॥ त्वं ज्ञानमयो विज्ञानमयोऽसि ॥

I.I.T. Jodhpur

Q.K.D. - Quantum Key Distribution

Protocol Discussed - BB84, Probabilistic analysis and Code Demo

presented by: Sanyam Jain (P20QC001)

Under supervision of Dr. Somitra Kumar Sanadhya

Slide 1

Contents:

- Introduction to Quantum Information
    - bit vs qubit, bloch sphere, quantum gates
- A quick history to quantum information and computing
- Why Quantum Crypto and What is QKD?
- Quantum Principles : HUP / Superposition and Quantum Entanglement
- BB84 protocol
- Animation to show working of BB84
- Showcasing working of BB84 on iPad
- Analysis using python (outputs from experiment)
- Recent case study of DRDO & ISRO
- References
- Coming up in next presentation...

before we go ahead…

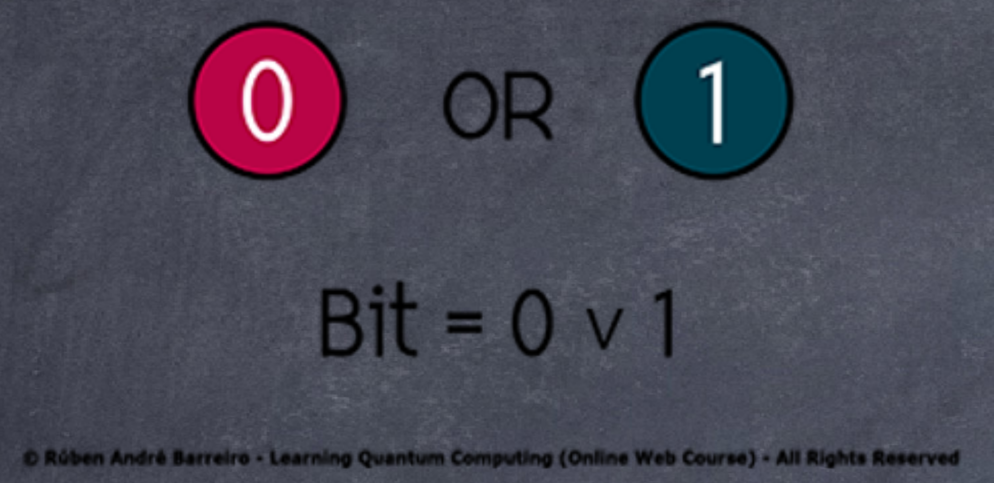
Without quantum safe encryption everything we have ever transmitted over a network or will ever transmit over a network is vulnerable because of course what governments are doing is they're downloading information now and when a quantum computer comes along they will be able to decrypt that now if that's information which has transient value that is not a problem but what if it's you're in its information with a value of ten years that means that if a quantum computer is available in 2030 you need to be quantum safe in 2020 what if it's your DNA information that can be used against you and your children what if it's military information that should be kept secure 50 years so this is a real problem and the question is now what do we do about key exchange do we use RSA and elect a curve and DHKE or do we go back to a kind of manual key exchange this is what they used in the time of the ancient Greeks they would put a code on the head of somebody they would tattoo it then wait till the hair grew and then they'd send that messenger into enemy lines and as soon as he arrived they would shave the head there are quite a few casualties but you know people were more expendable then so what do we do about key exchange.

— Kelly Richdale,
Aalto University

Slide 3

Introduction to Quantum Information

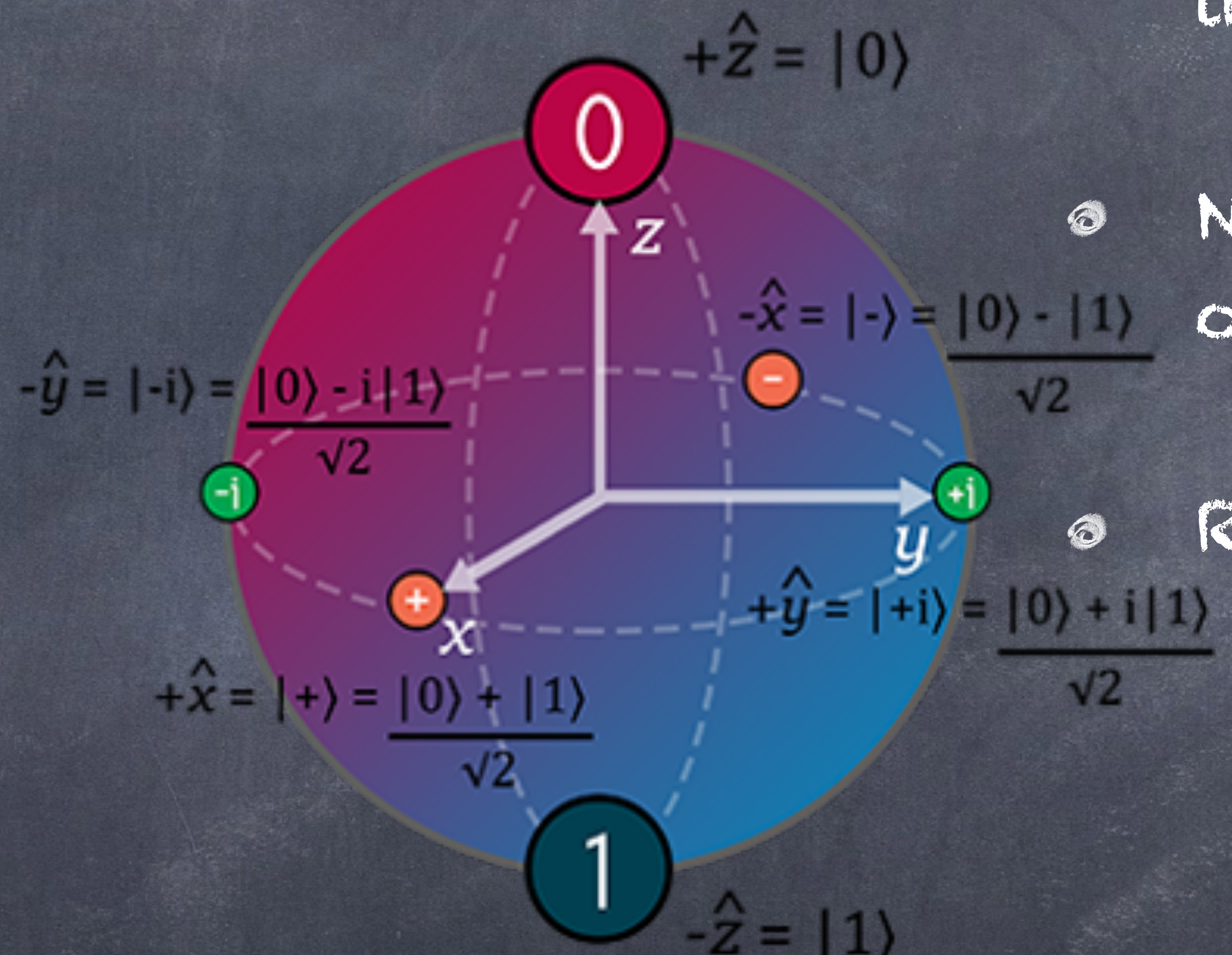
(1) bit vs qubit



Bit = 0 v 1

© Rúben André Barreiro - Learning Quantum Computing (Online Web Course) - All Rights Reserved

- Bit is a basic unit of classical information
- Deterministic (either 0/1)


$+\hat{z} = |0\rangle$
0
z
$-\hat{x} = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
$-\hat{y} = |-i\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$
-i
-
+i
y
+
x
$+\hat{y} = |+i\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
$+\hat{x} = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$
1
$-\hat{z} = |1\rangle$

$$\text{Qubit} = \alpha|0\rangle + \beta|1\rangle$$

© Rúben André Barreiro - Learning Quantum Computing (Online Web Course) - All Rights Reserved

- quBit is a basic unit of quantum information
- Non Deterministic (either 0/1) or Probabilistic
- Represented using Bloch sphere

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

Source:
Ruben, Github

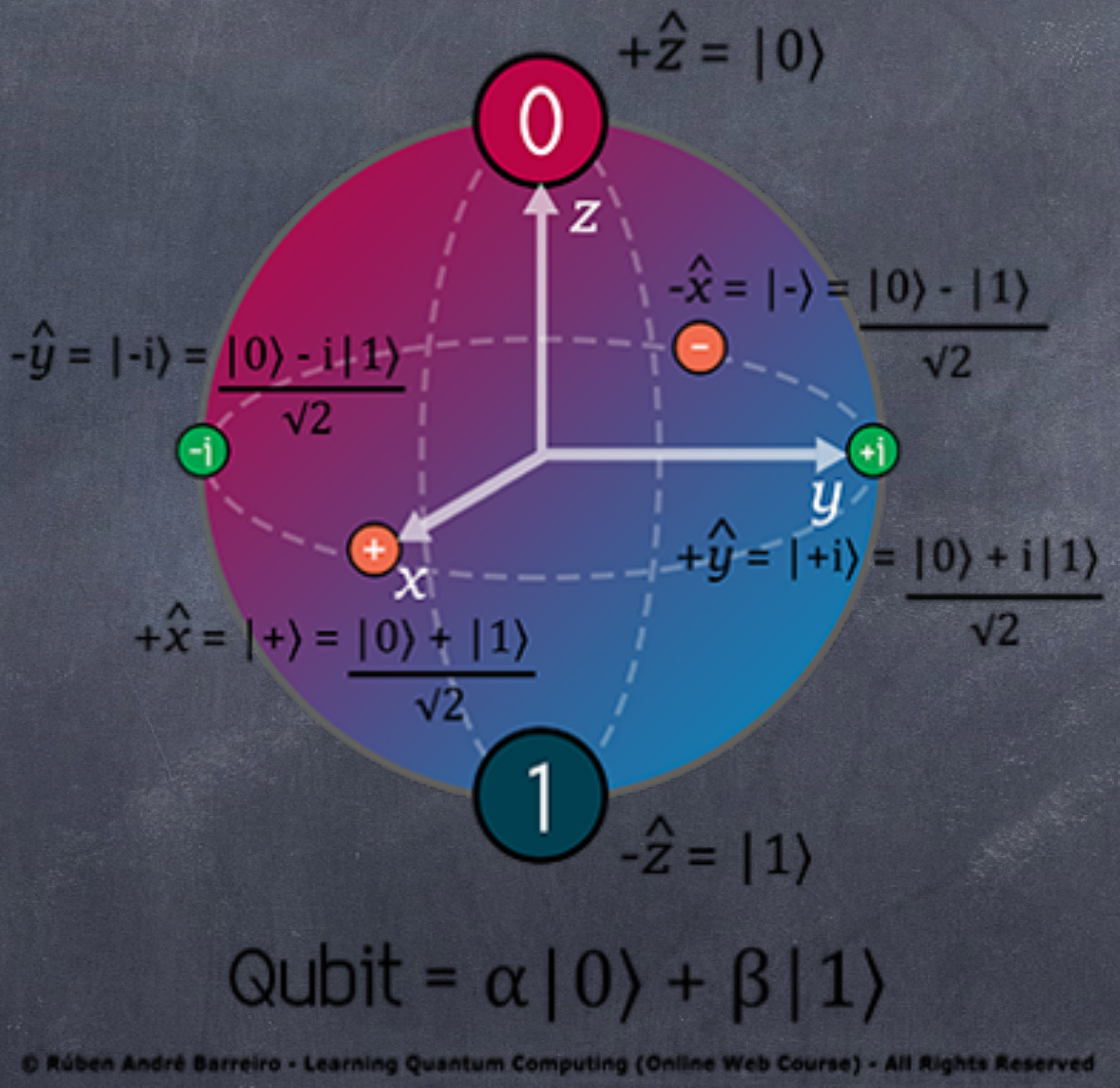
Slide 4

Introduction to Quantum Information

(2) bloch sphere

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

- Bloch sphere is a geometrical representation of qubit
- Represents spin up and spin down of a photon. That is |0⟩ or |1⟩



$+\hat{z} = |0\rangle$
0
z
$-\hat{x} = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
$-\hat{y} = |-i\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$
-i
+i
y
$+\hat{y} = |+i\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
x
$+\hat{x} = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$
1
$-\hat{z} = |1\rangle$
Qubit = α|0⟩ + β|1⟩

© Rúben André Barreiro - Learning Quantum Computing (Online Web Course) - All Rights Reserved

Source:
Ruben, Github

Introduction to Quantum Information

(3) quantum gates

- Identity Gate (I) •$|0\rangle \to |0\rangle$;
- Hadamard Gate (H) takes one bit as input and converts that to a superposition (+ or −). $|0\rangle \to |+\rangle$; $|1\rangle \to |-\rangle$; $|+\rangle \to |0\rangle$; $|-\rangle \to |1\rangle$;
- Not Gate (X) •$|0\rangle \to |1\rangle$;
- Mapping Gate (Y)
- Phase Flip (Z) Performs phase flip from "+" to "x" and vice versa.

Introduction to Quantum Information

(4) quantum bits

Together, a_i and b_i, provide us an index for the following four Quantum States of a Qubit (Quantum Bit):

1. $|\Psi_{00}\rangle = |0\rangle$, which is equivalent to the Classical Bit Value of 0 (i.e., ground state or ↑);

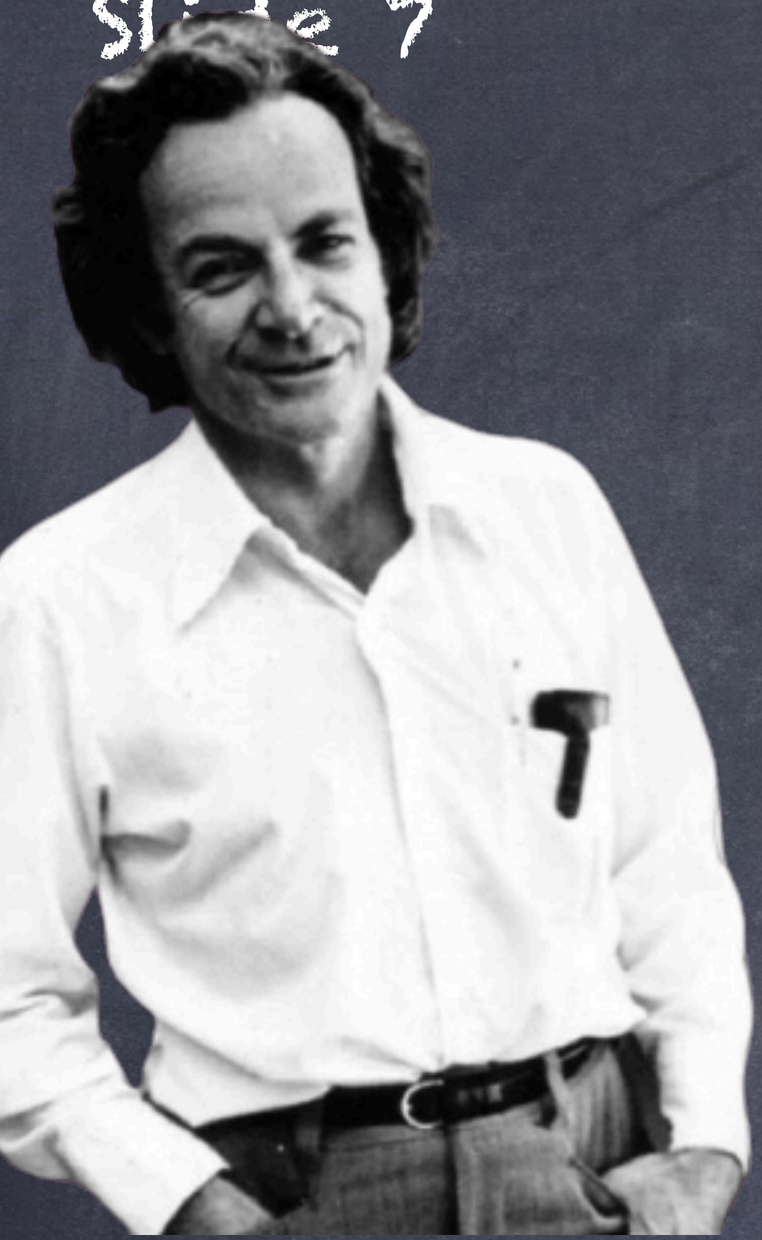
2. $|\Psi_{10}\rangle = |1\rangle$, which is equivalent to the Classical Bit Value of 1 (i.e., excited state or ↓);

3. $|\Psi_{01}\rangle = |+\rangle = 1/\sqrt{2}\ |0\rangle + 1/\sqrt{2}\ |1\rangle$, which is equivalent to a Quantum Superposition of States, based on the positive X-Axis of the Bloch Sphere;

4. $|\Psi_{11}\rangle = |-\rangle = 1/\sqrt{2}\ |0\rangle - 1/\sqrt{2}\ |1\rangle$, which is equivalent to a Quantum Superposition of States, based on the negative X-Axis of the Bloch Sphere;

Slide 7

Quick history to quantum information and computing



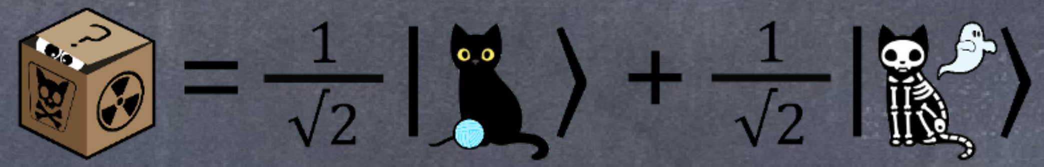
- 1970 - Scientists Gained Control over one photon quantum systems.
- Advent of separating photon from rest of the world to produce new results.
- This helped to exploit the power of photons in quantum information.
- At small scale, dozens of operations were able to perform on very few qubits represents state of the art in quantum computing.
- However there is a very drastic gap between bridging the small scale quantum machines to large scale to perform real world applications.

Why Quantum Cryptography and What is QKD?

- Cryptography - Public Key Cryptography , Secret Key Cryptography
- In PKC - same shared key is used for encryption / decryption. For sharing the key in first time DHKE is used.
- In SKC - One can use other's public key and encrypt the information and send it to receiver who can further decrypt it using its owns private key.
- While, crypto-systems are based on assumption of computing power of the attacker which is based on unproven assumptions of difficulty of certain problems such as integer factorisation.

Quantum Principles :
HUP / Superposition and Quantum Entanglement

- Protocols are mostly divided into 2 categories:
  - HUP - Heisenberg Uncertainty Principle.



  - QE - Quantum Entanglement.
  - HUP based protocols exploit the property of polarisation power of photons. Polarisation is then studied over the receiver side of the channel. The HUP guarantees that eve cannot measure the photons sent by Alice to bob without disturbing the photons state in detectable way. Thus revealing her presence.
  - QE based protocols ensure that in the presence of some eave, the entanglement between photons get collapsed. Calculation of Bell inequalities will result the change in polarization of the photons.

BB84 Protocol

- Communication is via classical channel as well as quantum channel makes it a quasi QKD
- Once measured the quantum state is get collapsed. Any Quantum Measurement of a Quantum System makes it collapse, resulting in a deterministic and irreversible Classical State.
- Most prominent Quantum Cryptography protocol, all other HUP based protocols are more or less variants of BB84.
- Process:
    - Generation of random bitstring and bases
    - Quantum transmission of encoded bits
    - Measured by the receiver.
    - Public comparison of bases and polarizations.
        - Information Reconciliation
        - Privacy Reconciliation

BB84 Protocol

- (1) Alice chooses $(4 + \delta)n$ random data bits.
- (2) Alice chooses a random $(4 + \delta)n$-bit string b. She encodes each data bit as $\{|0\rangle|1\rangle\}$ if the corresponding bit of b is 0 or $\{|+\rangle\ |-\rangle\}$ if b is 1.
- (3) Alice sends the resulting state to Bob.
- (4) Bob receives the $(4 + \delta)n$ qubits, announces this fact, and measures each qubit in the X or Z basisat random.
- (5) Alice announces b.
- (6) Alice and Bob discard any bits where Bob measured a different basis than Alice prepared. With high probability, there are at least 2n bits left (if not, abort the protocol). They keep 2n bits.
- (7) Alice selects a subset of n bits that will to serve as a check on Eve's interference, and tells Bob which bits she selected.
- (8) Alice and Bob announce and compare the values of the n check bits. If more than an acceptable number disagree, they abort the protocol.
- (9) Alice and Bob perform information reconciliation and privacy amplification on the remaining n bits to obtain m shared key bits.

Slide 12

BB84 Protocol

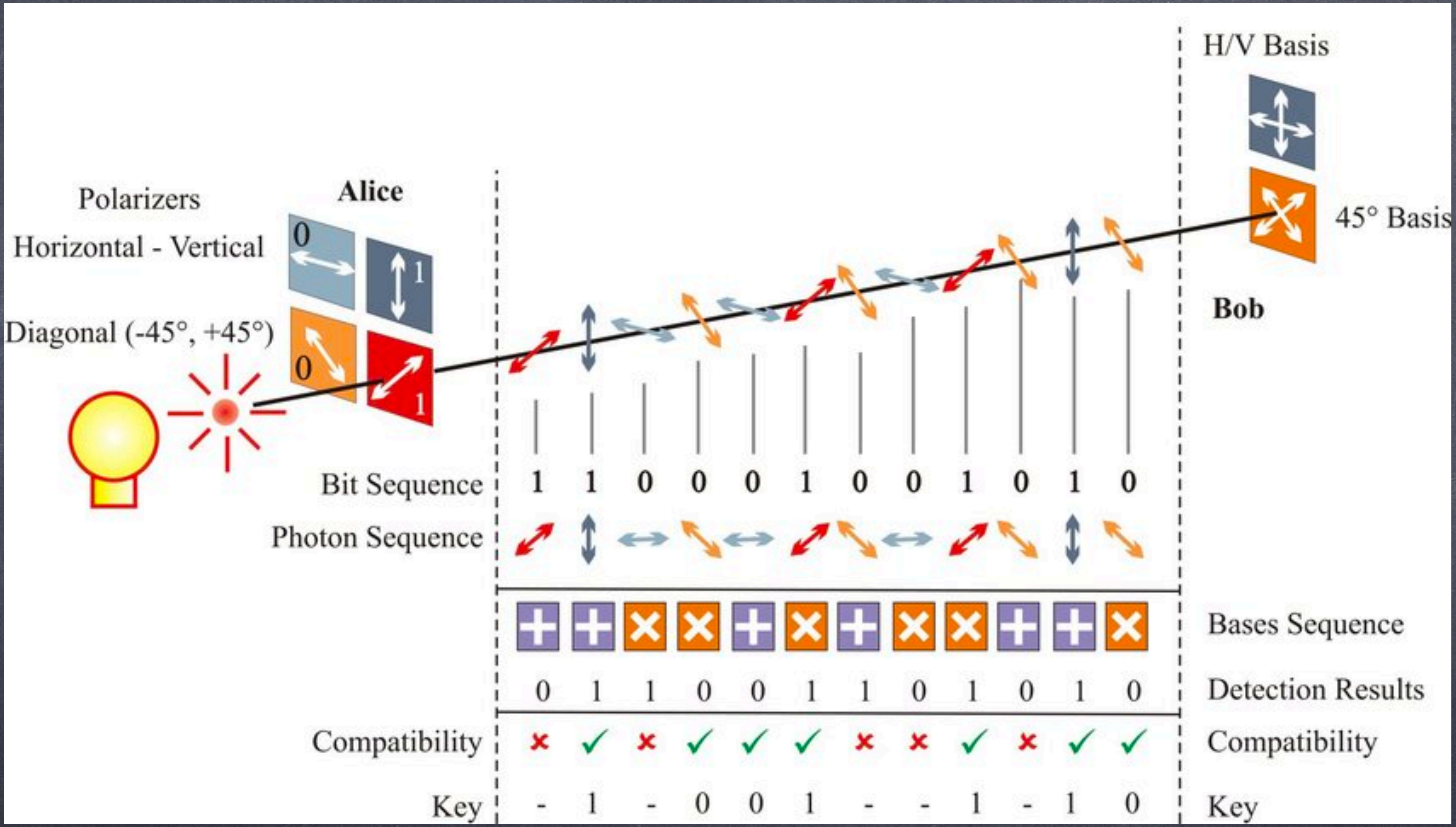
- Explaining the protocol over iPad….

without eave

with eave

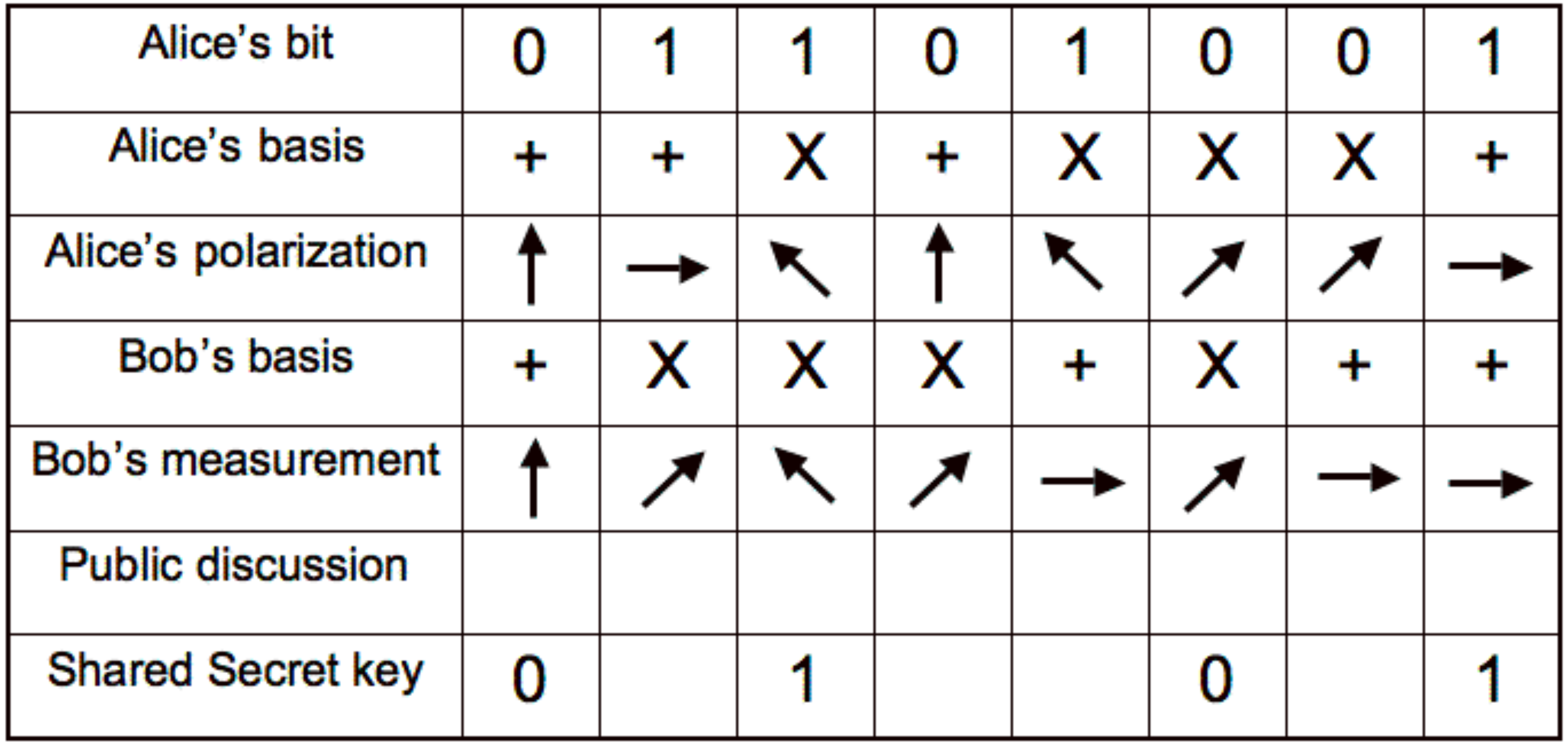
Source:
The Centre for Quantum Technologies in Singapore

BB84 Images



Bit Sequence	1	1	0	0	0	1	0	0	1	0	1	0	
Photon Sequence	⤢	↕	↔	⤡	↔	⤢	⤡	↔	⤢	⤡	↕	⤡	
	+	+	×	×	+	×	+	×	×	+	+	×	Bases Sequence
	0	1	1	0	0	1	1	0	1	0	1	0	Detection Results
Compatibility	✗	✓	✗	✓	✓	✓	✗	✗	✓	✗	✓	✓	Compatibility
Key	-	1	-	0	0	1	-	-	1	-	1	0	Key

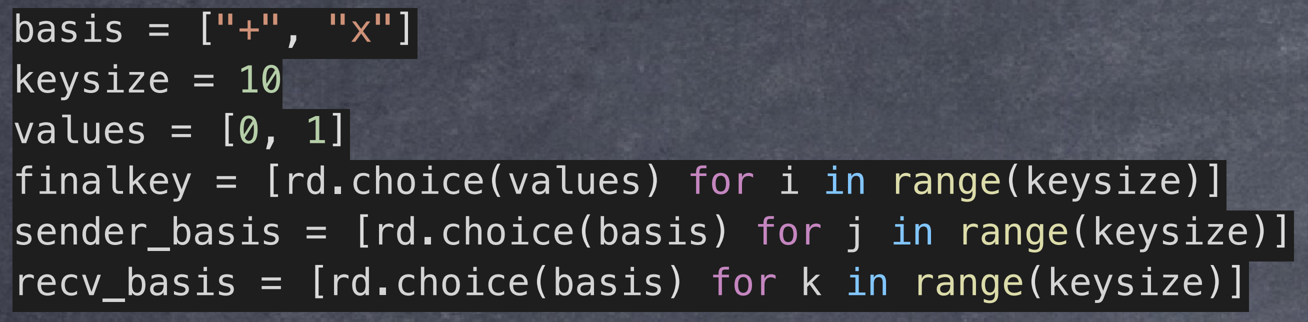
BB84 example



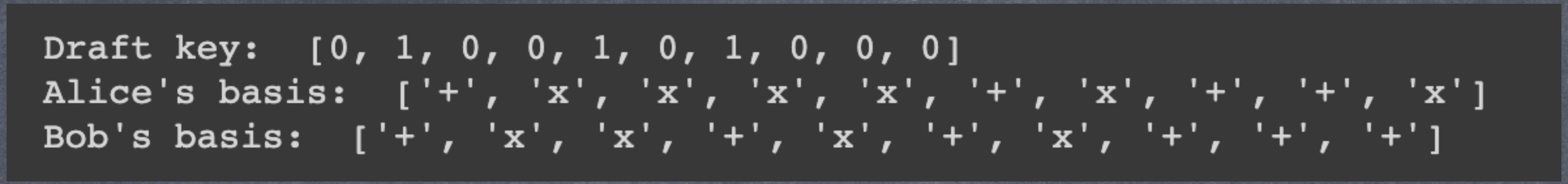
Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Slide 15

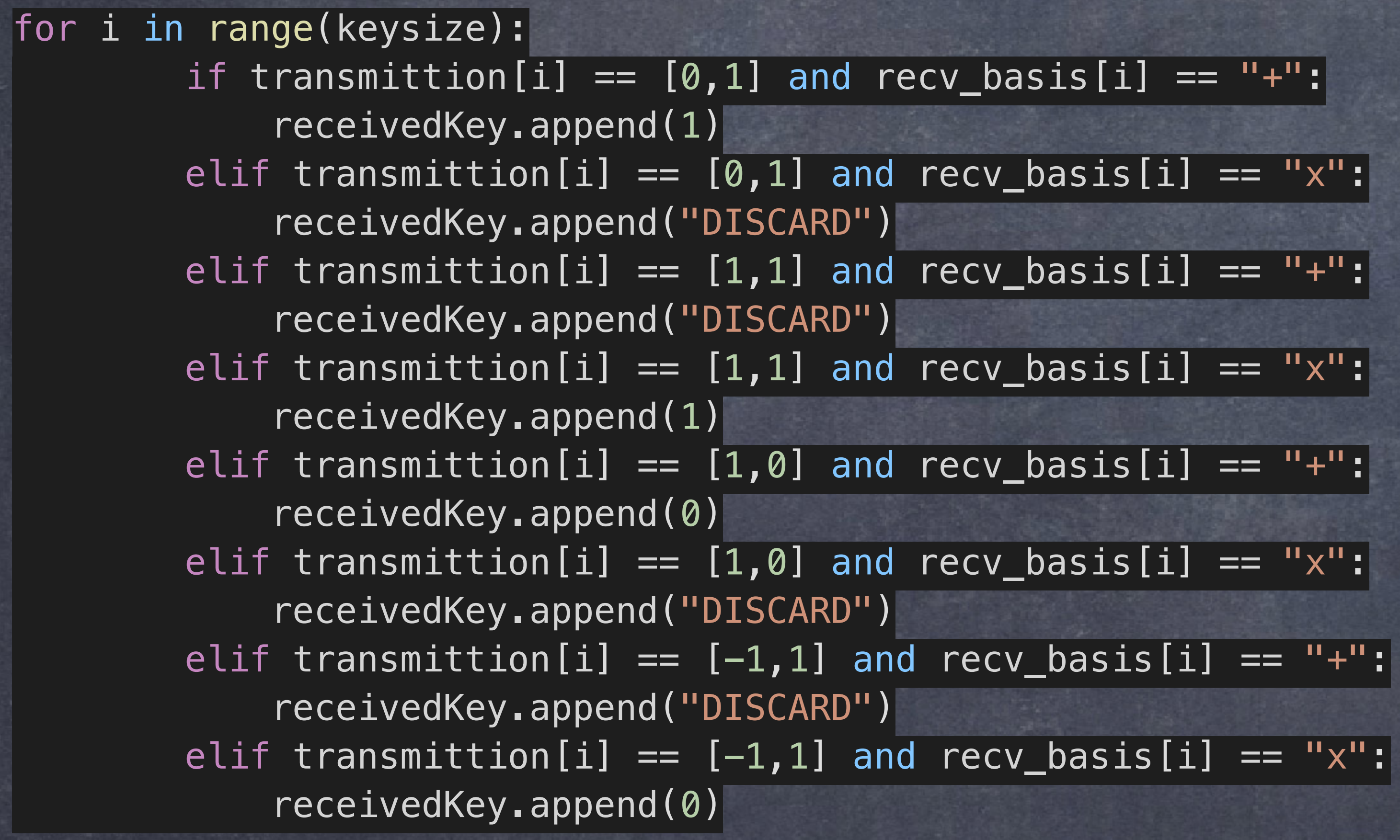
Analysis using Python



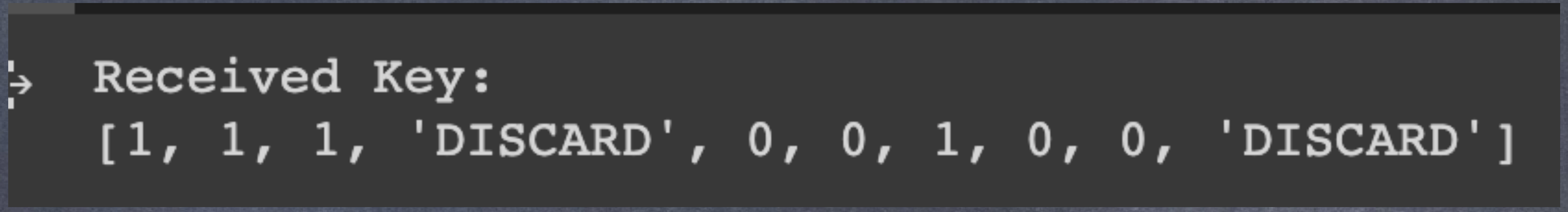
```
basis = ["+", "x"]
keysize = 10
values = [0, 1]
finalkey = [rd.choice(values) for i in range(keysize)]
sender_basis = [rd.choice(basis) for j in range(keysize)]
recv_basis = [rd.choice(basis) for k in range(keysize)]
```



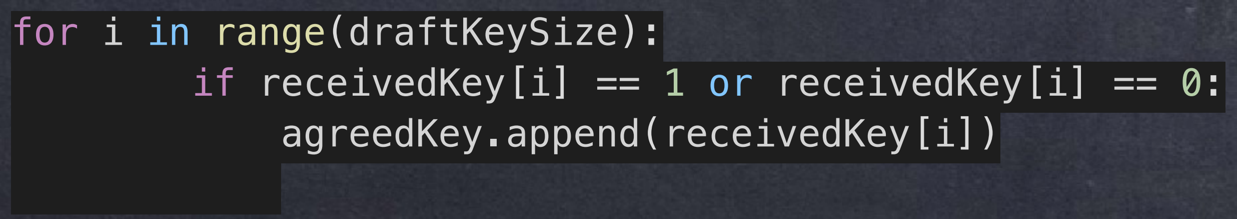
```
Draft key:  [0, 1, 0, 0, 1, 0, 1, 0, 0, 0]
Alice's basis:  ['+', 'x', 'x', 'x', 'x', '+', 'x', '+', '+', 'x']
Bob's basis:  ['+', 'x', 'x', '+', 'x', '+', 'x', '+', '+', '+']
```



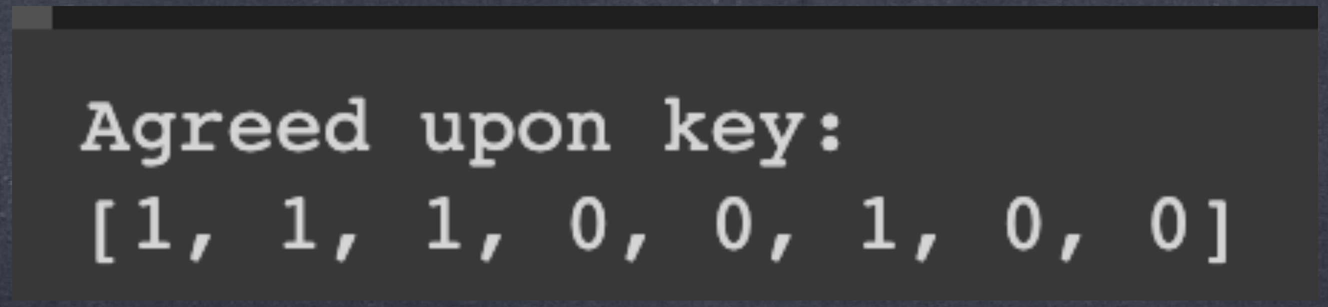
```
for i in range(keysize):
        if transmittion[i] == [0,1] and recv_basis[i] == "+":
            receivedKey.append(1)
        elif transmittion[i] == [0,1] and recv_basis[i] == "x":
            receivedKey.append("DISCARD")
        elif transmittion[i] == [1,1] and recv_basis[i] == "+":
            receivedKey.append("DISCARD")
        elif transmittion[i] == [1,1] and recv_basis[i] == "x":
            receivedKey.append(1)
        elif transmittion[i] == [1,0] and recv_basis[i] == "+":
            receivedKey.append(0)
        elif transmittion[i] == [1,0] and recv_basis[i] == "x":
            receivedKey.append("DISCARD")
        elif transmittion[i] == [-1,1] and recv_basis[i] == "+":
            receivedKey.append("DISCARD")
        elif transmittion[i] == [-1,1] and recv_basis[i] == "x":
            receivedKey.append(0)
```



```
Received Key:
[1, 1, 1, 'DISCARD', 0, 0, 1, 0, 0, 'DISCARD']
```

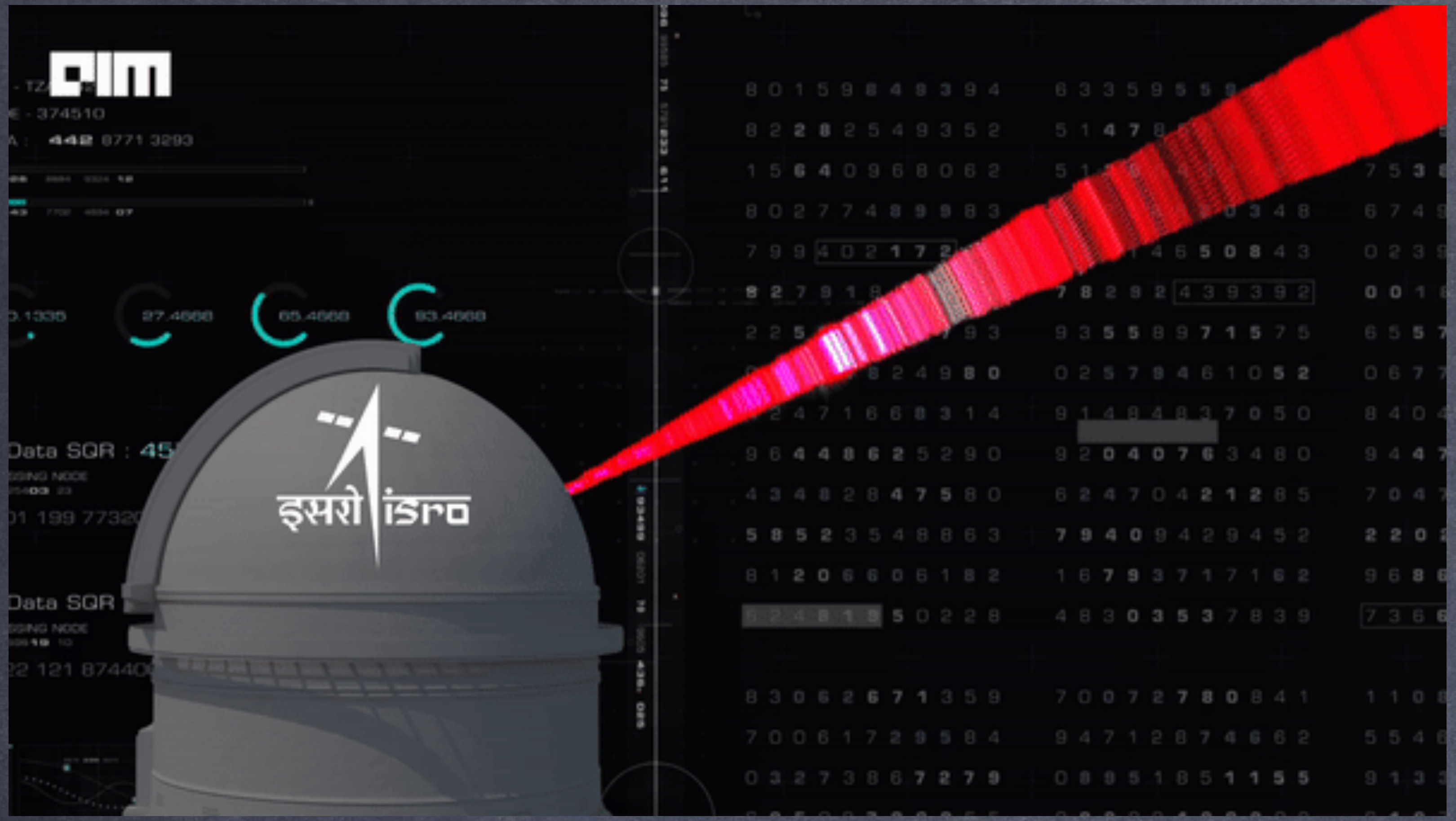


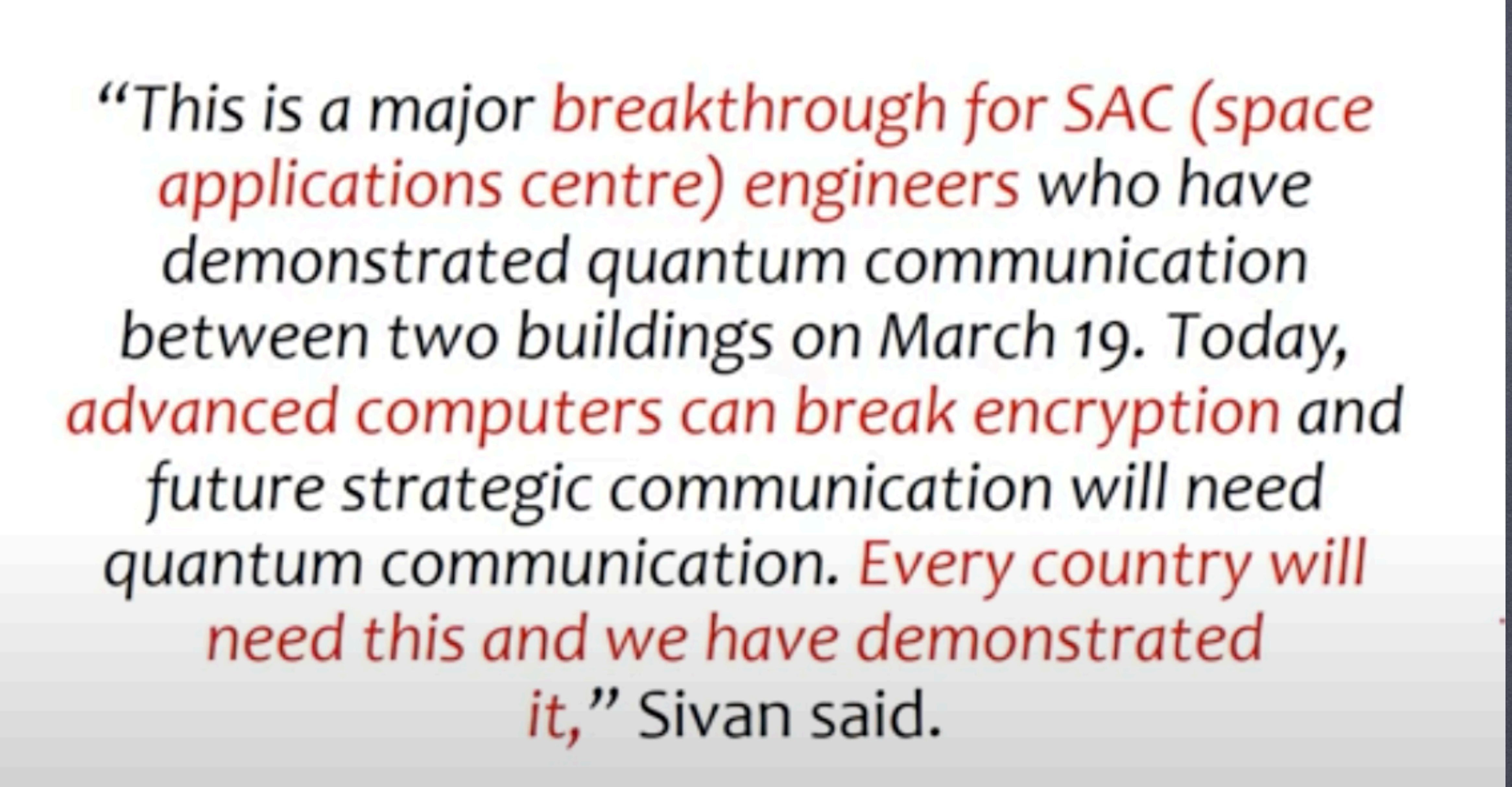
```
for i in range(draftKeySize):
        if receivedKey[i] == 1 or receivedKey[i] == 0:
            agreedKey.append(receivedKey[i])
```



```
Agreed upon key:
[1, 1, 1, 0, 0, 1, 0, 0]
```

DRDO and ISRO recent work: QuEST Project by QuIC lab




“This is a major breakthrough for SAC (space applications centre) engineers who have demonstrated quantum communication between two buildings on March 19. Today, advanced computers can break encryption and future strategic communication will need quantum communication. Every country will need this and we have demonstrated it,” Sivan said.

- March 2021
- Quantum Communication over 300m channel.
- Used QKD in SAC (Space Agency Ahmedabad)
- The experiment is important to conduct satellite based quantum communication. Which China has already conducted successfully via Micius in 2016 also known as Quantum Experiments at Space Scale.

Image Source:
PIB website, Indiatimes news

Primary References

Arpita Maitra, Goutam Paul, Another Look at Symmetric Incoherent Optimal Eavesdropping against BB84, 2011, INDOCRYPT 2012

Anne Broadbent, C.Shaffner, Quantum Cryptography Beyond Quantum Key Distribution, 2015, Design Codes and Cryptography

Mihai Zichu Mina, Emil Simion, A Scalable Simulation of the BB84 Protocol Involving Eavesdropping, 2020, Cryptology ePrint Archive

Yaroslav Balytskyi , Manohar Raavi , Anatoliy Pinchuk, Sang-Yoon Chang, PT -Symmetric Quantum State Discrimination for Attack on BB84 Quantum Key Distribution, 2021, Conf: TBA

Alexandru-Ștefan Gheorghieș , Darius-Marian Lăzăroi , and Emil Simion, A Comparative Study of Cryptographic Key Distribution Protocols, 2021, Project: Cybersecurity

Slide 17

Secondary References for images and animations...

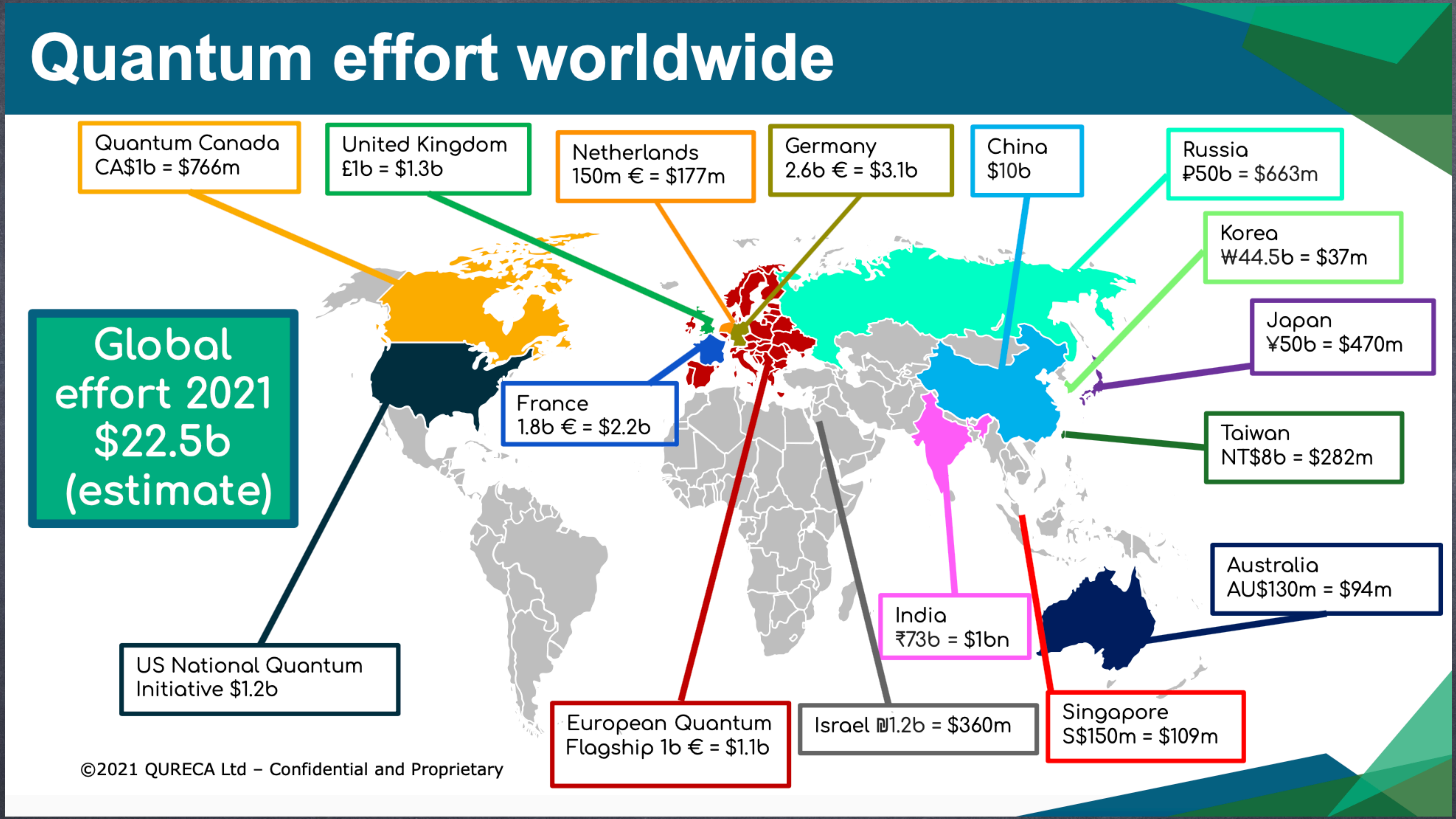
- BB84 Protocol of quantum key distribution - YouTube
  - https://www.youtube.com/watch?v=44G9UuB2RWI&ab_channel=%EC%B0%BD%ED%95%98%EA%B9%80
- Quantum Optics - Quantum cryptography the BB84 QKD scheme - YouTube
  - https://www.youtube.com/watch?v=MlsrCzDdAbE&ab_channel=intrigano
- Quantum Key Distribution Animation - YouTube
  - https://www.youtube.com/watch?v=cWpqlgF7uEA&ab_channel=InstituteforQuantumComputing

Slide 18

Coming up next…

- I will present B92 protocol and Eckert's protocol in next presentation.
- I will also present popular attack called Photon Splitting attack.
- I will try to simulate a communication between 2 parties backed with quantum emulators (IBM qiskit) realtime. May be 2 parties agreeing upon a strong key.
- That is will try to simulate it with and without eave. How much interference does eave produce and the resulting deflection on the key-agreement.
- In simpler words, I will try to study how fast Alice and Bob can converge with minimum trials needed in the presence of non-naíve protagonists and antagonist. (assuming eave, alice and bob all knows sufficient quantum mechanics)

Thank You



Quantum effort worldwide

Global effort 2021 $22.5b (estimate)

Quantum Canada
CA$1b = $766m

United Kingdom
£1b = $1.3b

Netherlands
150m € = $177m

Germany
2.6b € = $3.1b

China
$10b

Russia
₽50b = $663m

Korea
₩44.5b = $37m

Japan
¥50b = $470m

France
1.8b € = $2.2b

Taiwan
NT$8b = $282m

Australia
AU$130m = $94m

India
₹73b = $1bn

US National Quantum
Initiative $1.2b

European Quantum
Flagship 1b € = $1.1b

Israel ₪1.2b = $360m

Singapore
S$150m = $109m

Source:
Google Images