Quantum Cryptography

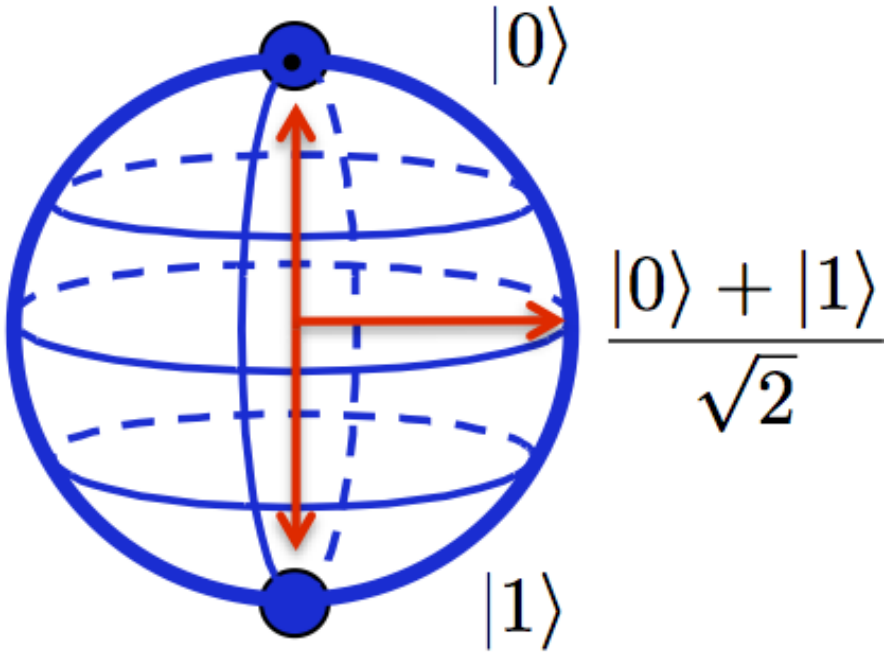
Jordan Klumper, Kimberly Mandery

MATH5347: Cryptography

November 2018

Quantum Computing: Qubit

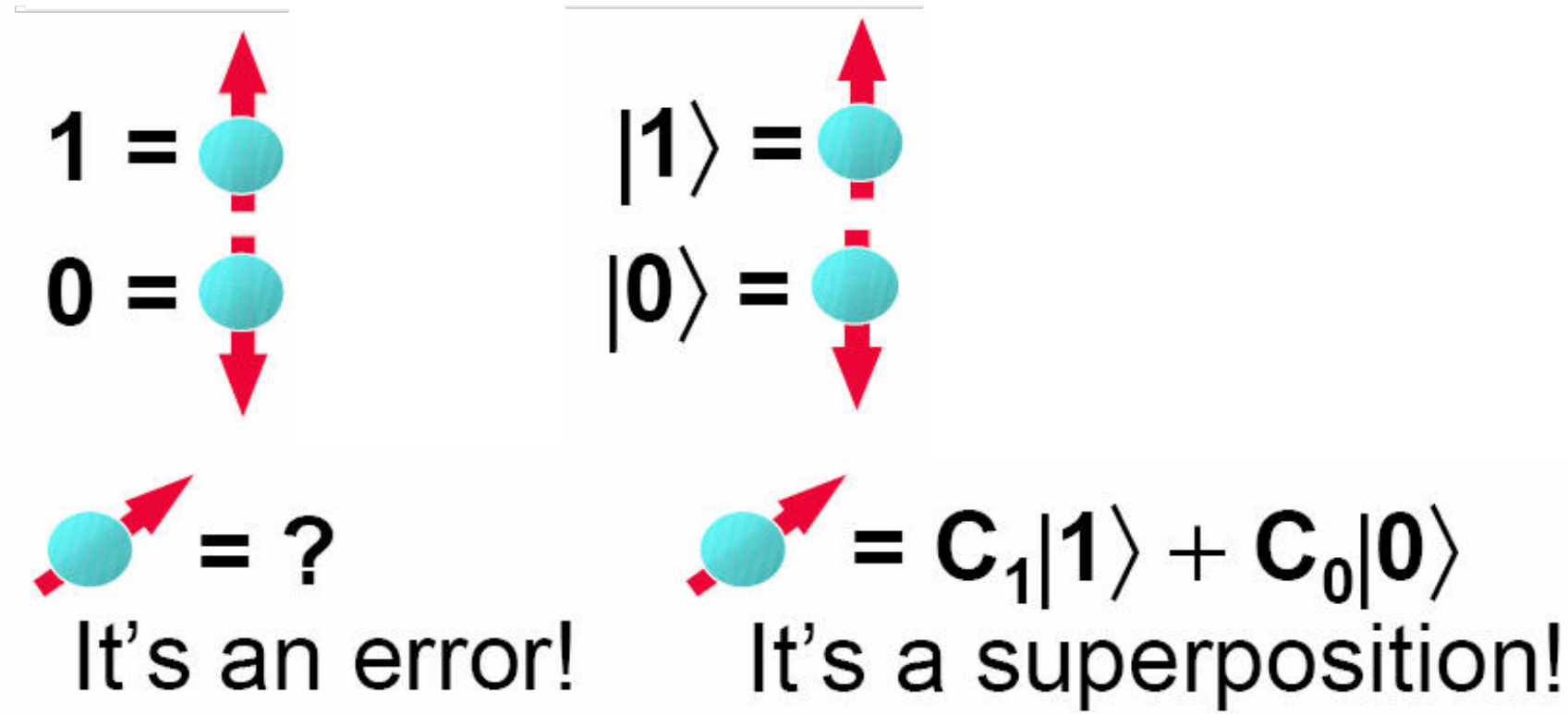
Classical Bit



Qubit

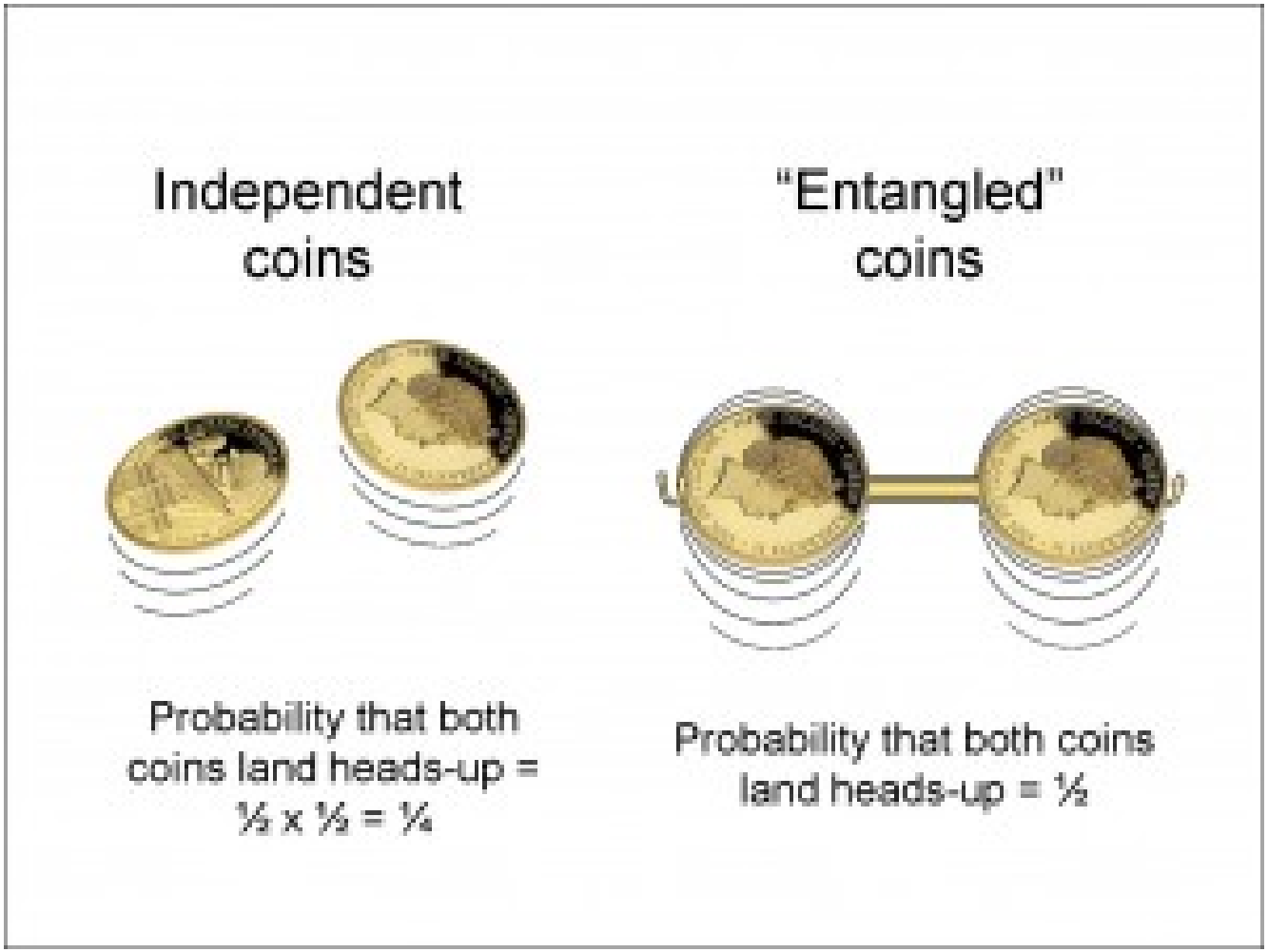
Quantum Computing: Superposition

Classical Bit vs Quantum Bit

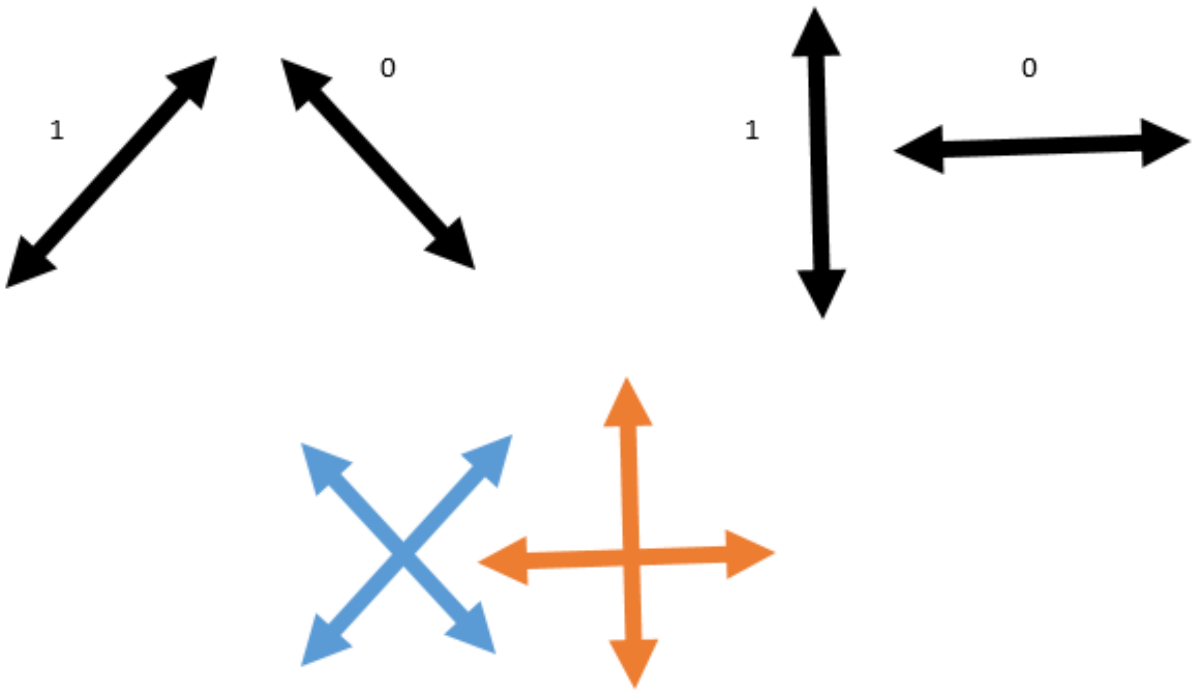


Quantum Computing: Superposition

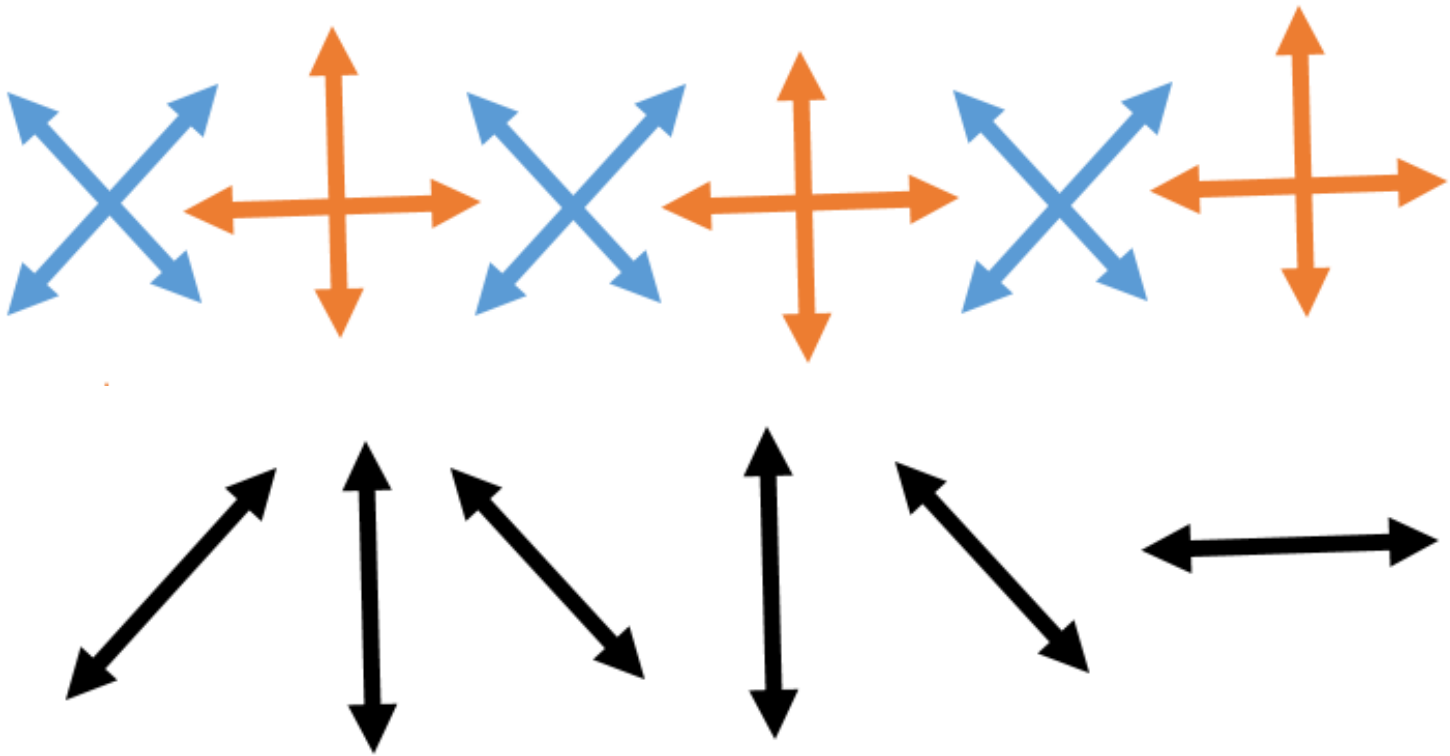
Quantum Computing: Entanglement



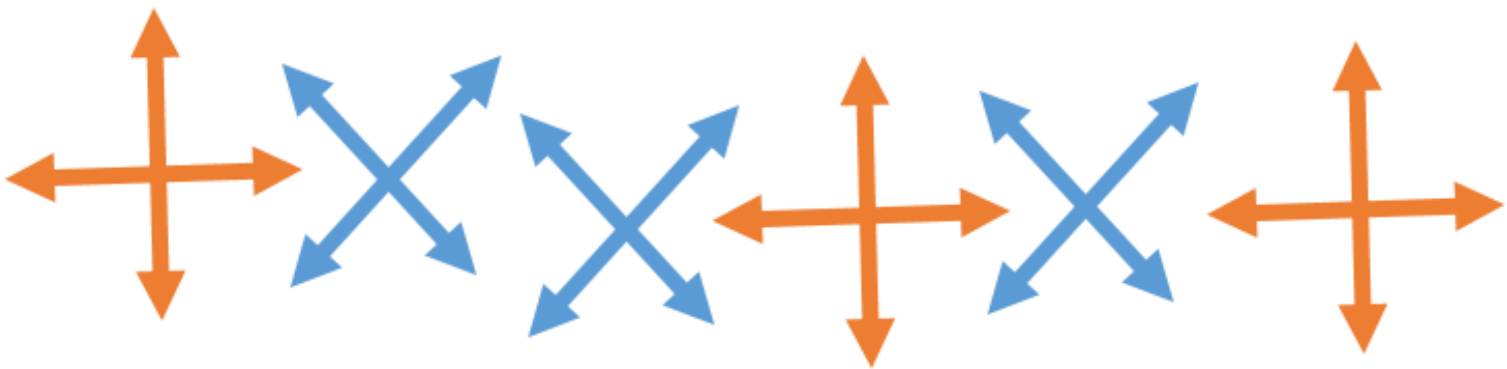
Quantum Key Exchange



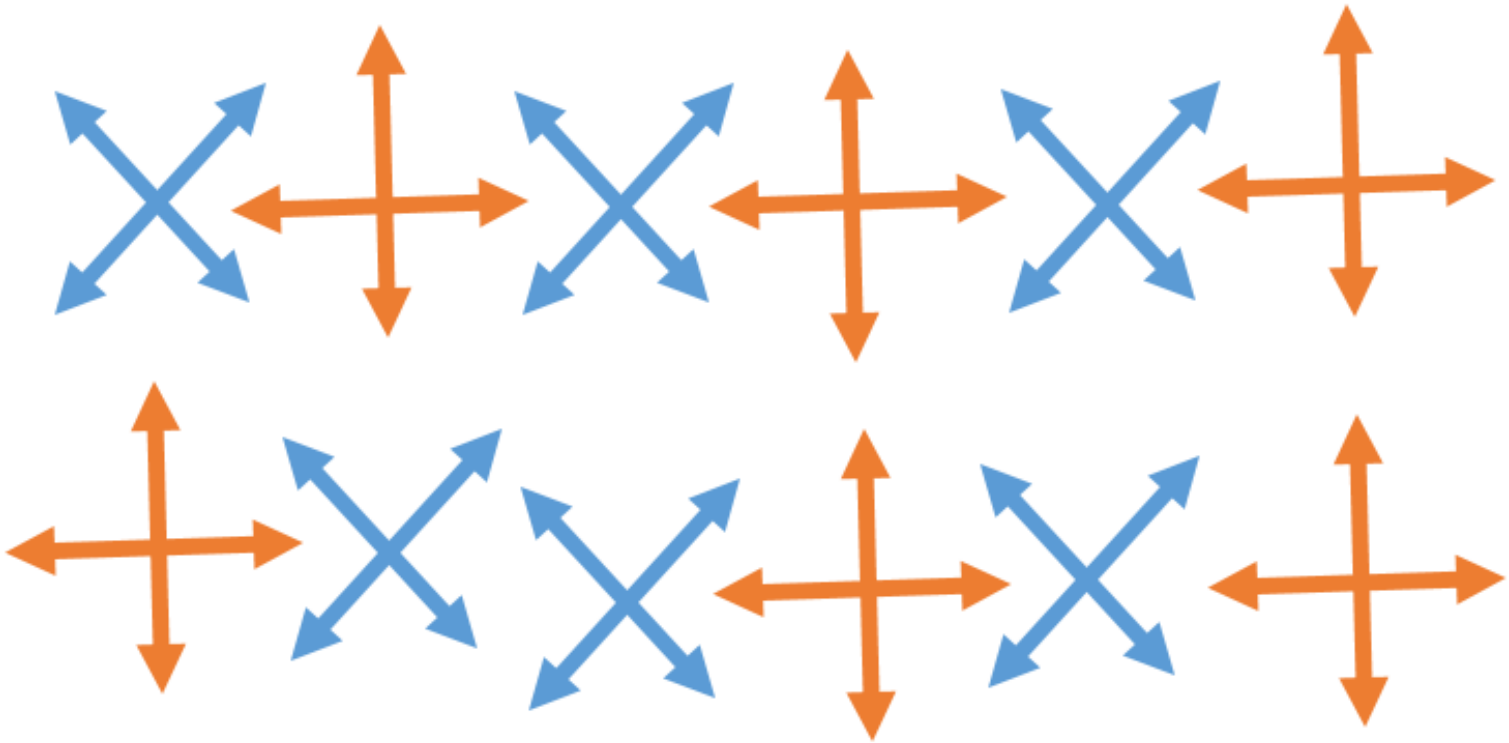
Quantum Key Exchange



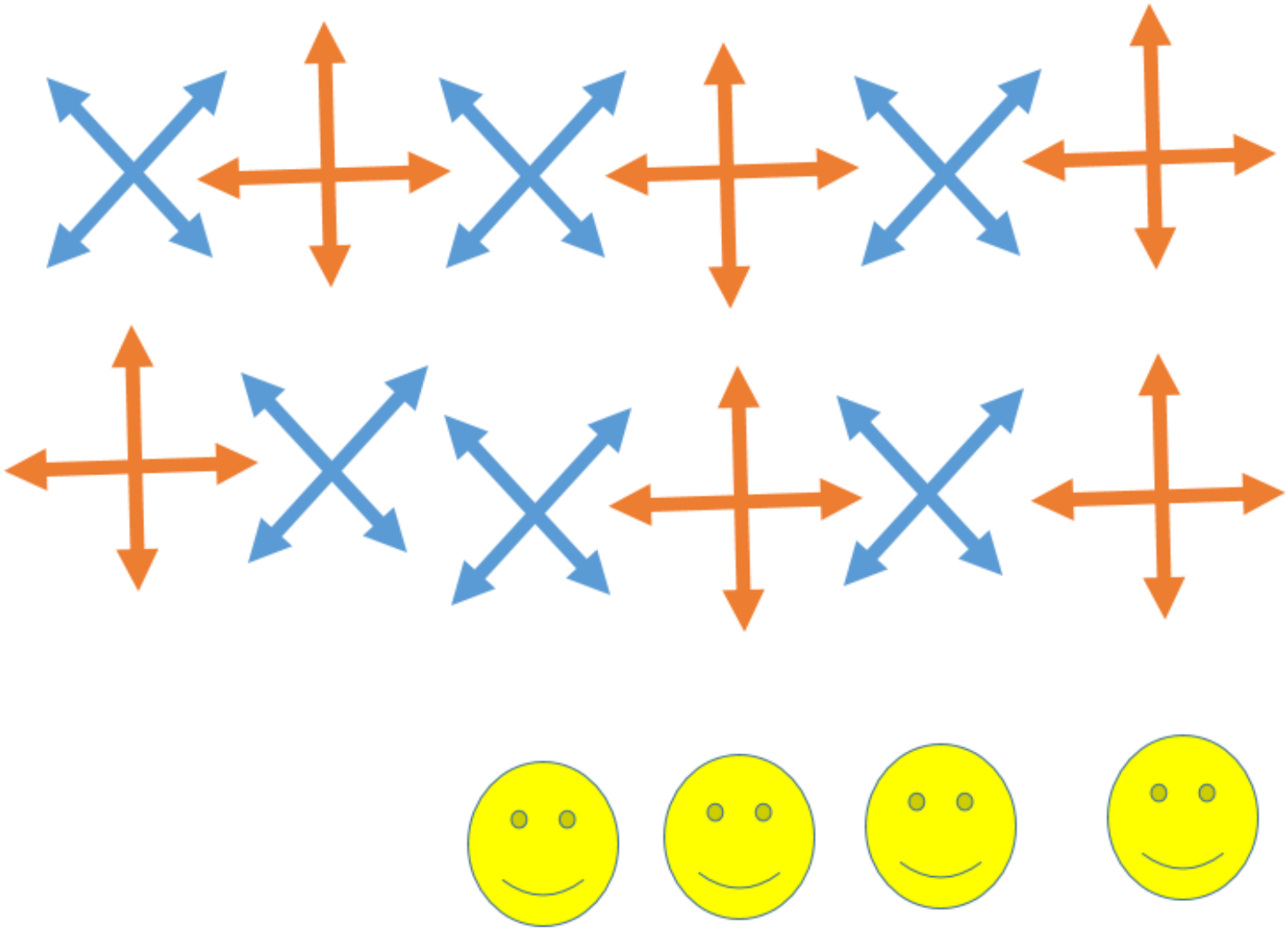
Quantum Key Exchange



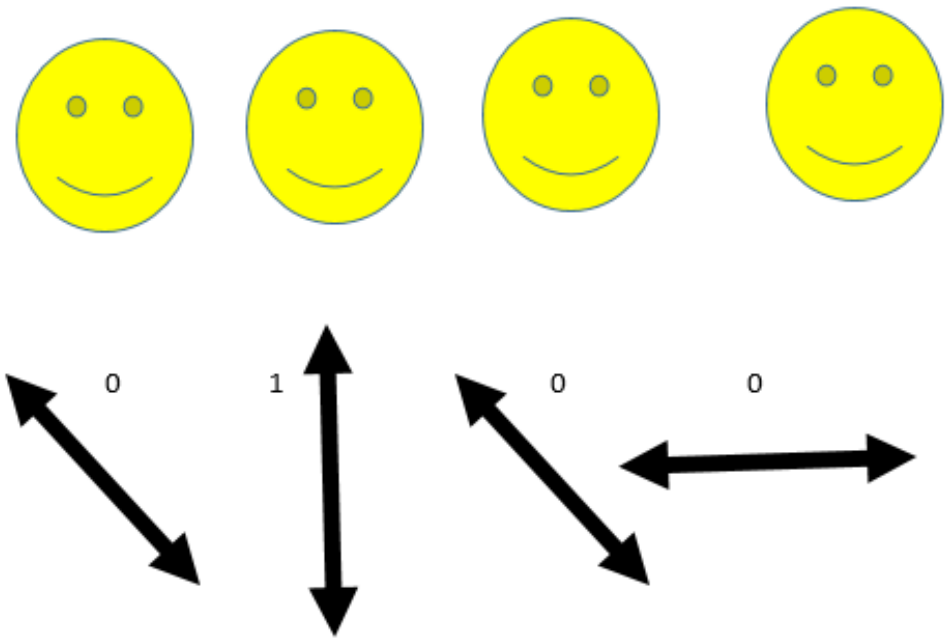
Quantum Key Exchange



Quantum Key Exchange

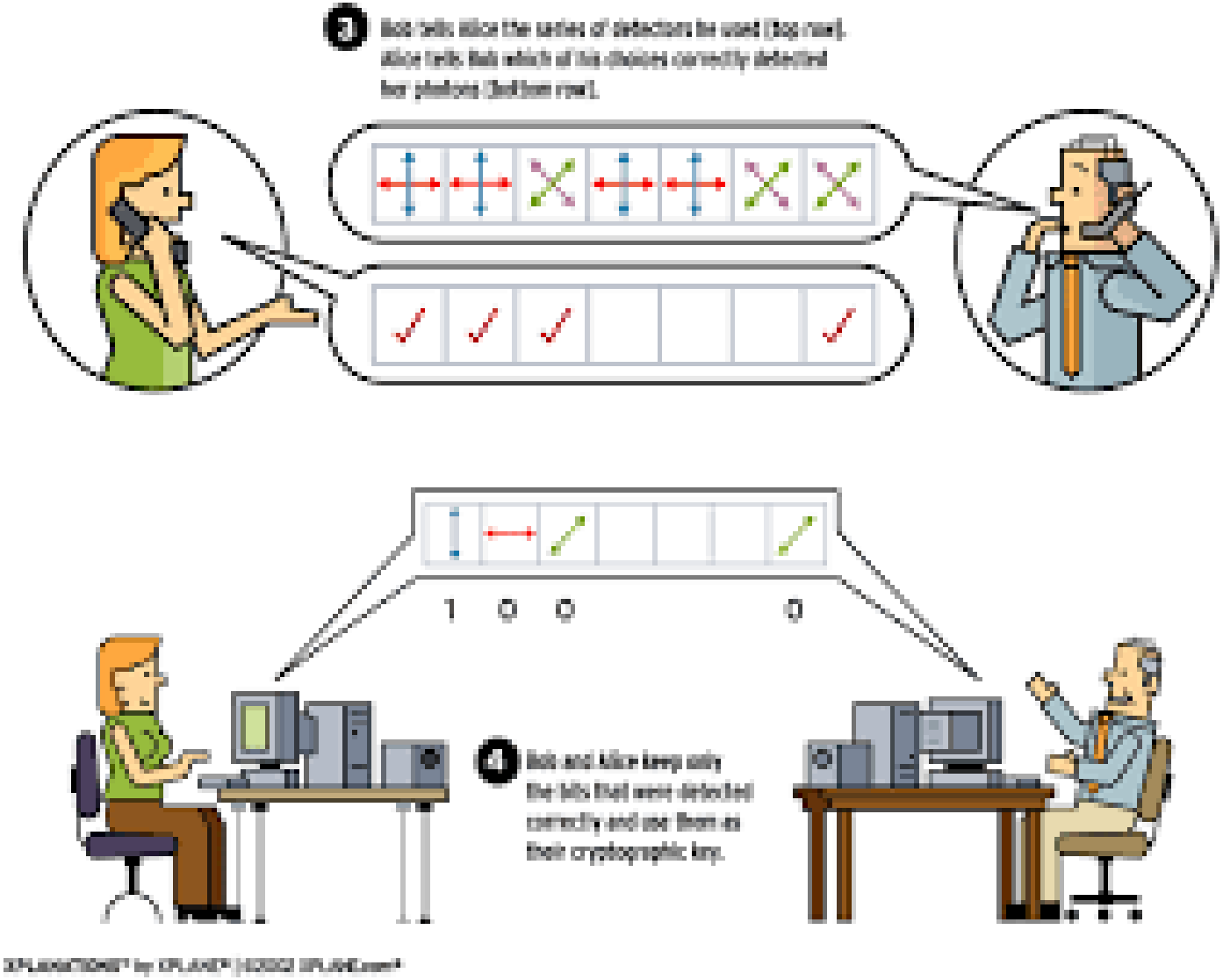


Quantum Key Exchange

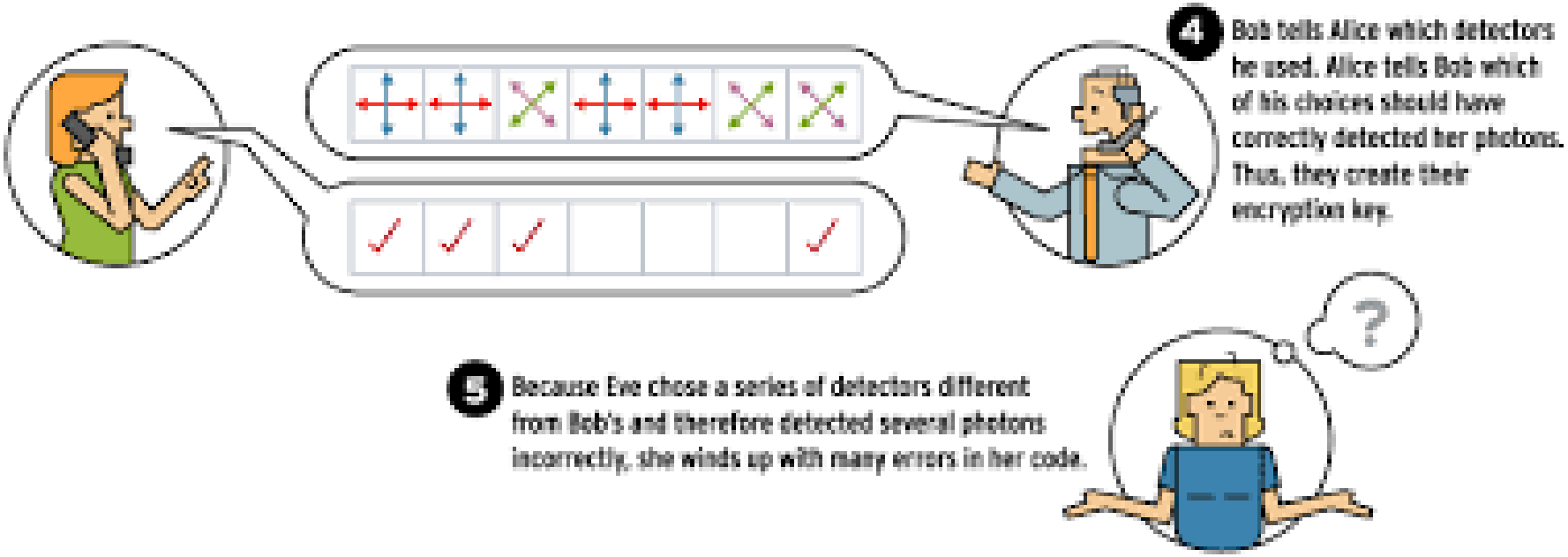


▸ Human Tetris

Quantum Key Exchange



Quantum Key Exchange



Why does this matter in Cryptography?

Most used systems potentially insecure
Shor's Algorithm

Shor's Algorithm

1. Pick a number $a < N$
   where a not a factor of N.

Shor's Algorithm

1. Pick a number $a < N$
   where a not a factor of N.
2. Find r such that a mod N
   where $a^r \equiv 1$ mod N,
   this is called the period or order

Shor's Algorithm

1. Pick a number $a < N$
   where a not a factor of N.
2. Find r such that a mod N
   where $a^r \equiv 1$ mod N,
   this is called the period or order
3. Check: r is even
   and $a^{1/2} + 1 \not\equiv 1$ mod N

Shor's Algorithm

1. Pick a number $a < N$
   where a not a factor of N.
2. Find r such that a mod N
   where $a^r \equiv 1$ mod N,
   this is called the period or order
3. Check: r is even
   and $a^{1/2} + 1 \not\equiv 1$ mod N
4. Then $p = gcd(a^{1/2} - 1, N)$
   and $q = gcd(a^{1/2} + 1, N)$

Shor's Algorithm

1. Quantum Fourier Transform : uses resonances to amplify the basic state associated with the correct period and suppress amplitudes that incorrectly interfere.

Shor's Algorithm

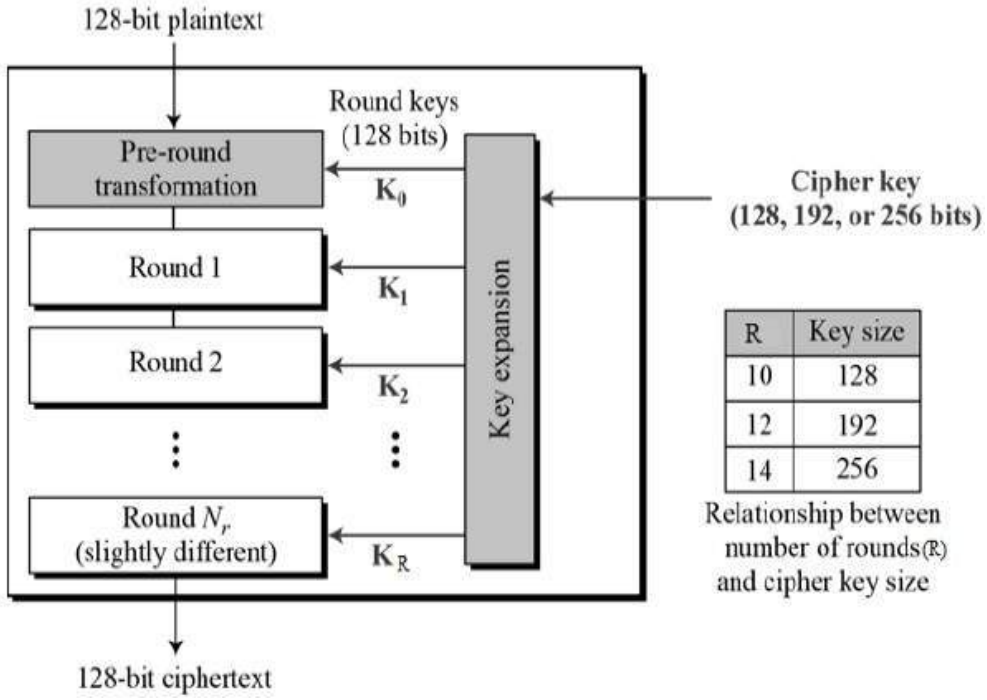
1. Quantum Fourier Transform : uses resonances to amplify the basic state associated with the correct period and suppress amplitudes that incorrectly interfere.
2. Complex Analysis (i.e. complex roots of unity) : can then be used in order to find most probabilistic space.

AES - Advanced Encrypton Standard

What is AES?

A single key (symmetric key) is used in both encrypting and decryption. Messages are split into 128-bit size pieces that are turned into matrices.

Figure: AES Schematic



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

AES

How is it broken?

- Shor's Algorithm is not helpful

AES

How is it broken?

- Shor's Algorithm is not helpful
- Grover's Algorithm (another quantum algorithm) which allows the computation time to break AES to go from $\mathcal{O}(n)$ in classical to $\mathcal{O}(\sqrt{n})$ in quantum computing

AES

How is it broken?

- Shor's Algorithm is not helpful
- Grover's Algorithm (another quantum algorithm) which allows the computation time to break AES to go from $\mathcal{O}(n)$ in classical to $\mathcal{O}(\sqrt{n})$ in quantum computing

How is it made resistant to quantum computing?

- Choose largest keys possible, increases the time it takes.
- Use authentication systems which offers additional layers to the security of the system.

RSA - Rivest-Shamir-Adleman

What is RSA?

An asymmetrical cryptosystem that utilizes the discrete logarithm problem, that is it's difficult to factor the product of two very large primes

1. Choose two large similar sized primes p and q.
2. Find $n = p \cdot q$ which is our modulus
3. Find $\phi(n) = \phi(p) \cdot \phi(q) = (p-1)(q-1)$
4. Given e, the encryption key, find d where $d \equiv e^{-1} \pmod{\phi(n)}$
5. We now have our public key: (n, e) and our private key: (d, p, q)

How is it broken?

RSA

How is it broken?

- Given our public key: (n, e), Shor's algorithm allows us to find p and q

RSA

How is it broken?

- Given our public key: (n, e), Shor's algorithm allows us to find p and q
- With p and q we can readily find d using step 4 on the previous slide now that $\phi(n)$ is easily computed

How is it made resistant to quantum computing?

RSA

How is it broken?

- Given our public key: (n, e), Shor's algorithm allows us to find p and q
- With p and q we can readily find d using step 4 on the previous slide now that $\phi(n)$ is easily computed

How is it made resistant to quantum computing?

- As of right now there aren't any widely accepted ways to improve RSA

RSA

How is it broken?

- Given our public key: (n, e), Shor's algorithm allows us to find p and q
- With p and q we can readily find d using step 4 on the previous slide now that $\phi(n)$ is easily computed

How is it made resistant to quantum computing?

- As of right now there aren't any widely accepted ways to improve RSA
- XMSS (Extended Merkle Signature Scheme) has been suggested as a replacement as it's resistant to quantum algorithms.

RSA

How is it broken?

- Given our public key: (n, e), Shor's algorithm allows us to find p and q
- With p and q we can readily find d using step 4 on the previous slide now that $\phi(n)$ is easily computed

How is it made resistant to quantum computing?

- As of right now there aren't any widely accepted ways to improve RSA
- XMSS (Extended Merkle Signature Scheme) has been suggested as a replacement as it's resistant to quantum algorithms.
- Rather than a discrete logarithm problem, XMSS uses a hash-based function for security, these are considered quantum resistant

ECC - Elliptical Curve Cryptography

What is ECC?

A cryptosystem that uses an algebraic structure created by points on an elliptic curve over a finite field. It's another system based on the discrete logarithm problem.

Elliptic curve form: $Y^2 = X^3 + AX + B$ where $4A^3 + 27B^2 \neq 0$

Discrete logarithm problem: Give points P and Q find n such that

$$Q = nP$$

How is it broken?

ECC

How is it broken?

- Similar to RSA, Shor's algorithm can be used to find n and allowing an eavesdropper to determine the private key

ECC

How is it broken?

- Similar to RSA, Shor's algorithm can be used to find n and allowing an eavesdropper to determine the private key

How is it made resistant to quantum computing?

ECC

How is it broken?

- Similar to RSA, Shor's algorithm can be used to find n and allowing an eavesdropper to determine the private key

How is it made resistant to quantum computing?

- Supersingular Isogeny Key Exchange is a direct improvement to ECC

ECC

How is it broken?

- Similar to RSA, Shor's algorithm can be used to find n and allowing an eavesdropper to determine the private key

How is it made resistant to quantum computing?

- Supersingular Isogeny Key Exchange is a direct improvement to ECC

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}$$

ECC

How is it broken?

- Similar to RSA, Shor's algorithm can be used to find n and allowing an eavesdropper to determine the private key

How is it made resistant to quantum computing?

- Supersingular Isogeny Key Exchange is a direct improvement to ECC

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}$$

- If the j-invariant of two curves is the same, they are isomorphic over the same field.

ECC

How is it broken?

- Similar to RSA, Shor's algorithm can be used to find n and allowing an eavesdropper to determine the private key

How is it made resistant to quantum computing?

- Supersingular Isogeny Key Exchange is a direct improvement to ECC

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}$$

- If the j-invariant of two curves is the same, they are isomorphic over the same field.

Alice finds $\phi_A(E)$ sends it to Bob who finds $\phi_B(E_A)$ which is E_{AB}
Now Bob has E_{AB}, similar to above Alice ends up with E_{BA}
$E_{AB} \cong E_{BA}$

When will this occur?

When will this occur?

- As of 2018 Google has created a 72-qubit quantum chip, the largest yet.

When will this occur?

- As of 2018 Google has created a 72-qubit quantum chip, the largest yet.
- To even begin writing software on quantum computers, hundreds to thousands of qubits would be needed.

When will this occur?

- As of 2018 Google has created a 72-qubit quantum chip, the largest yet.
- To even begin writing software on quantum computers, hundreds to thousands of qubits would be needed.
- To run Shor's algorithm on a 2,000-bit number a quantum computer is estimated to require 130 million cubits.

When will this occur?

- As of 2018 Google has created a 72-qubit quantum chip, the largest yet.
- To even begin writing software on quantum computers, hundreds to thousands of qubits would be needed.
- To run Shor's algorithm on a 2,000-bit number a quantum computer is estimated to require 130 million cubits.
- For quantum cryptography, estimates say we are 10 to 20 years away, but estimates vary widely.

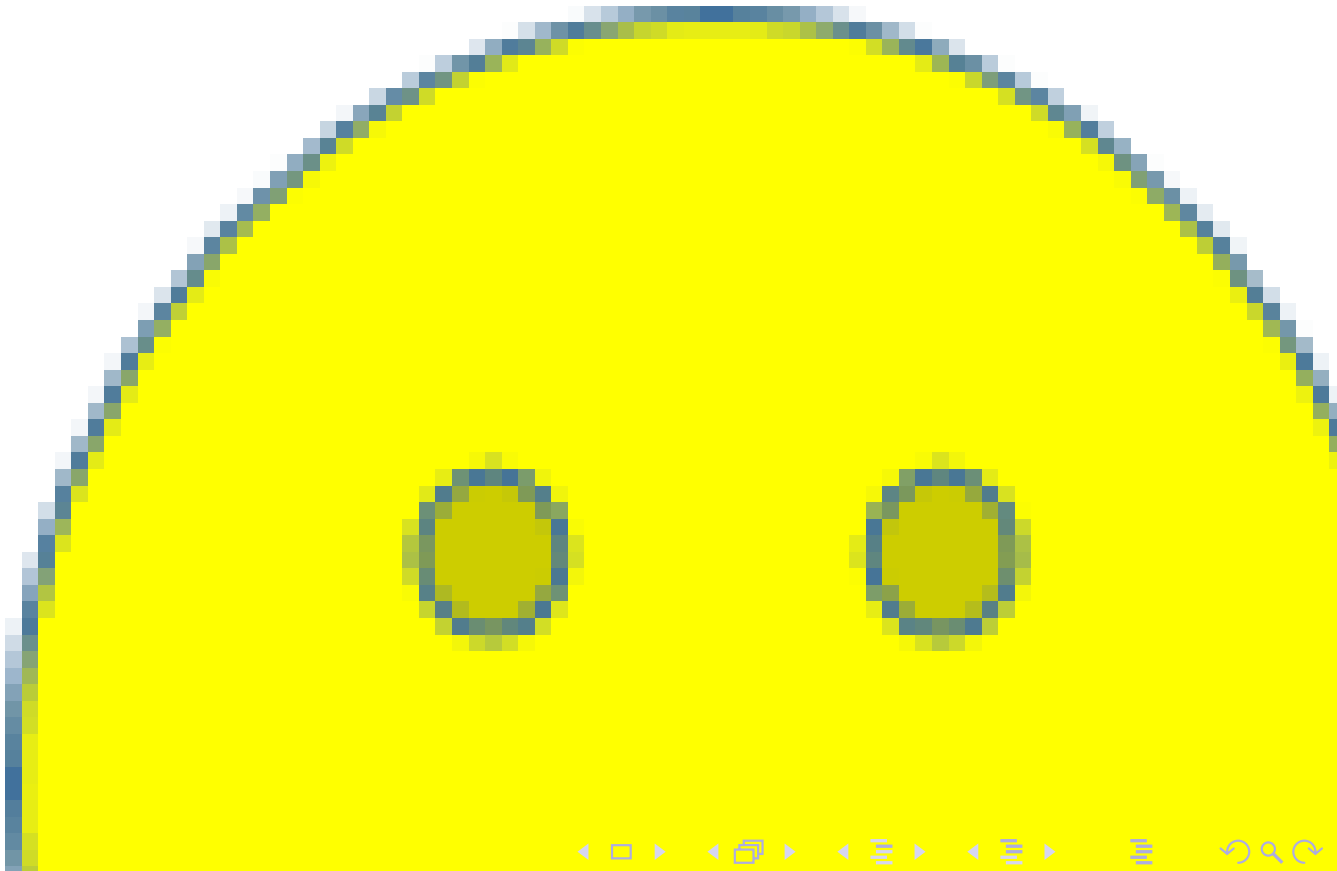
Thanks

Thanks

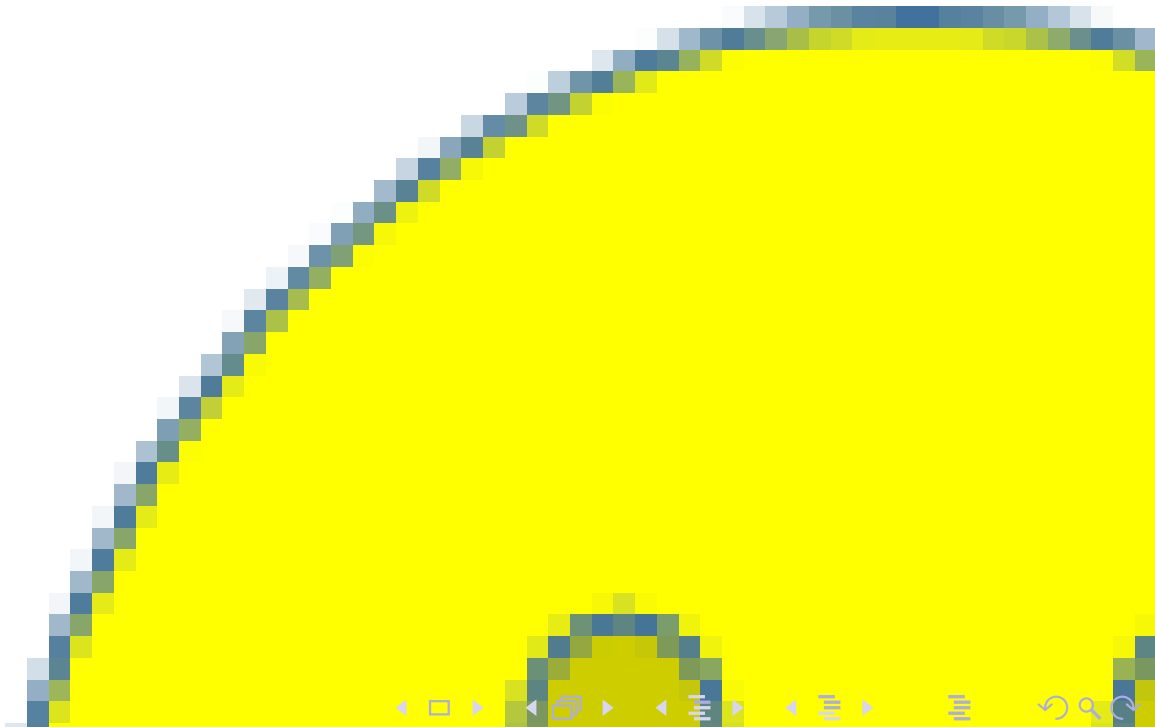
Thanks

Thanks

Thanks



Thanks



Resources


Visualizing 2-Qubit Entanglement
http://algassert.com/post/1716


Quantum Theory
https://whatis.techtarget.com/definition/quantum-theory


Quantum Error Correction
https://en.wikipedia.org/wiki/quantum-error-correction


Richard Feynman Talks
https://en.wikiquote.org/wiki/Talk:Richard$_F$*eynman*


Superposition Double-Slit Paradox
https://phys.org/news/2014-10-superposition-revisited-resolution-double-slit-paradox.html


Alice and Bob Lab Example
https://ieeexplore.ieee.org

Resources


Complexity of Classical vs Shor's Algorithm
https://quantumexperience.ng.bluemix.net/proxy/tutorial/full-user-guide/004-Quantum_Algorithms/110-Shor%27s_algorithm.html


Jeffrey Hoffstein, Jill Pipher, J.H. Silverman *An Introduction to Mathematical Cryptography* 2008: Springer-Verlag New York


How secure is today's encryption against quantum computers?
https://betanews.com/2017/10/13/current-encryption-vs-quant


Advanced Encryption Standard
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard


Grover's Algorithm
https://en.wikipedia.org/wiki/Grover%27s_algorithm


Hash-based cryptography
https://en.wikipedia.org/wiki/Hash-based_cryptography

Resources

Quantum Computing Lecture
https://people.eecs.berkeley.edu/ luca/quantum/lecture02.pd

Advanced Encryption Standard
https://www.tutorialspoint.com/cryptography/advanced_encryption_stand

Kerberos (protocol)
https://en.wikipedia.org/wiki/Kerberos_(protocol)

Overview of History of Elliptic Curves and its use in cryptography
https://www.ijser.org/researchpaper/Overview-of-History-of-Elliptic-Curves-and-its-use-in-cryptography.pdf

The 256-bit AES Resists Quantum Attacks
https://www.researchgate.net/publication/316284124_The_AES-256_Cryptosystem_Resists_Quantum_
Attacks

RSA (cryptosystem)
https://en.wikipedia.org/wiki/RSA_(cryptosystem)

Questions?