Quantum Cryptography

Mahima Mary Mathews, PhD Scholar, IIIT Kottayam
Research Coordinator and Consultant, Cyberlabs IIIT Kottayam

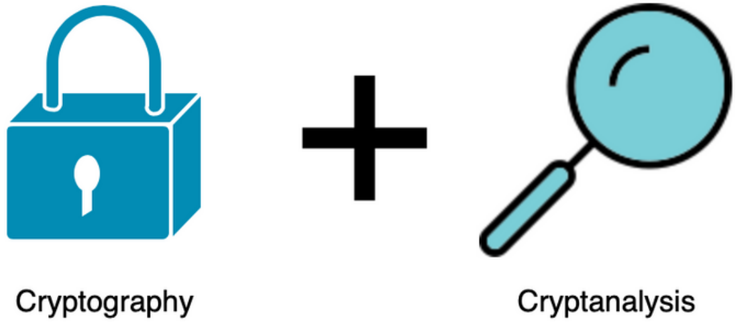
03-June-2023

Cryptology

Study of codes, both creating and solving them the problem.

Criptos = Secret , Logos = Science

Kryptos = Hidden, Graphein = Write



Cryptography

Art of creating codes.

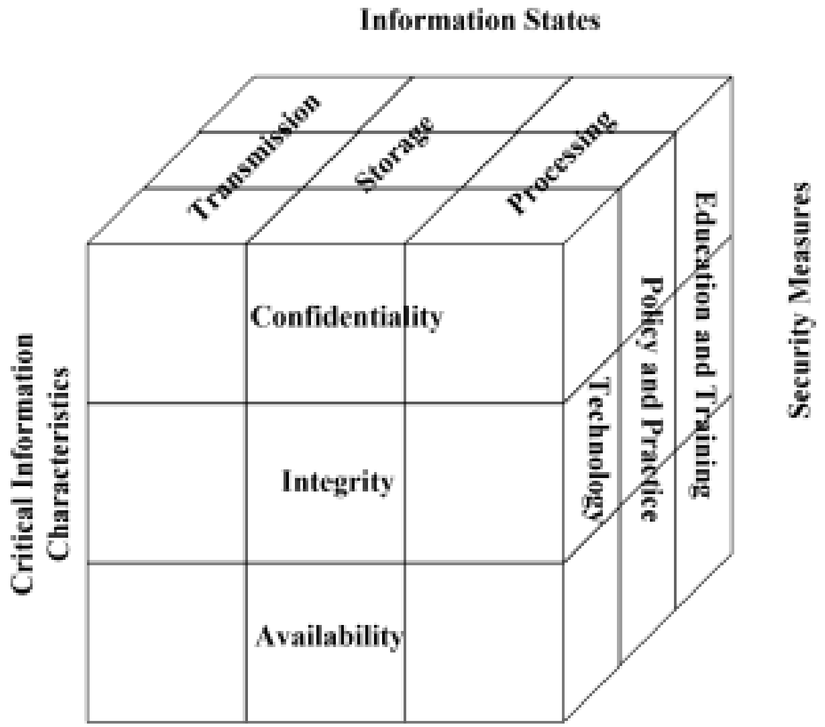
Cryptanalysis

Art of surreptitiously revealing the contents of coded messages, breaking codes, that were not intended for you as a recipient.

Cryptography is important in protecting data and users, ensuring confidentiality, and preventing cyber criminals from intercepting sensitive corporate information.

Information Security

- Hardware
- Software
- Network
- People
- Procedures
- Data



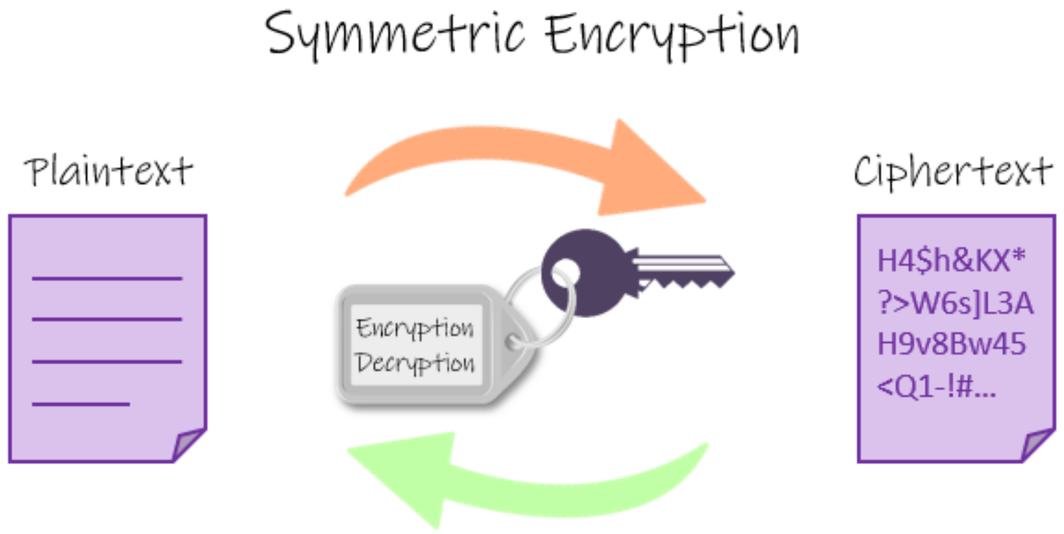
McCumber Cube

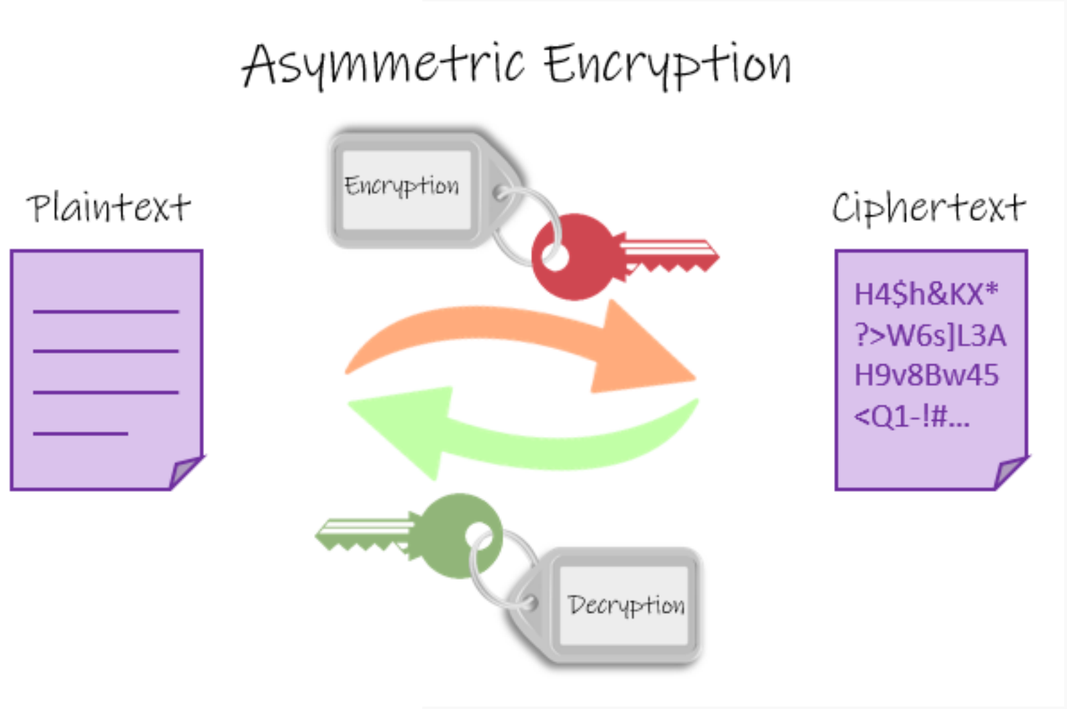
Classical Cryptography

Feature / Algorithm	Hash	Symmetric	Asymmetric
No. of Keys	0	1	2
NIST recommended Key length	256 bits	128 bits	2048 bits
Commonly used	SHA	AES	RSA
Key Management/Sharing	N/A	Big issue	Easy & Secure
Effect of Key compromise	N/A	Loss of both sender & receiver	Only loss for owner of Asymmetric key
Speed	Fast	Fast	Relatively slow
Complexity	Medium	Medium	High
Examples	SHA-224, SHA-256, SHA-384 or SHA-512	AES, Blowfish, Serpent, Twofish, 3DES, and RC4	RSA, DSA, ECC, Diffie-Hellman

Source : https://www.cryptomathic.com/news-events/blog/differences-between-hash-functions-symmetric-asymmetric-algorithms

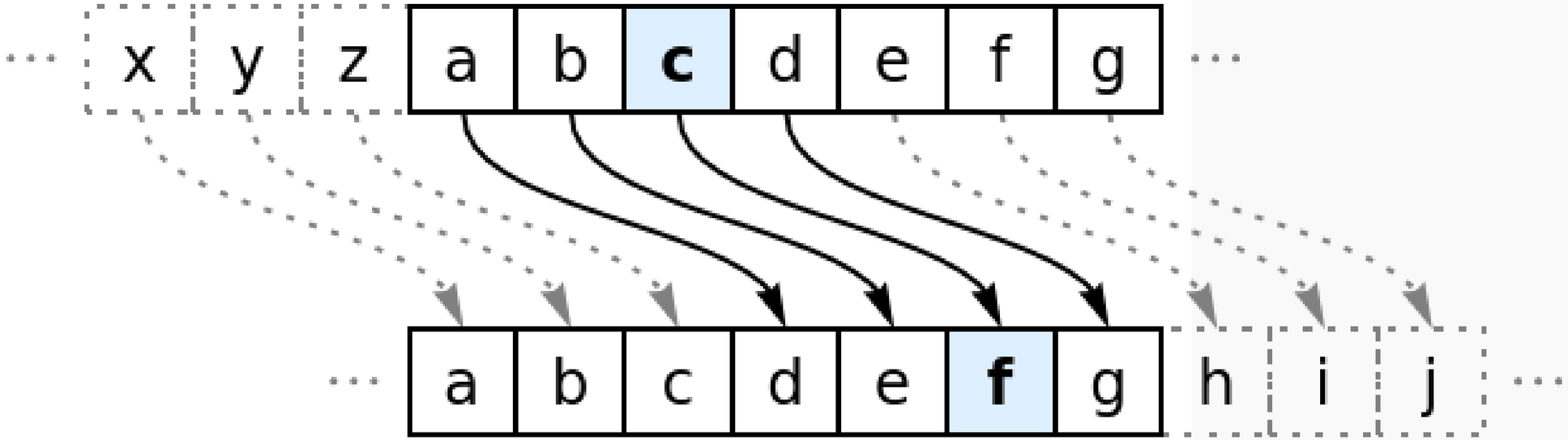
Classical Cryptography





Source : https://www.101computing.net/symmetric-vs-asymmetric-encryption/

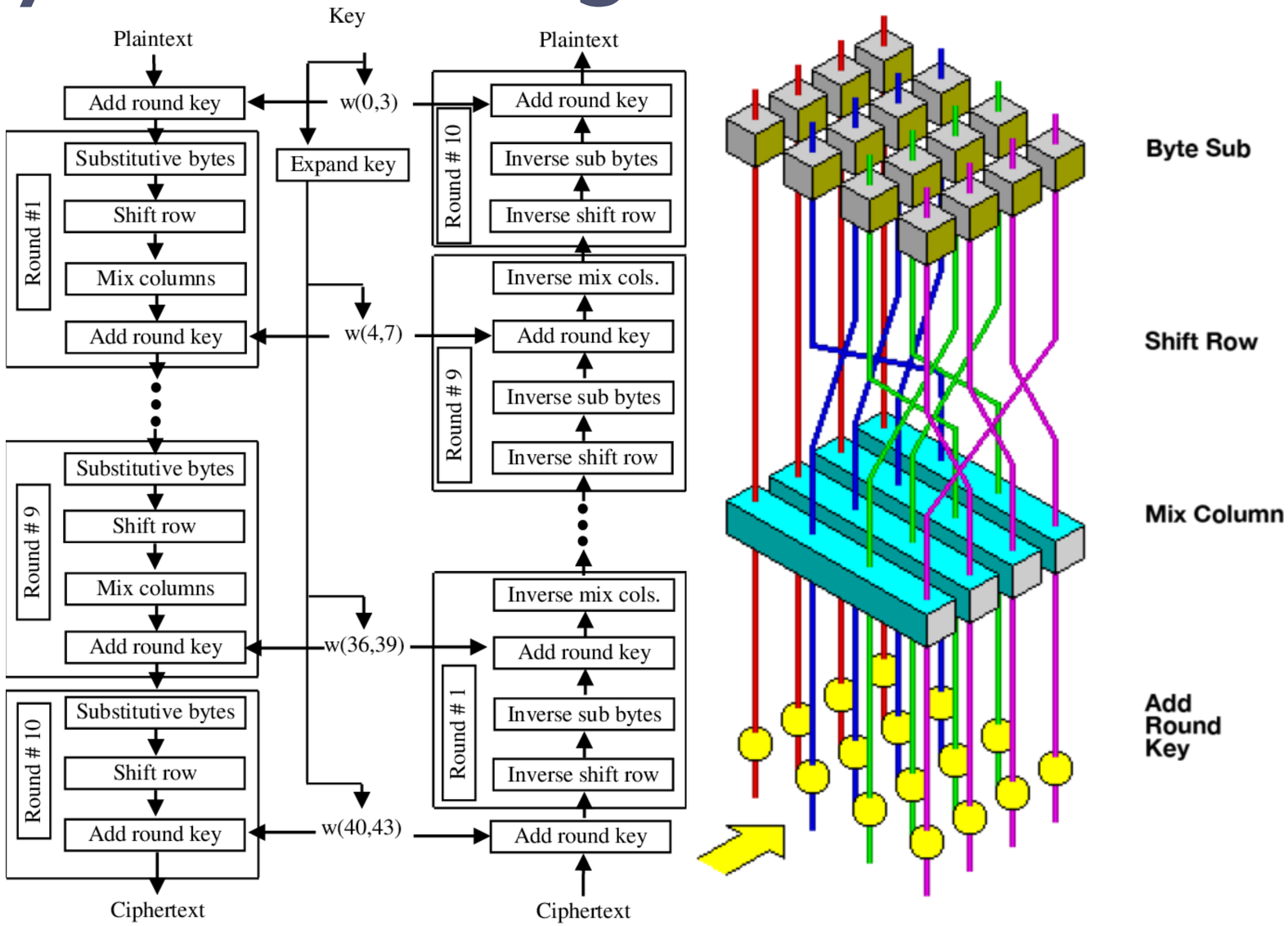
Symmetric Algorithm - Caesar Cipher



Example Website

Source : https://www.wolframcloud.com/obj/

Symmetric Algorithm - AES



[Example Website]

Source :

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

https://www.researchgate.net/

Asymmetric Algorithm - RSA

Key Generation

Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext	$M < n$
Ciphertext	$C = M^e \pmod{n}$

Decryption

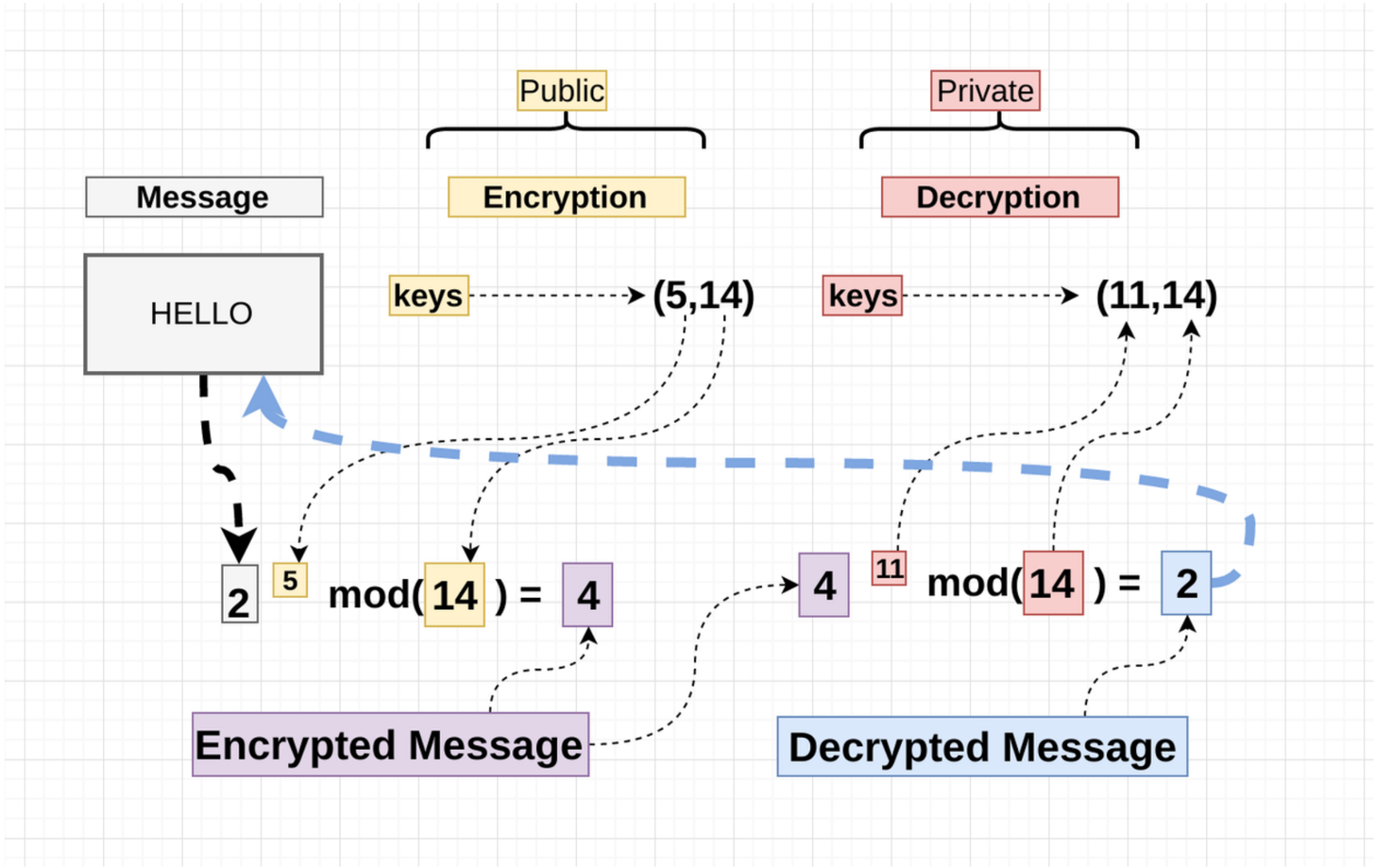
Ciphertext	C
Plaintext	$M = C^d \pmod{n}$

Example Website

Source :

https://www.researchgate.net/

Asymmetric Algorithm - RSA



Example Website

Source :

https://hackernoon.com/how-does-rsa-work-f44918df914b

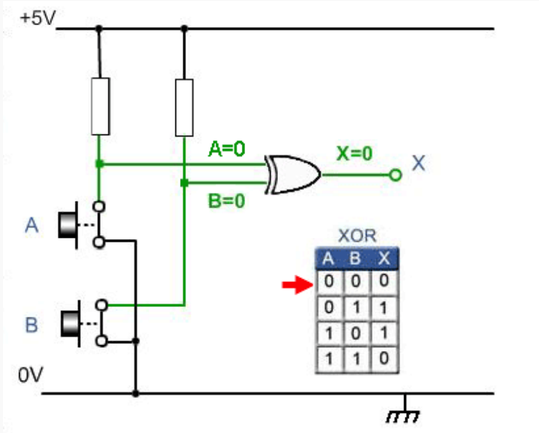
Hash Function

A "fingerprint" of a file, message, or other block of data. To be useful for integrity assurance, message authentication etc. a hash function H must have the following properties :

Simple Hash :

https://learnabout-electronics.org/

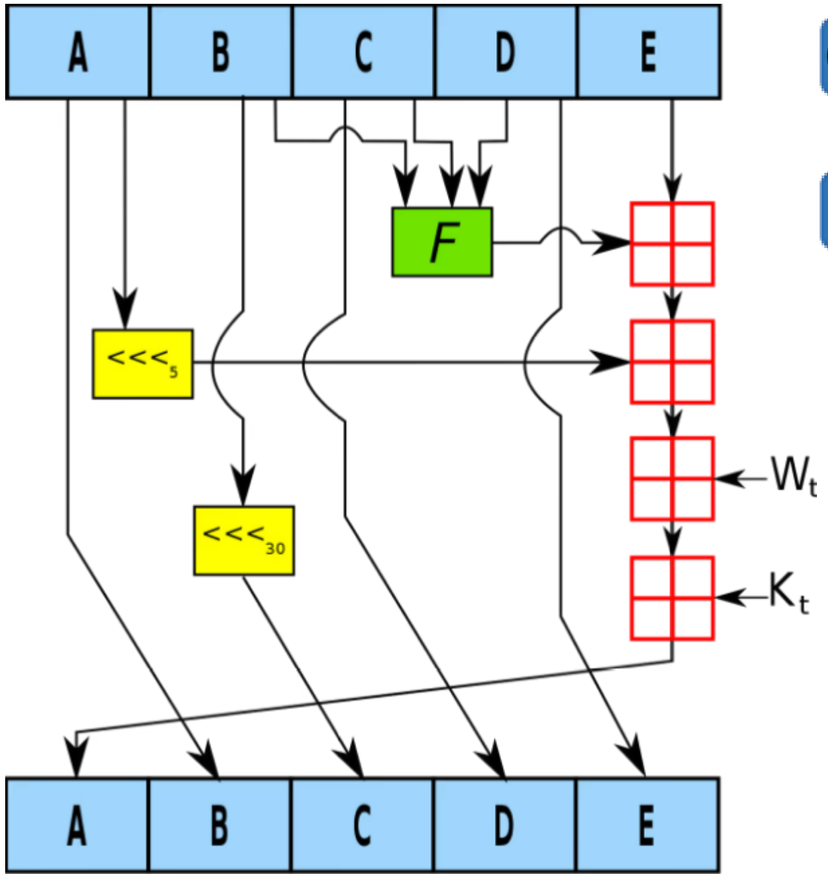
1. H can be applied to a block of data of any size.
2. H produces a fixed-length output.
3. H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
4. **One-way property**: For any given value h, it is computationally infeasible to find x such that H(x) = h.
5. **Weak collision resistance**: For any given block x, it is computationally infeasible to find y x such that H(y) = H(x).
6. **Strong collision resistance** : It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).

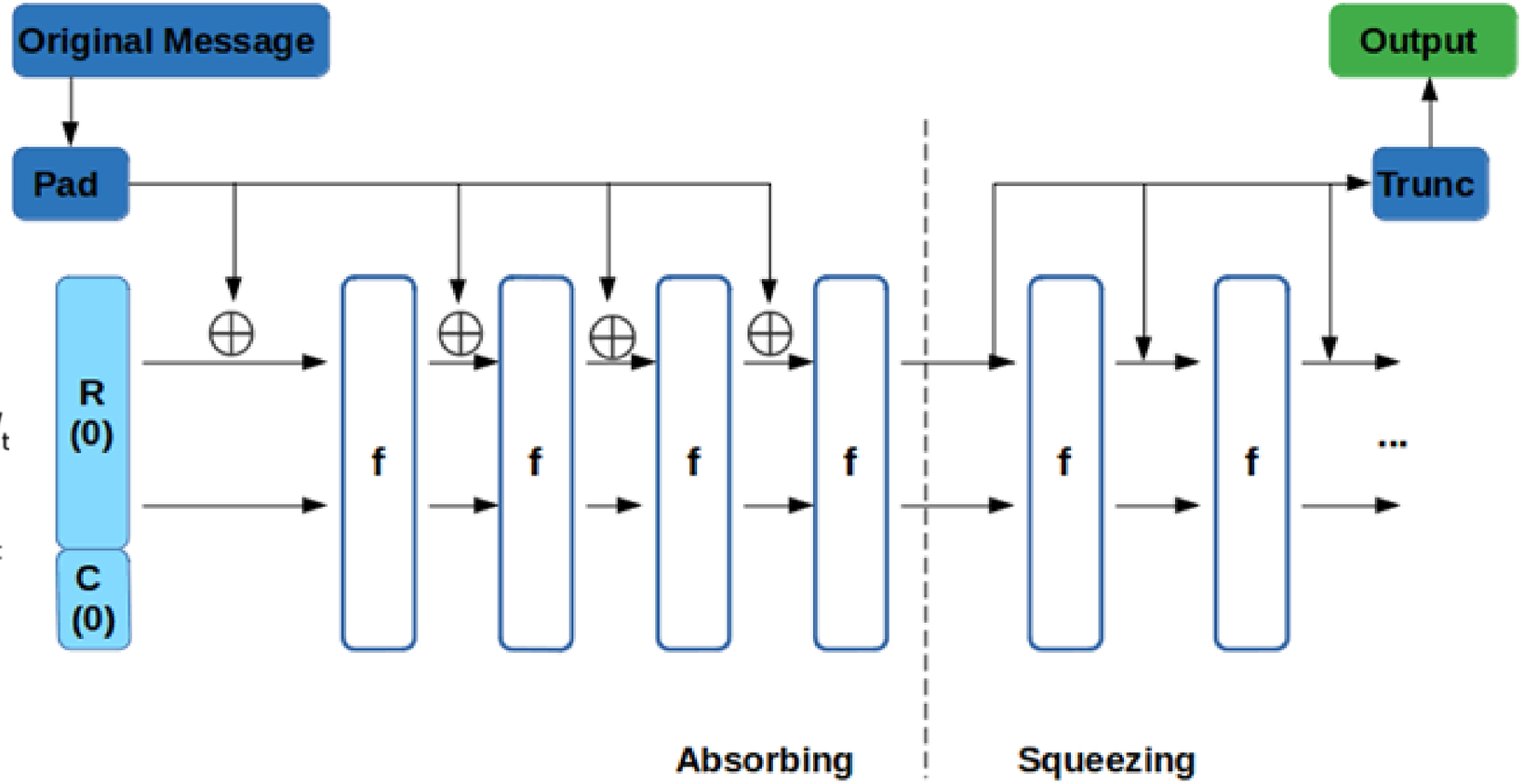


Other Important Terms:

- One-way hash function: (4 and 5); Weak one-way hash function: (4 and 5);
- Collision- resistant hash function: (4, 5, and 6); Strong one-way hash function: (4, 5, and 6).

Hash Function - SHA 1 vs SHA 3





Source : https://upload.wikimedia.org/ , https://codesigningstore.com/

Quantum Computing

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

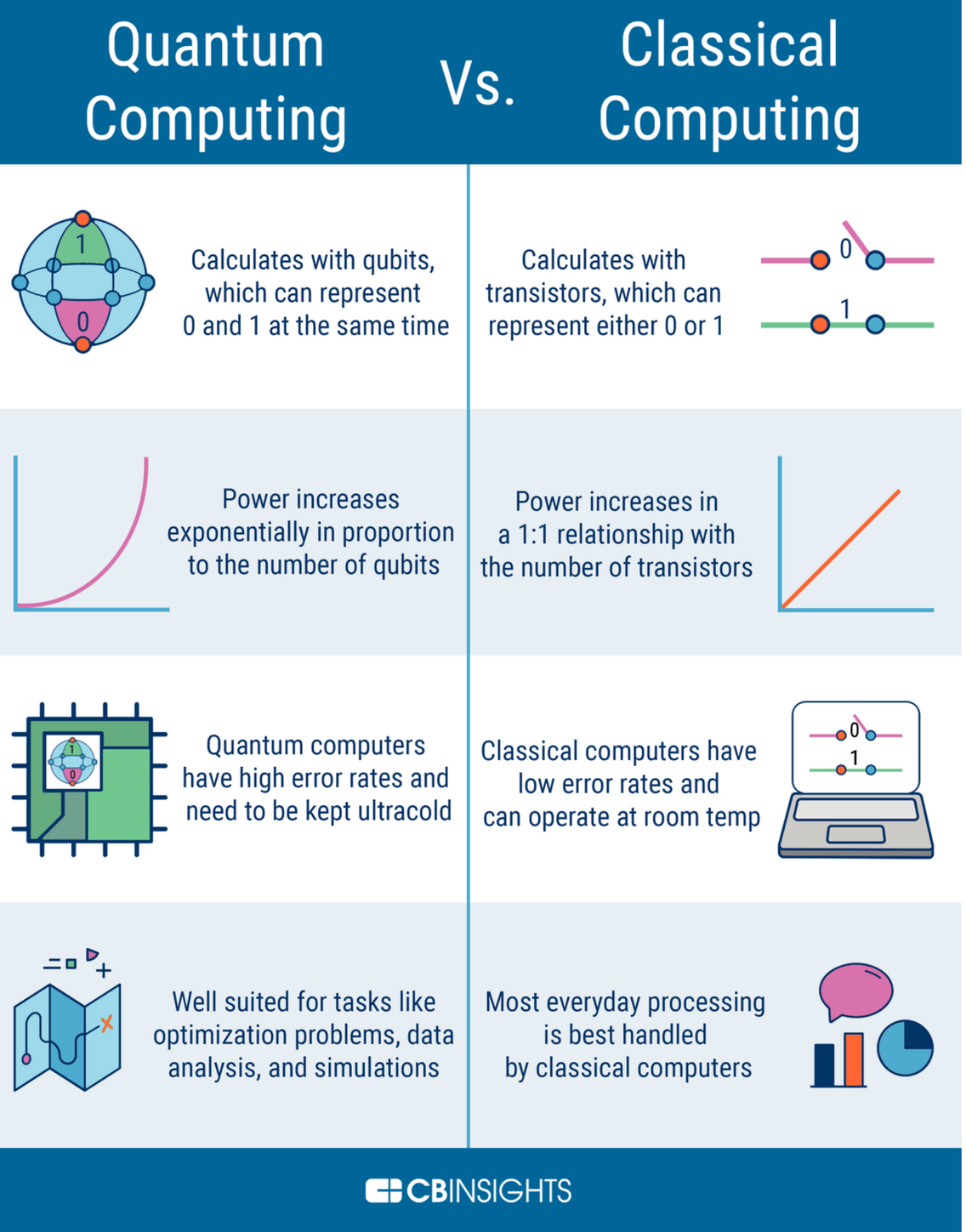
Then:

$$\sqrt{(|\alpha|^2+|\beta|^2)} = 1$$

Probability of measuring a state $|\psi\rangle$ in the state $|x\rangle$, $p(|x\rangle)=|\langle\psi|x\rangle|^2$

Column vectors -> kets $|a\rangle$ and Row vectors -> bras $\langle a|$.

The symbols ⟨ and | tell, $\langle a|$ is a Row vector, $|a\rangle$ is a Column vector.



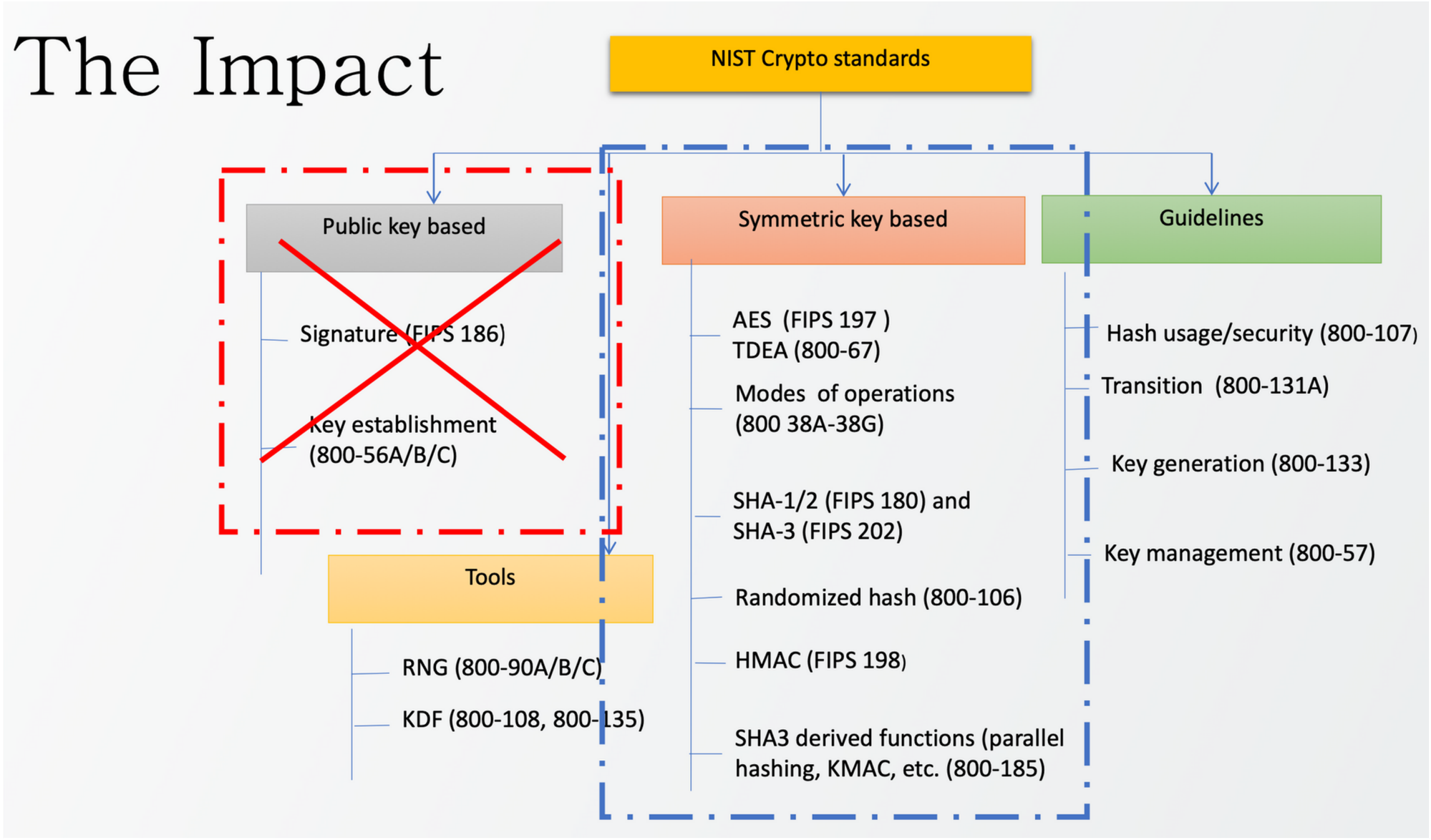
Impact of Quantum Computers

- Shor's Algorithm will help us factorize integers and finding discrete logarithms in Polynomial time, eventually breaking RSA and ECC.
  - Breaking a 2048-bit RSA(1977) algorithm requires 4098 qubits and 5.2 trillion Toffoli gates
  - Breaking a curve with a 256-bit modulus (128-bit security level) need 2330 qubits and 126 billion Toffoli gates.

- 1996, Grover's Algorithm will reduce the searching time

A quantum distinguisher which distinguishes Cipher outputs from a random permutation could be used to help reverse many types of block ciphers currently in use and break many forms of modern cryptography.

The Impact



Source : https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/PQCrypto-April2018_Moody.pdf

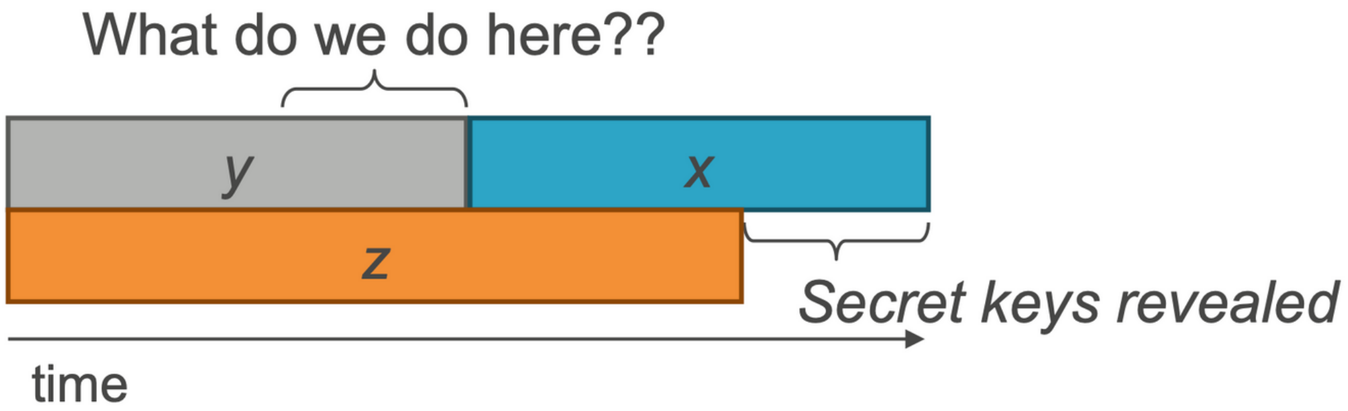
Time to worry ?

X : How long do you need encryption to be secure?

Y : How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution?

Z : How long will it take for a large-scale quantum computer to be built (or for any other relevant advance?

Cause of concern appears, if (Theorem : Mosca) X + Y > Z



Security in Quantum Era

- Quantum phenomenon based Cryptographic system
  - Encrypting, decrypting and keys algorithms are derived from quantum principles.
  - Quantum Cryptography (QC)
    - QKD, QSS, QSDC
  - Quantum Random Number Generators (QRNG)

- Physical characteristics or phenomenon based
  - Physical Unclonable Functions (PUF)
  - Physical or Phenomenon based True Random Number Generators

Security in Quantum Era

- Post Quantum Cryptography
  - Based on families of problems considered to be not solvable by Quantum Computers in bounded-error quantum polynomial (BQP) time.
    - Public-Key Encryption (PKE)
    - Key Encapsulation Mechanism (KEM)
    - Signature Schemes

- Combined architecture
  - Encrypting and decrypting algorithms depend on the classical methods
  - For example : Keys for message encrypting and decrypting are obtained from Quantum key distribution (QKD) protocol.

Quantum Cryptography

Quantum cryptography exploits the naturally occurring properties of quantum mechanics to perform cryptographic tasks.

- Quantum Key Distribution
- Quantum Secret Sharing
- Quantum Secure Direct Communication
- Quantum Random Number Generators (QRNG)
- Quantum Stream Cipher

- Quantum states can make possible new or improved cryptographic protocols protecting classical information. Example: QKD, Unclonable encryption
- Cryptographic methods can be applied to protect quantum information. Example: QSS

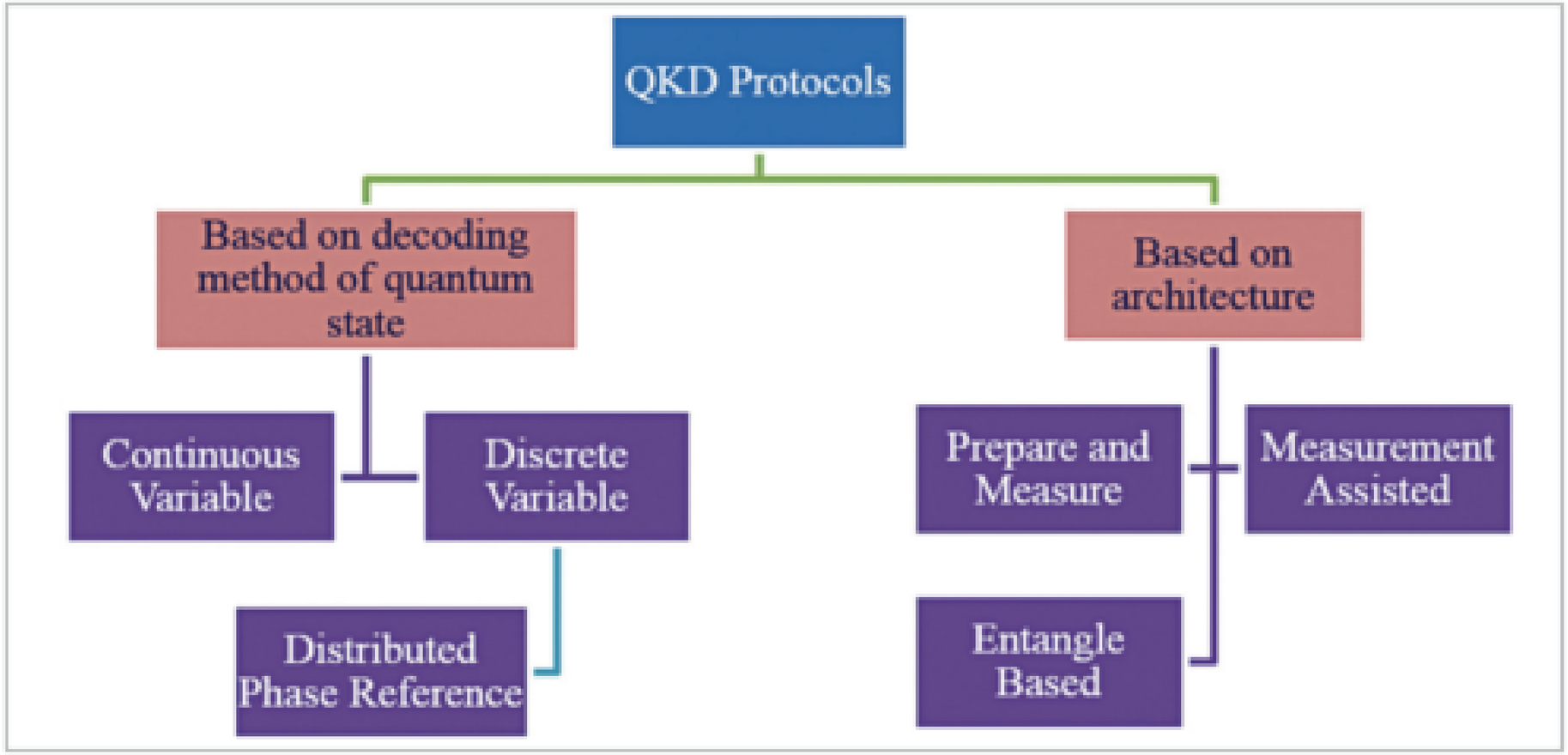
Fundamental Quantum Phenomenons

- Uses separate individual Quantum Objects:

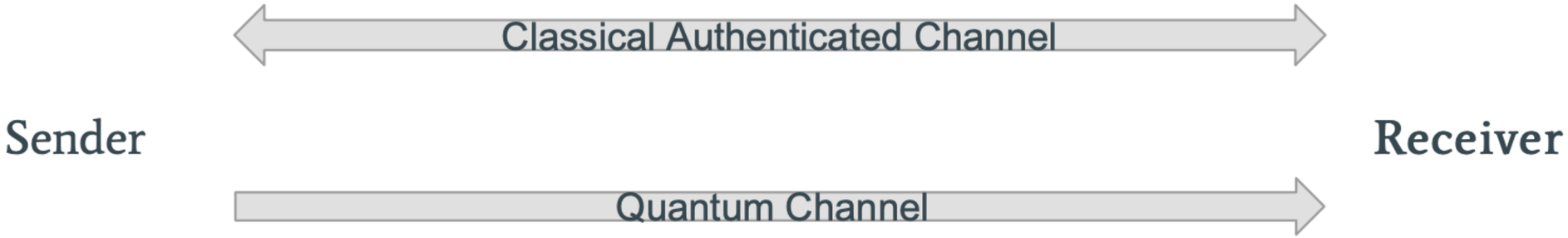
  Molecules, Atoms, Electrons, Photons

- Important Quantum Effects:
  - Superposition
  - Entanglement
  - Interference
  - Other important Effects
    - No-Cloning Theorem
    - Tunneling Effect
    - Uncertainty Principle
    - Teleportation

Quantum Key Distribution



Quantum Key Distribution - BB84



Attackers
Can read both channels

Quantum Key Distribution - BB84

Quantum States of Four polarizations:

- 0 - $|0\rangle$, polarization with degree 0. 
- 1 - $|1\rangle$, polarization with degree 90. 
- 0 - $|+\rangle$, polarization with degree 45. 
- 1 - $|-\rangle$, polarization with degree 135. 


Correct

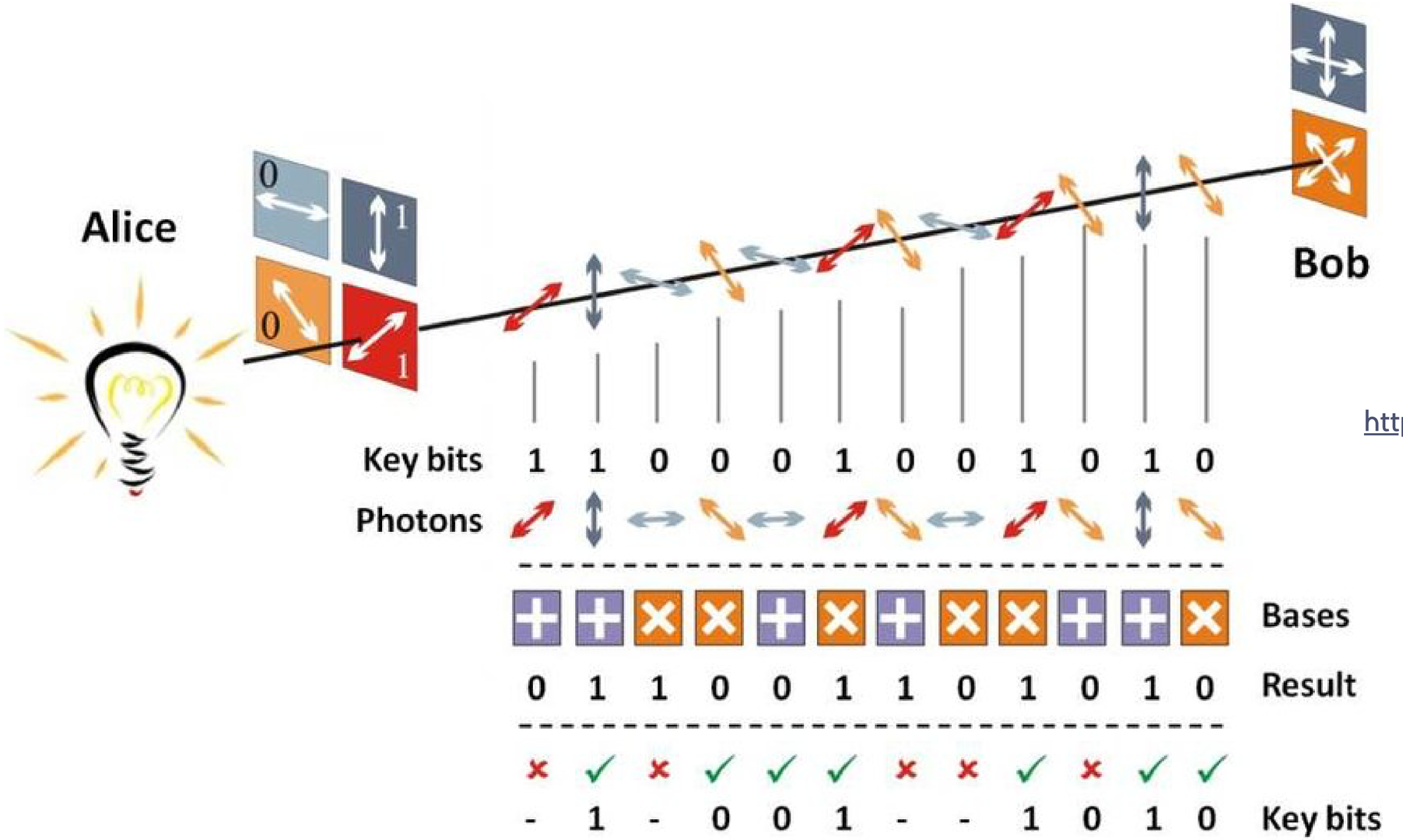

Random


Correct


Random

Simulation

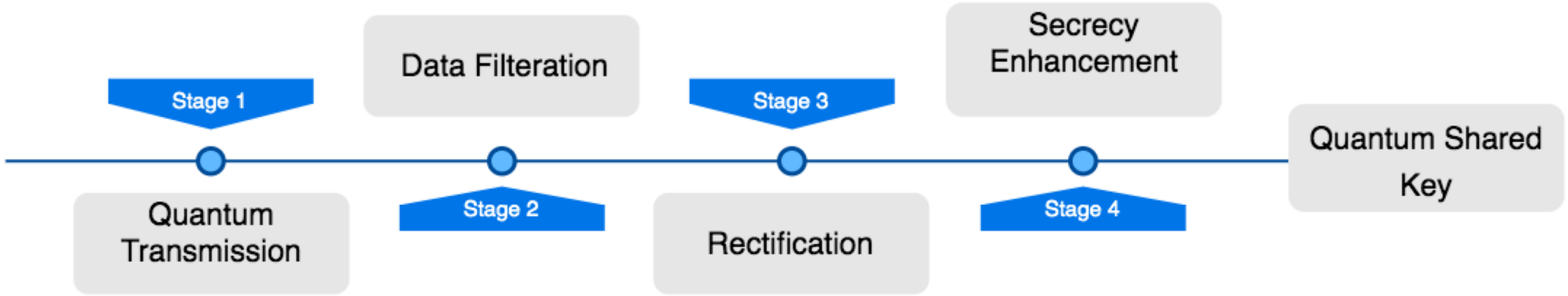
Quantum Key Distribution - BB84



Source :

https://www.researchgate.net/

Quantum Key Distribution - BB84



Source :https://pub.mdpi-res.com/sensors/sensors-22-06284/article_deploy/html/images/sensors-22-06284-g004.png?1661256423

Quantum Key Distribution - E91

Uses entangled state of two qubits.

- If sender and receiver measure in the same basis, the outcomes are correlated or anti-correlated depending in which basis they are measured.
- The probability of outcomes is uniformly random.

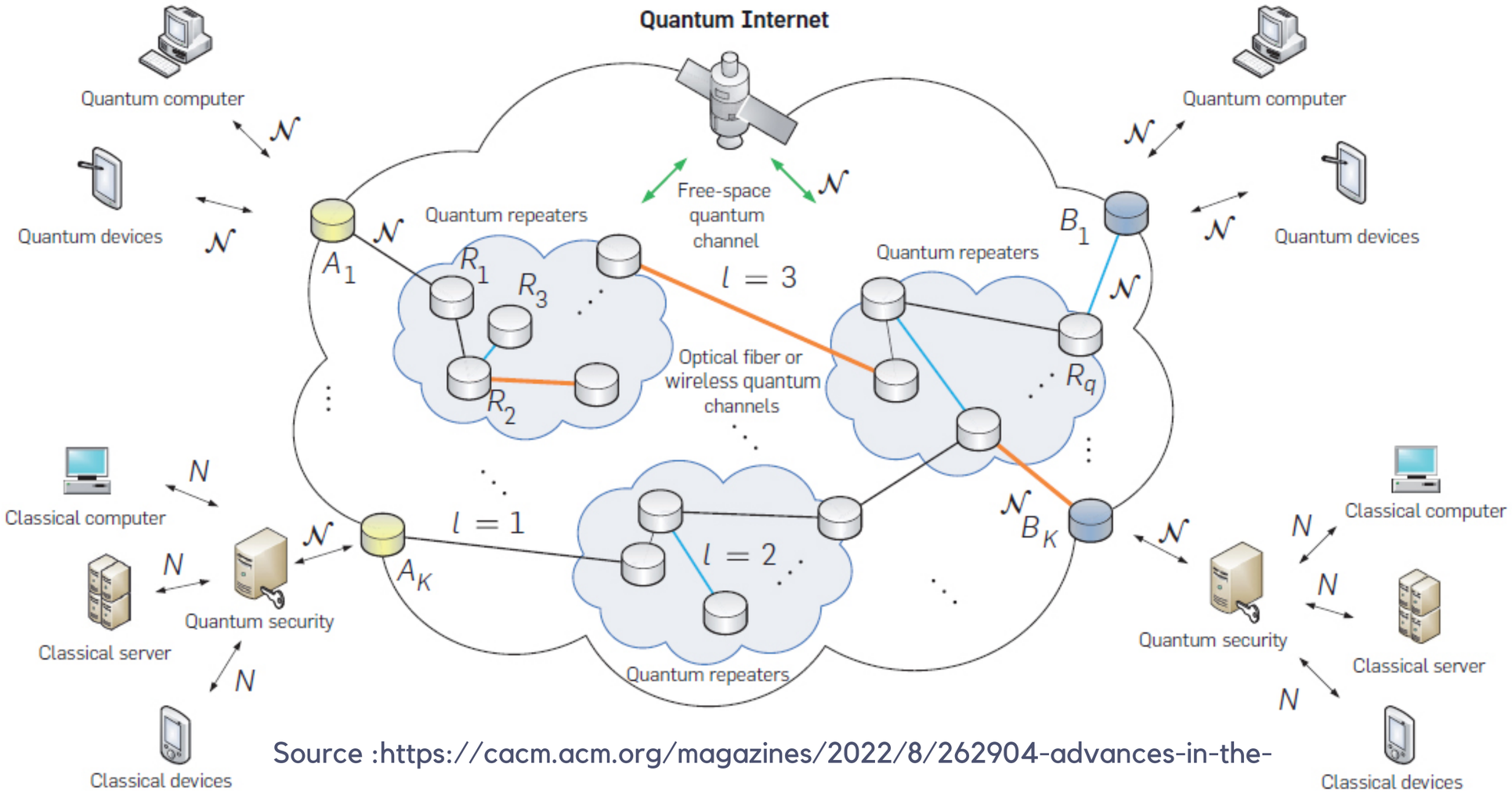
- Consider measurement in X basis
  - Probabilities are |++> = ½, |--> = ½ , |+-> = 0, |-+> = 0
  - If sender measures |+>, the receiver always measure |+>
  - If sender measures |->, the receiver always measure |->
- Consider measurement in Z basis
  - Probabilities are |00> = 0, |11> = 0 , |01> = ½ , |10> = ½
  - If sender measures |0>, the receiver always measure |1>
  - If sender measures |1>, the receiver always measure |0>
  - Results are anti-correlated, so the receiver usually flips to obtain correlated secret.

Quantum Key Distribution - E91

- If sender and receiver share maximally entangled state, they guaranteed security due to monogamy of entanglement.

- Monogamy of entanglement
  - Stronger the entanglement, more secure the secret key is.
  - It is very fundamental property of Quantum states
  - It constrains how correlated multiple qubits can be i.e it guarantees that two entangled states will not have any correlation with a third party
  - Maximally Entangled state = Established key is secure as a third party will never have any information about it.
  - If sender and receiver measure in the same basis, the outcomes are correlated or anti-correlated depending in which basis they are measured.
  - The probability of outcomes is uniformly random.

Quantum Internet



Source :https://cacm.acm.org/magazines/2022/8/262904-advances-in-the-quantum-internet/fulltext

Thank You