: Djordjevic, I.B.

Physical-Layer Security, Quantum

Key Distribution, and Post-Quantum

Cryptography. Entropy 2022, 24, 935.

<https://doi.org/10.3390/e24070935>

-Idea that Eve is omnipotent and only limited by laws of physics is unreasonable, there are many ways to detect an eavesdropper in geometric space. This greatly increases the secret key rate

-Build a global quantum communication network by using LEO satellite QCM to connect existing terrestrial quantum networks, thus providing security for 5g+, internet of things, optical networks, and autonomous vehicles

-Underwater quantum key distribution

International Journal of Theoretical Physics (2021) 60:3744–3759

https://doi.org/10.1007/s10773-021-04865-2

n-Bit Quantum Secret Sharing Protocol Using Quantum

Secure Direct Communication

Mohammad Sadegh Sadeghi-Zadeh1 & Mahsa Khorrampanah2 &

Monireh Houshmand1 & Hossein Aghababa 3 & Yousef Mafi3

09-02-2021

-Propose sending n-bit message to m receivers

-Alice sending

-Bob 1, Bob2, Bob 3, …, Bob m receivers

-Eve eavesdropper

-Bobs must collaborate with each other to decrypt message

-Alice only communicates with Bobs through Quantum channel

-Bobs only communicate with each other through secured classical channel

-n=m

-Alice keeps the first n qubits

-Alice sends each Bob a qubit

-Alice sends 0’s as 0 value qubits

-Alice sends 1’s as 1 value qubits

-Alice CNOTs the qubits

-Alice sends the qubits randomly to the Bobs

-Bobs measure the state of the qubits

-Alice shares table over classic channel of which Bob received which random bit

-Bobs communicate the appropriate bit to the appropriate Bob based on Alice’s table

<https://quantum-computing.ibm.com/composer/docs/iqx/guide/>

Charlie Bennett, Lev Bishop, Sergey Bravyi, Andrew Cross, Jay Gambetta, Paul Nation, John Smolin, Kristan Temme, Abby Cross (editor)

-Classical Computer uses bits 0 or 1, so an n bit computer can have 2n states from 00…0 to 11…1

-Through a special type of superposition, a quantum computer can have exponentially many states at once from |00…0> to |11…1> of its quantum bits, called qubits

-Entangled states are states of the whole computer that do not assign to a digital or analog assignment of the individual qubits

-Quantum Physics are confusing due to 2 counterintuitive statements:

1. A Physical System in a **Definite** state can still behave **Randomly**

2. Two systems that are too far apart to influence each other can behave in ways that, while individually random, are somehow strongly correlated

-States of qubits can be written as |0> = (10) and |1> = (01)

-The simples quantum gates are 2x2 unitary matrices, for example (0110) = X is the not gate that maps |0> to |1> and |1> to |0>

-In simplest terms, a superposition is a linear combination

-The Hadamard Gate [ 1/√(2) (111-1)] can demonstrate the first counterintuitive statement. Experimentally, H|0> = |0> half the time, and = |1> the other half. The same applies for H|1>. We will call these states |+> and |->, respectively. Based on classical probability, the expectation is that a second application of the H gate will yield the same variable results, but it does not! H(H|0>) always equals |0>. The interference caused by the negative causes this behavior. Writing it out, |+> = 1/√(2) (|0> + |1>), while |-> = 1/√(2) (|0> - |1>)

-The Born rule states that for |Ψ> = α|0> + ß|1>, P(0) = |α|2 and P(1) = |ß|2 for α, ß ∈ ℂ

-Based on the rules of classical probability, |α|2 + |ß|2 = 1, so we can rewrite |Ψ> as √(1-p)|0> + eφγp|1> where 0 ≤ p ≤ 1 is the probability of |1>, 0 ≤ φ < 2π is the quantum phase, and γ is any number in [0, 2π)

7. Shor's Algorithm I: Understanding Quantum Fourier Transform, Quantum Phase Estimation - Part 1

Sep 1, 2020

Lecturer: Abraham Asfaw

Lecture Notes and Labs: <https://qiskit.org/learn/intro-qc-qh>

<https://www.youtube.com/watch?v=mAHC1dWKNYE>

-First consider Shor’s algorithm as a solution to finding the periodicity of a function

-ie f(x) = f(y) for x≠y iff |x-y| = kp for all x,y

-Classical time: exp(cN1/3log(N)2/3) : VERY SLOW

-n2log(n)log(log(n)) slightly faster than O(n3), but an exponential speedup

-Works due to quantum fourier transform and modular exponentiation

-converts from factoring problem to periodicity problem

-not accessible because several qubits are required, and getting good ones is hard

-Shor’s algorithm is quantum phase estimation in disguise

-**Quantum Fourier Transform**

-change of basis from computational basis to fourier basis

-1 qubit computational basis: {|0>, |1>}

-1 qubit fourier basis: {|+>, |->}









-This QFT is Hadamard Gate

https://www.youtube.com/watch?v=pq2jkfJlLmY

-n qubits

--1 qubit {0, 1} basis states

--2 qubits {00, 01, 10, 11} basis states

--n qubits have 2n basis states

-N = 2n

-|x~> is QFT of |x> = [1/√(N)]Σy=0N-1 exp([2πixy]/N)|y>

EX: 1 qubit

N=2

QFT|x> = 1/√2 Σexp(2π1xy/2)|y>

Circuit to implement QFT:

-each qubit went from |xk> to

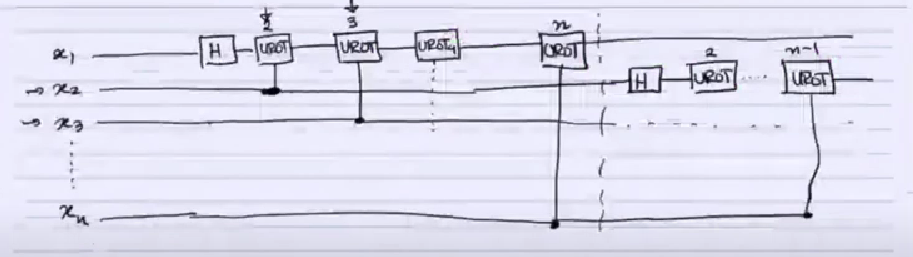
-Hadamard gates applied to |xk>

--H|xk> =

-Unitary-Rotation Gate

--UROTk|xj> =

=

-The Circuit

x1

UROT2

UROT2

UROT2

H

x2

UROT2

x3

…

xn

<https://www.youtube.com/watch?v=5kcoaanYyZw>

Quantum Phase Estimation:

-using QFT to do something useful

-Unitary Matrix has eigenvalues of form eiΘ and eigenvectors form orthogonal basis

<https://www.youtube.com/watch?v=YpcT8u2a2jc>

Diagram, schematic

Description automatically generated

<https://learn.qiskit.org/summer-school/2020/shors-algorithm-i-fourier-transform-phase-estimation>

<https://www.youtube.com/watch?v=dscRoTBPeso>