Foundation & Challenges of Quantum Computing

Debajyoti Bera
IIIT-Delhi
www.iiitd.ac.in

Random Bits

Classical randomized algorithms use classical coins (random bits).

Classical randomized algorithms are efficient

Quicksort, Monte-Carlo simulation, sampling, …

Satisfiability of 3SAT Boolean formula

Brute force $O(2^n)$

Deterministic $O(1.439^n)$

Randomized $O(1.321^n)$

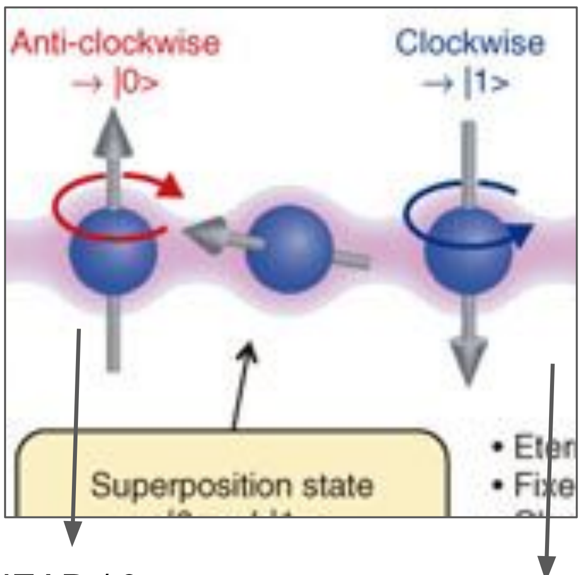
Remote verification of equality of bit strings

Brute force $O(n)$

Randomized $O(\log n)$

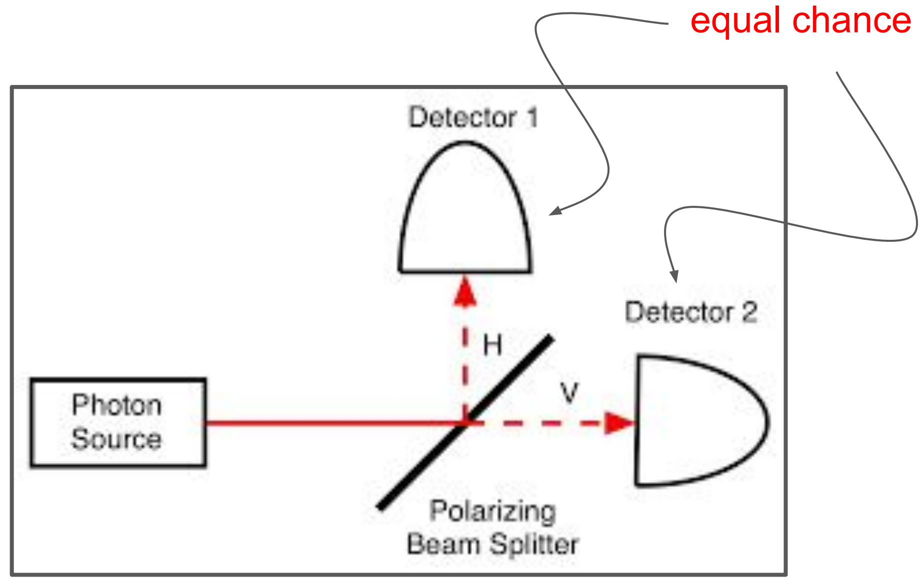
Qubits

Photon polarization, Electron spin,
direction of current in Joesphon junction, ...



HEAD / 0

TAIL / 1

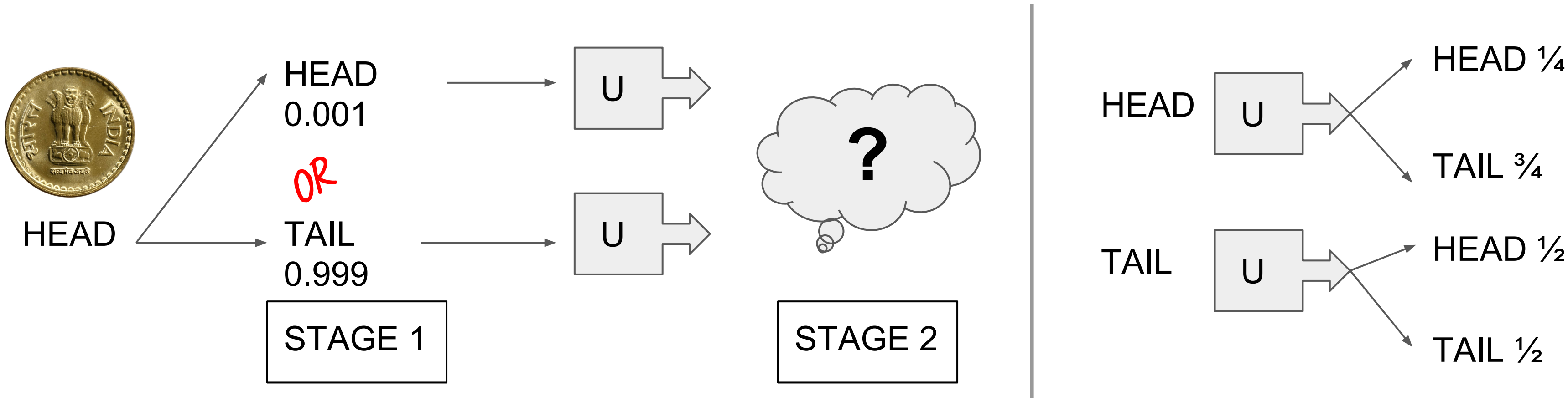


Quantum operations are inherently probabilistic.

Quantum ≈ Randomized +++++

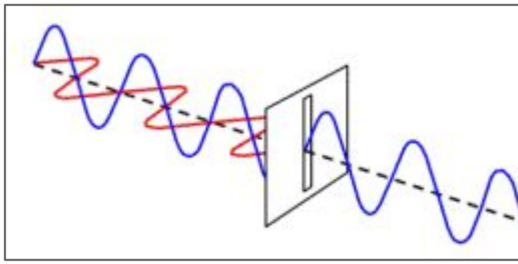
(different rules of randomization)

Probabilities of Classical states



Probability of HEAD in stage 2	
Stage 1 can be HEAD w/p .001	[OR] Stage 1 can be TAIL w/p 0.999
Prob. of HEAD = ¼	Prob. of HEAD = ½
Final prob. = (0.001 x ¼) + (0.999 x ½)	

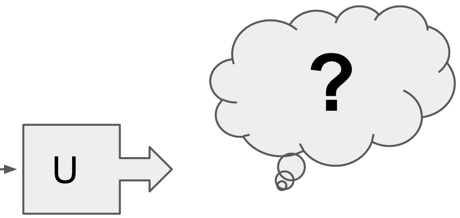
Probabilities of Quantum states



Horizontal polarised photon

HOR
0.001
AND
VER
0.999

STAGE 1



STAGE 2

superposition

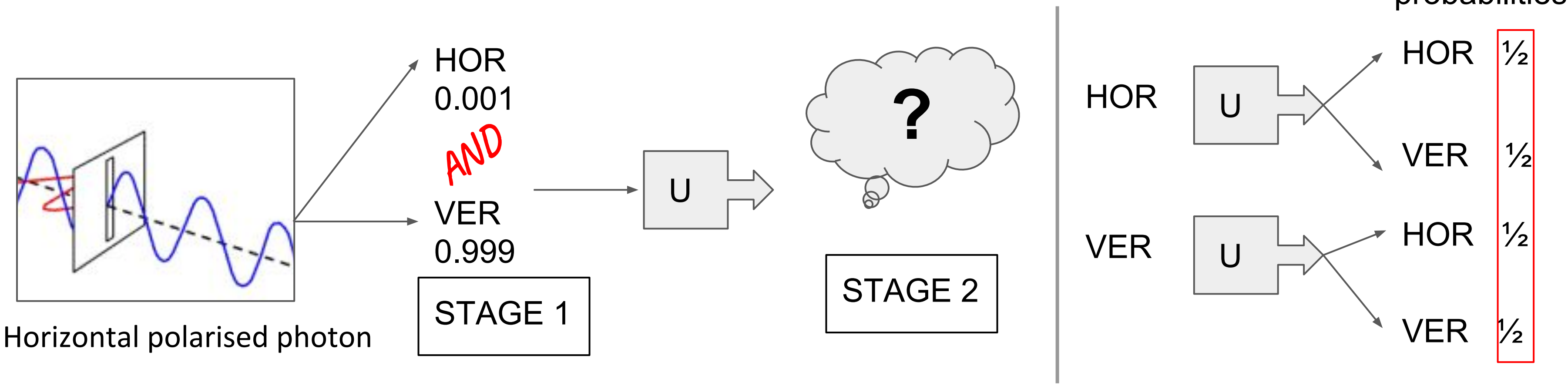
Stage-1
HOR
VER

AND

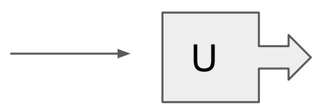
HOR
0.001
OR
VER
0.999

collapse under measurement

Probabilities of Quantum states

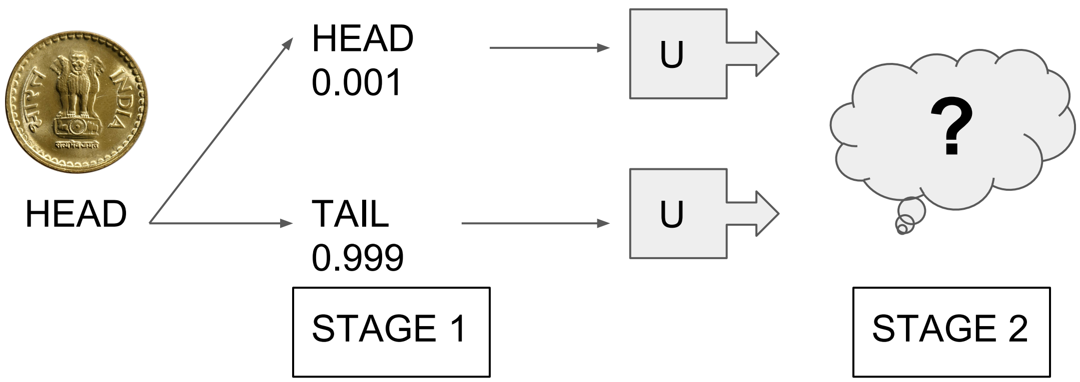


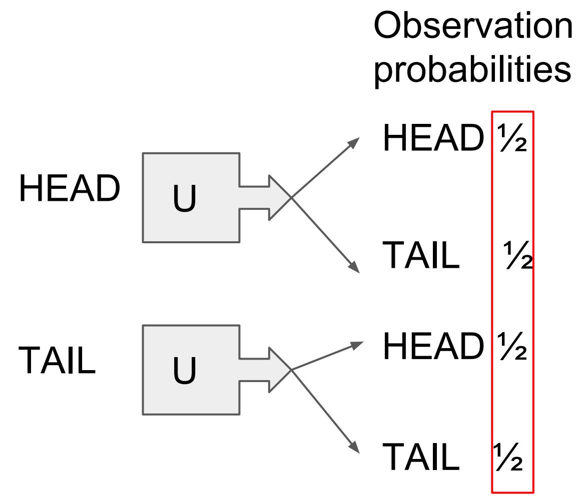
Stage-1
HOR
AND VER

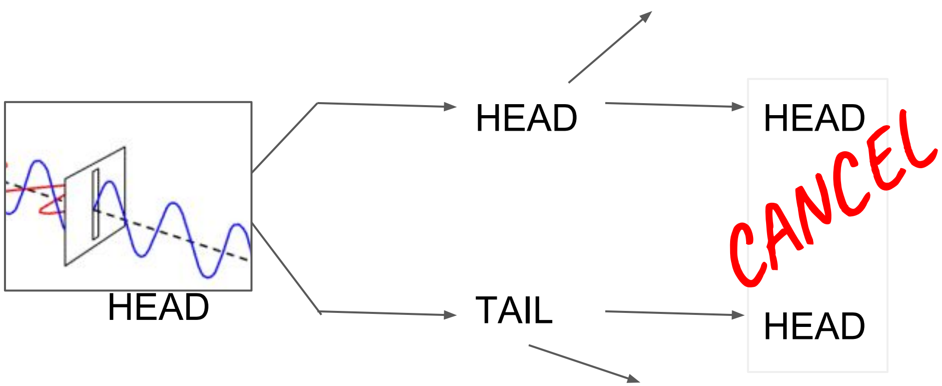


Probability of HOR in stage 2
~~Prob. of HOR from H in stage-1 + Prob. of HOR from V in stage-1~~

Evolution of Quantum states







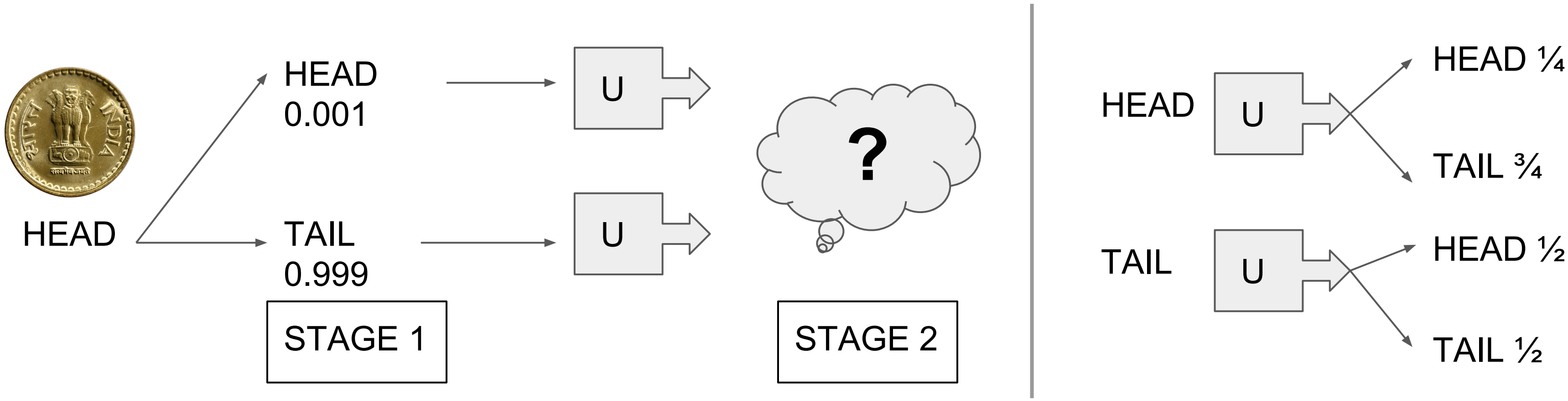
Destructive interference

U could be designed *s.t.* prob. of HEAD is **ZERO** in Stage-2

Classical : State is a unit L1-norm real vector, U is stochastic

Quantum: State is a unit L2-norm complex vector, U is unitary

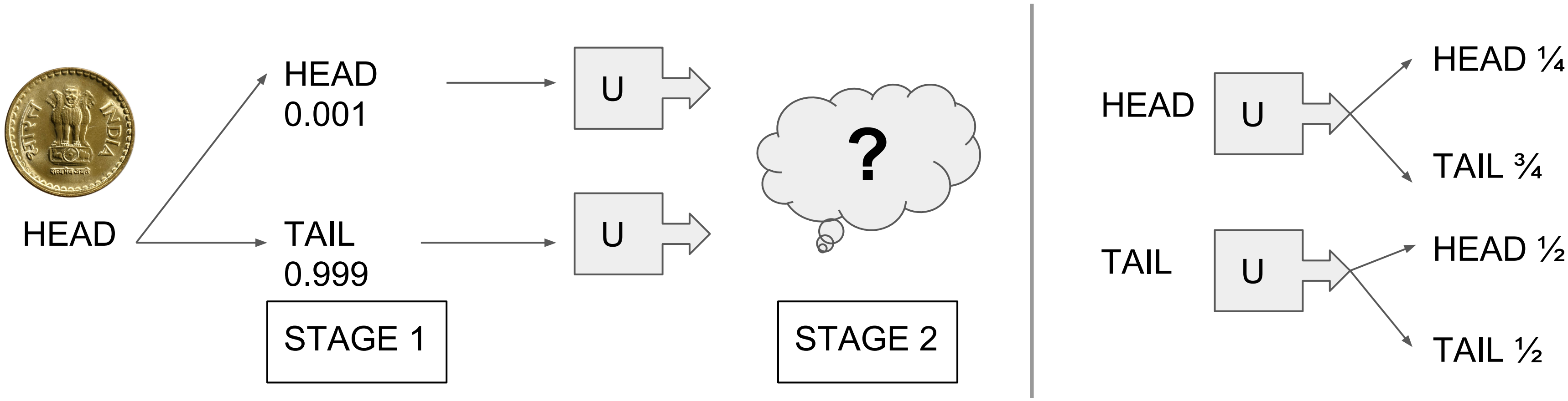
Evolution of Classical states



$$\begin{pmatrix} 0.001 \\ 0.999 \end{pmatrix} = 0.001 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 0.999 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

State vector @ stage-1 HEAD TAIL

Evolution of states



$$\begin{pmatrix} .499.. \\ .500.. \end{pmatrix} = \begin{pmatrix} \frac{1}{4} & \frac{1}{2} \\ \frac{3}{4} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} .001 \\ .999 \end{pmatrix}$$

$$\begin{pmatrix} \frac{1}{4} & \frac{1}{2} \\ \frac{3}{4} & \frac{1}{2} \end{pmatrix}$$

State vector @ stage-2

State vector @ stage-1

Operation U

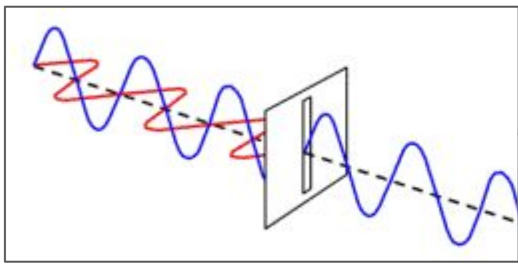
Classical : State is a unit L1-norm real vector, U is stochastic

Quantum: State is a unit L2-norm complex vector, U is unitary

Quantum Searching in Database

A[1]	A[2]	A[3]	A[4]
0	0	1	0

Task: Find some x *s.t.* A[x] = 1.
Any A[j] can be queried.
Efficiency measure : no. of queries.



Quantum possibilities : **AND** of			
i=1	i=2	i=3	i=4

Query A[i]

Quantum possibilities : **AND** of			
A[1]=0	A[2]=0	A[3]=1	A[4]=0

Measure

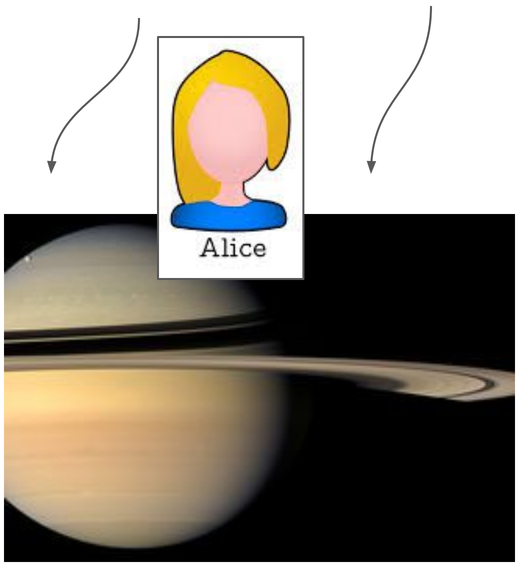
Get A[3]=1 with prob. ¼

Grover's amplitude amplification

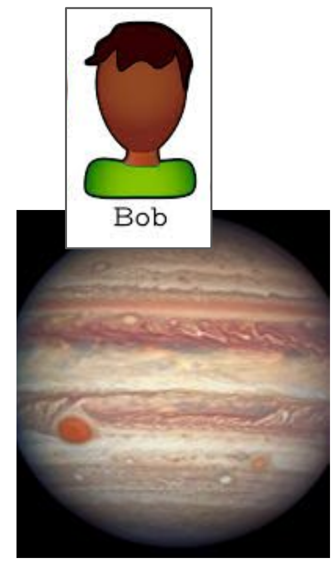
Always ...
A[3]=1
Other possibilities cancel each-other

Secret Key Distribution

Two coins.
HH or TT with equal probability.



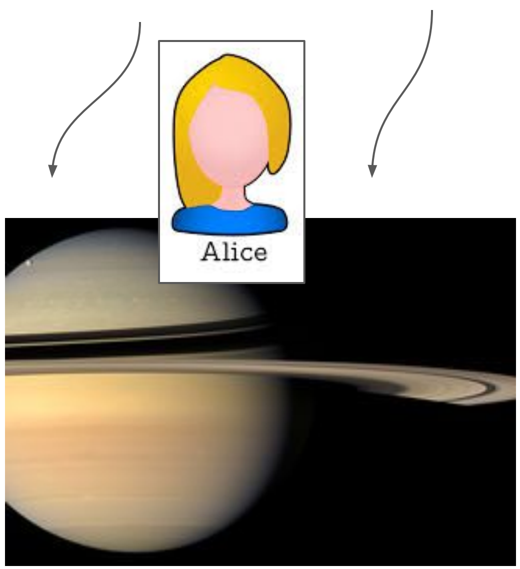
Alice throws one coin to Bob



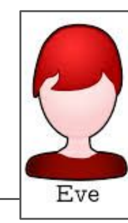
1. Alice checks her coin.
2. Bob checks his coin.
3. Alice and Bob share a random bit.
4. This can be repeated for multi-bit key.

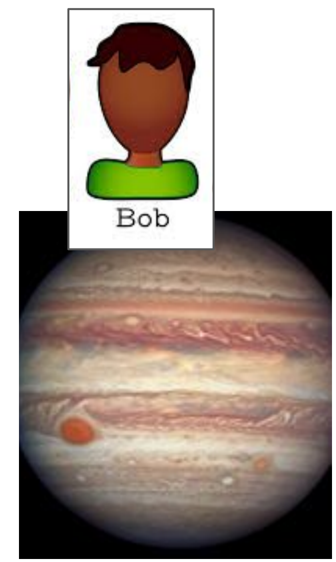
Secret Key Distribution (with Eve)

Two coins.
HH or TT with equal probability.



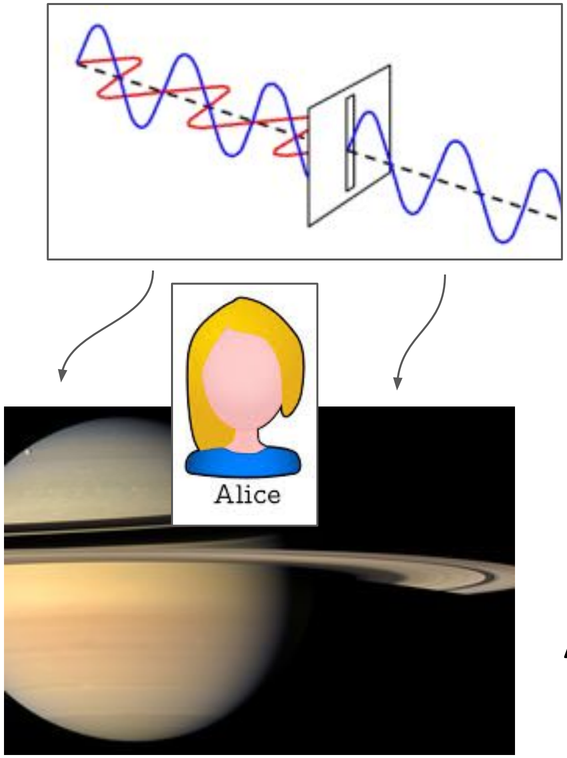
Alice throws one coin to Bob



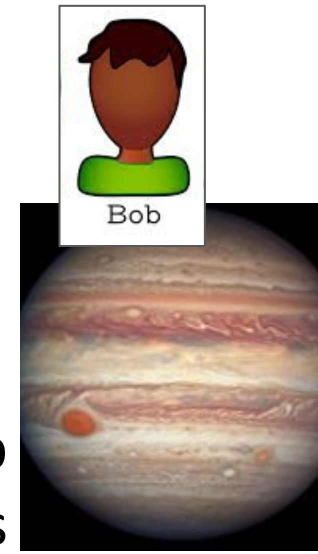


1. Alice checks her coin.
2. Bob checks his coin.
3. Alice and Bob share a random bit.
4. Eve also knows the shared bit.

Quantum Key Distribution



Two qubits. HH AND TT with equal probability.



Alice send one qubit to Bob

Alice measures

Bob measures

If Eve intercepts and measures, say H, Alice and Bob get HH.
If Eve does not intercept, Alice & Bob gets HH or TT with prob. ½.

Alice & Bob run random verification tests to detect Eve.

Possible since state of qubit "collapses" during measurement.

Where are the quantum Browsers and Softwares?

Qubits cannot be copied!

```
is the code that does the bubble sort.
for (int i = ar.length - 1; i > 0; i--) {
    for (int j = 0; j < i; j++) {
        if (ar[j] > ar[j + 1]) {
            temp = ar[j];
            ar[j] = ar[j + 1];
            ar[j + 1] = temp;
```

Quantum variables hold multiple values *at the same time!*

Output: A quantum state proportional to $|x\rangle$ where $x \approx x^* = A$

Algorithm:

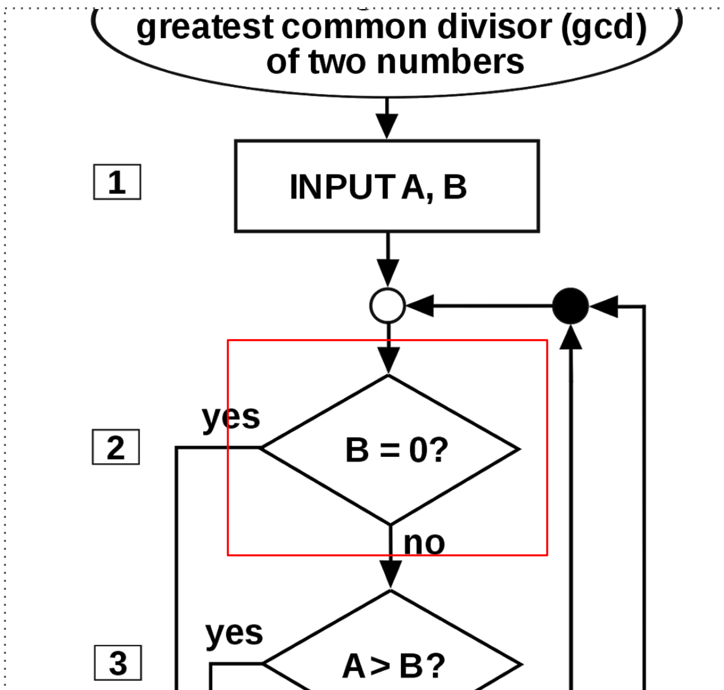
1. Prepare the quantum state $|b\rangle = \frac{1}{\|b\|_2} \sum_{i=1}^{n} \beta_i |v_i\rangle$.
2. Perform phase estimation to create the state $\frac{1}{\|b\|_2} \sum_{i=1}^{n} \beta_i |v$

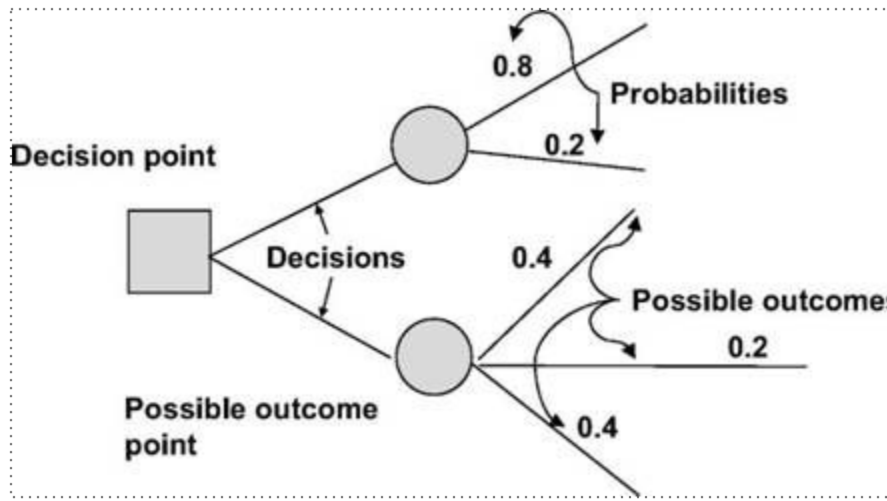
China working on quantum internet

Where are the quantum Browsers and Softwares?

Measuring qubit changes its state.

Final probability is NOT the sum of sub-tree probabilities.





Promises and Prospects

- **1981** Feynman proposed quantum computer to efficiently simulate many-body quantum systems

moonshot

- **1984** Bennett and Brassard designed quantum protocol for secret key sharing
- **1991** Another QKD protocol by Ekert

BB84 running on 2000KM fiber-optic cable in China

QKD networks : DARPA, Tokyo, Vienna, Japan, …

Promises and Prospects

Technology not clear

- **1985** Deutsch proposed a general purpose programmable quantum computer
- **1992** Deutsch and Jozsa solved a (toy) problem in half the time taken by the best classical algorithm
- **1993** Simon designed algorithm that is efficient on quantum computer but inefficient classically
- **1996** Grover designed algorithm to search in a database of N elements using √N "lookups" (classical best is N/2)

Quantum supremacy race

1994 √N is the best

… better-than-classical algorithms for problems on numbers, graphs, geometric objects, strings, statistics, communication, data structures, … but limited speedup

Promises and Prospects

2001 15 factored using 10^{18} identical molecules

Requires high-precision

- **1994** Shor designed algorithms to factor n-bit number in $O(n^2)$ time (classical best is $O(\exp(n^{1/3}))$)
- **1995** Shor and Steane designed error-correcting codes

Oops!

- **1998** Gottesman and Knill showed how to **efficiently** simulate certain quantum algorithms **classically**
- **2017** Microsoft releases 40-qubit classical simulator

ODE, PDE, machine learning

- **2009** Harrow+ designed linear system “solver” Quantum ML

Attacks on cryptography

- **2015** Grassl showed 3000-7000 qubits needed to search AES key using Grover’s algorithm
- **2016** Google simulated a Hydrogen molecule with 9 qubits

* Maybe you believe in the experiments yet disagree with the meaning

Summary

Quantum mechanics that drive quantum computing is mysterious

But if you are a believer … (*)

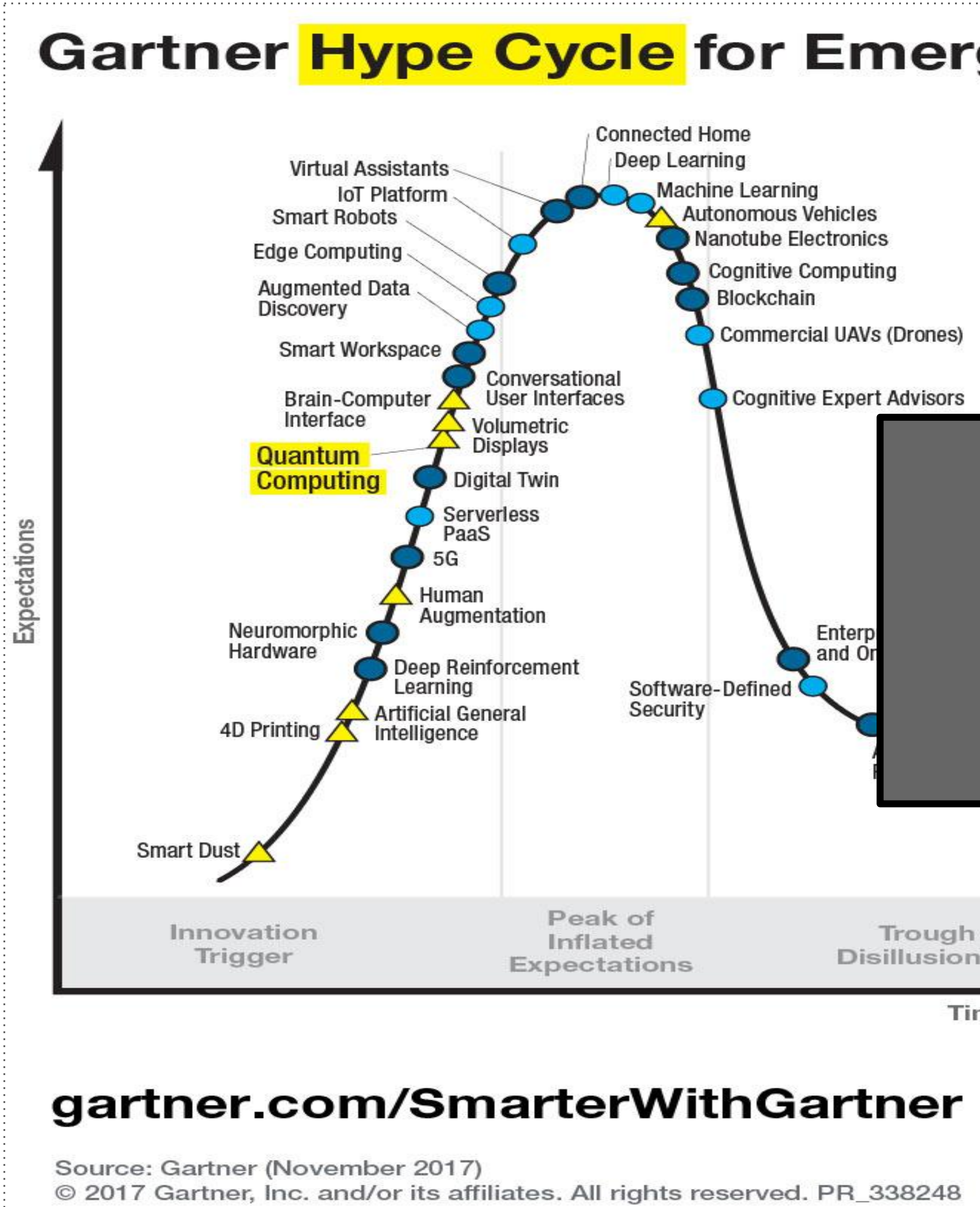
Quantum algorithm design and analysis possible using knowledge of algorithms, probability and linear algebra.

Thanks to physicists, material scientists, engineers, mathematicians, … in universities, R&D labs and corporates ...

These algorithms can be implemented on real quantum computers and experimented with.

Too early to say how and where QC will become useful …

Just the right time to enter the game.


Gartner Hype Cycle for
Connected Home
Deep Learning
Virtual Assistants
IoT Platform
Machine Learning
Autonomous Vehicles
Smart Robots
Nanotube Electronics
Edge Computing
Cognitive Computing
Augmented Data Discovery
Blockchain
Commercial UAVs (Drones)
Smart Workspace
Conversational User Interfaces
Cognitive Expert Advisors
Brain-Computer Interface
Volumetric Displays
Quantum Computing
Digital Twin
Serverless PaaS
5G
Human Augmentation
Neuromorphic Hardware
Deep Reinforcement Learning
Software-Defined Security
Artificial General Intelligence
4D Printing
Smart Dust
Expectations
Innovation Trigger
Peak of Inflated Expectations
Trough
gartner.com/SmarterWithGartner
Source: Gartner (November 2017)
© 2017 Gartner, Inc. and/or its affiliates. All rights reserved. PR_338248

THANK YOU