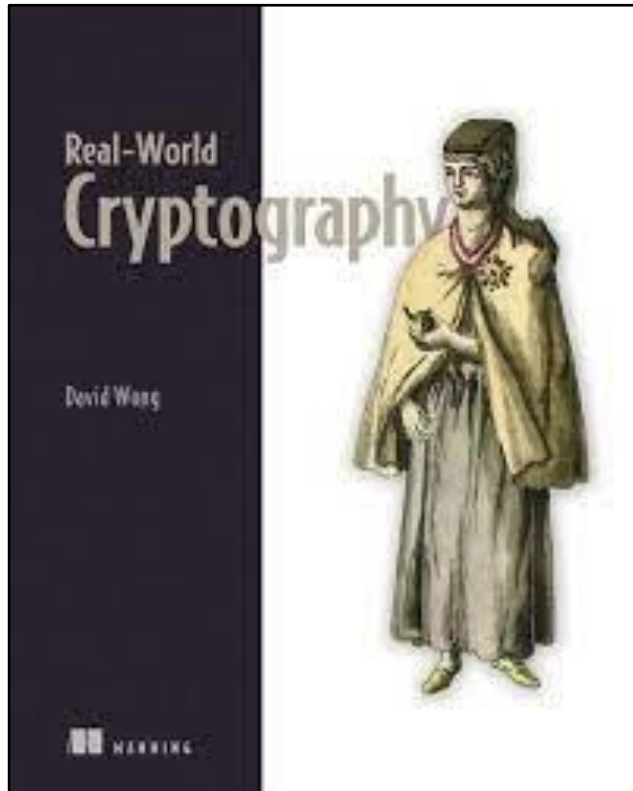
Key concepts in cryptography, such as computational security, attacker models, and forward secrecy

The strengths and limitations of the TLS protocol behind HTTPS secure websites

Quantum computation and post-quantum cryptography

About various vulnerabilities by examining numerous code examples and use cases

How to choose the best algorithm or protocol and ask vendors the right questions



Real-World Cryptography David Wong

ISBN:1617296716

Best practices for using cryptography Diagrams and explanations of cryptographic algorithms

Implementing digital signatures and zero-knowledge proofs

Specialized hardware for attacks and highly adversarial environments

Identifying and fixing bad practices
Choosing the right cryptographic tool for any problem

做世界一流的研究(神人)

- (1) 重要的問題
- (2) 新穎性直觀的想法，讓人容易理解
- (3) 研究方法流程嚴謹
- (4) 實驗要能全面性涵蓋，並能線上展示
- (5) 結果令人信服且有意義

Shih-Fu Chang is a Taiwanese American computer scientist and electrical engineer noted for his research on multimedia information retrieval, computer vision, machine learning, multimedia Security and signal processing. He is currently the dean of the School of Engineering and Applied Science of Columbia University.

做個有意義的研究_(達人)

- (1) 用傳統方法產生創新的應用 Cryptanalysis using AI
- (2) 實作及比較某一個重要領域的方法，比較其效能，並提出深入分析或提出一個benchmark (Modified AES)
- (3) 對一個重要問題或演算法，完整實作一個好用的程式庫

- 例如林智仁老師的libsvm，被引用次數超過四萬次。而進行研究的初期，必須讓自己的想法有初步的work，可用一些現成的資料測試驗證，先有一些實驗結果再繼續做研究。

QUIZ 0

- 你為什麼要上密碼工程?
- 你對上密碼工程有什麼想要學到的東西?
- 這門課你需要老師先幫你做些什麼?
- 今天的簡介是開心還是害怕?
- E-mail jerry.shieh@nycu.edu.tw
- 姓名 學號 系所別 年級