Trends in Quantum Technology

First International Quantum Communication Conclave

Dr. Rajkumar Upadhyay
Chief Executive Officer
Centre for Development of Telematics (C-DOT)
New Delhi, India
ceo@cdot.in

27 March 2023

Agenda

- Introduction
- Quantum Technologies
- The Global Picture
- Quantum Communication
  - The Need
  - Candidate Technologies
  - Applications
- Quantum Communication & C-DOT
- Summary

Quantum technology has been around for a long time..

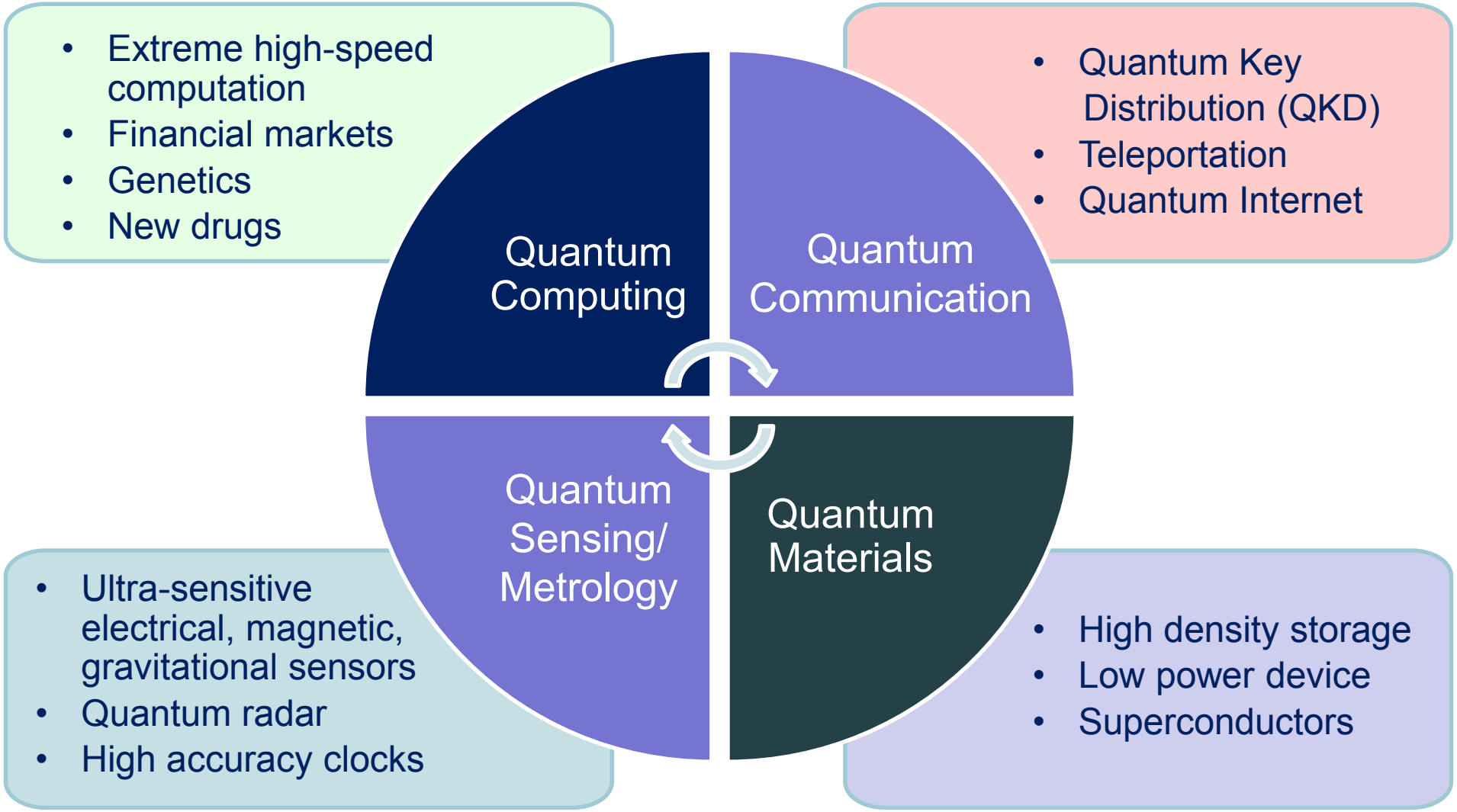
Lasers work using the quantum mechanical effect known as **stimulated emission**

Solar cells work based on quantum mechanical effect known as **photovoltaic effect**

MRI uses the quantum phenomenon called **magnetic resonance**

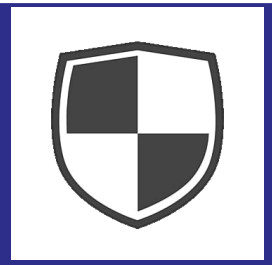
…But a few emerging technologies will change our computational, communication, and sensory infrastructure in the coming years, unleashing potential use cases and previously unimaginable capabilities

Verticals of Quantum Technologies



The Future is Quantum!

सी-डॉट
C-DOT



Defense & Security

Ultra secure communication, high precision sensing

Drug Discovery

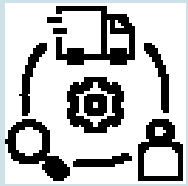
Fast paced research by reducing the search space and time

Healthcare

Increased throughput, reduced wait time, improved outcomes

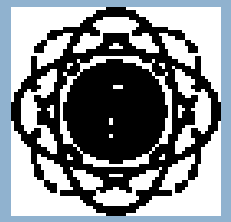
Manufacturing

Reduced wastage and emissions, optimized synthesis and assembly



Supply Chain

Higher accuracy, better warehouse management, higher transport efficiency



Energy

Minimize loss and carbon emissions, optimal usage of resources

Finance

Reduced cost and time, portfolio optimization, secured transactions

Oil & Gas

Optimized allocation and utilization of resources, higher profitability

We are in the midst of second quantum revolution..

Global acceleration in investments

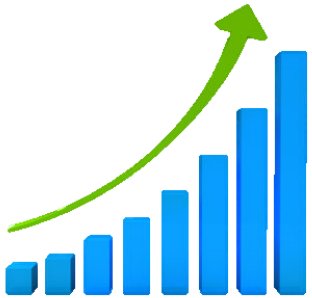
~$1.85 billion

Investments in quantum start-ups in 2022, 10% more than 2021*

Technology maturing rapidly

<10 years

Estimated timeline to unleash the full potential as technology matures**



Market expected to grow exponentially

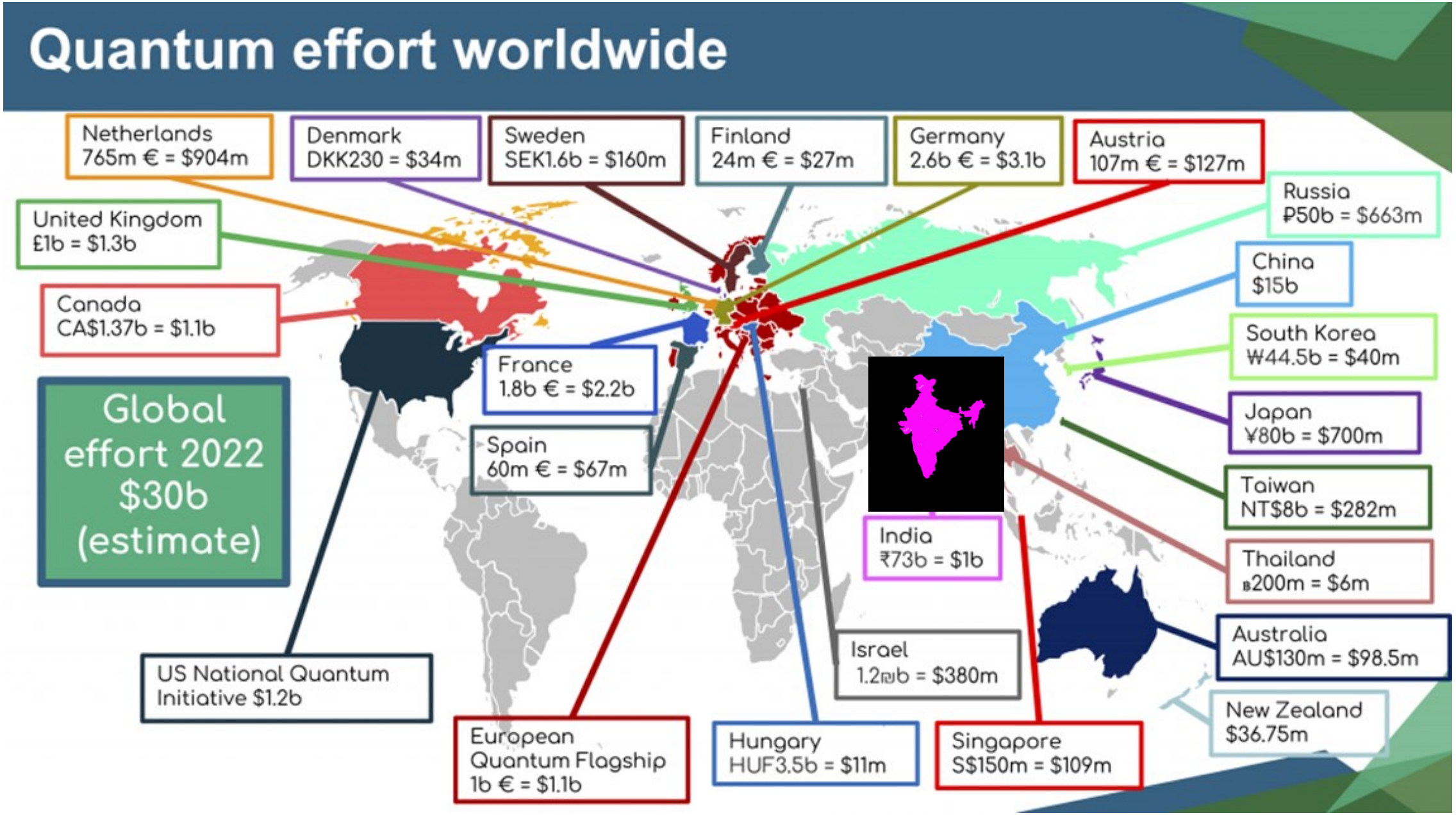
~$44 billion

Projected market size in 2028, to grow with a CAGR of 30.2%***

2023 General Assembly of the UN to proclaim 2025 the **International Year of Quantum Science and Technology**

Source:
* https://finance.yahoo.com/news/worldwide-quantum-computing-industry-2043-154500826.html
** McKinsey Technology Trends Outlook 2022-Quantum Technologies August 2022
*** Quantum Technology Market: Overview by Market Research Stores

Quantum effort worldwide



Source: https://qureca.com/overview-on-quantum-initiatives-worldwide-update-2022/

Global Startup Heat Map: Quantum Technology

StartUs insights

1040

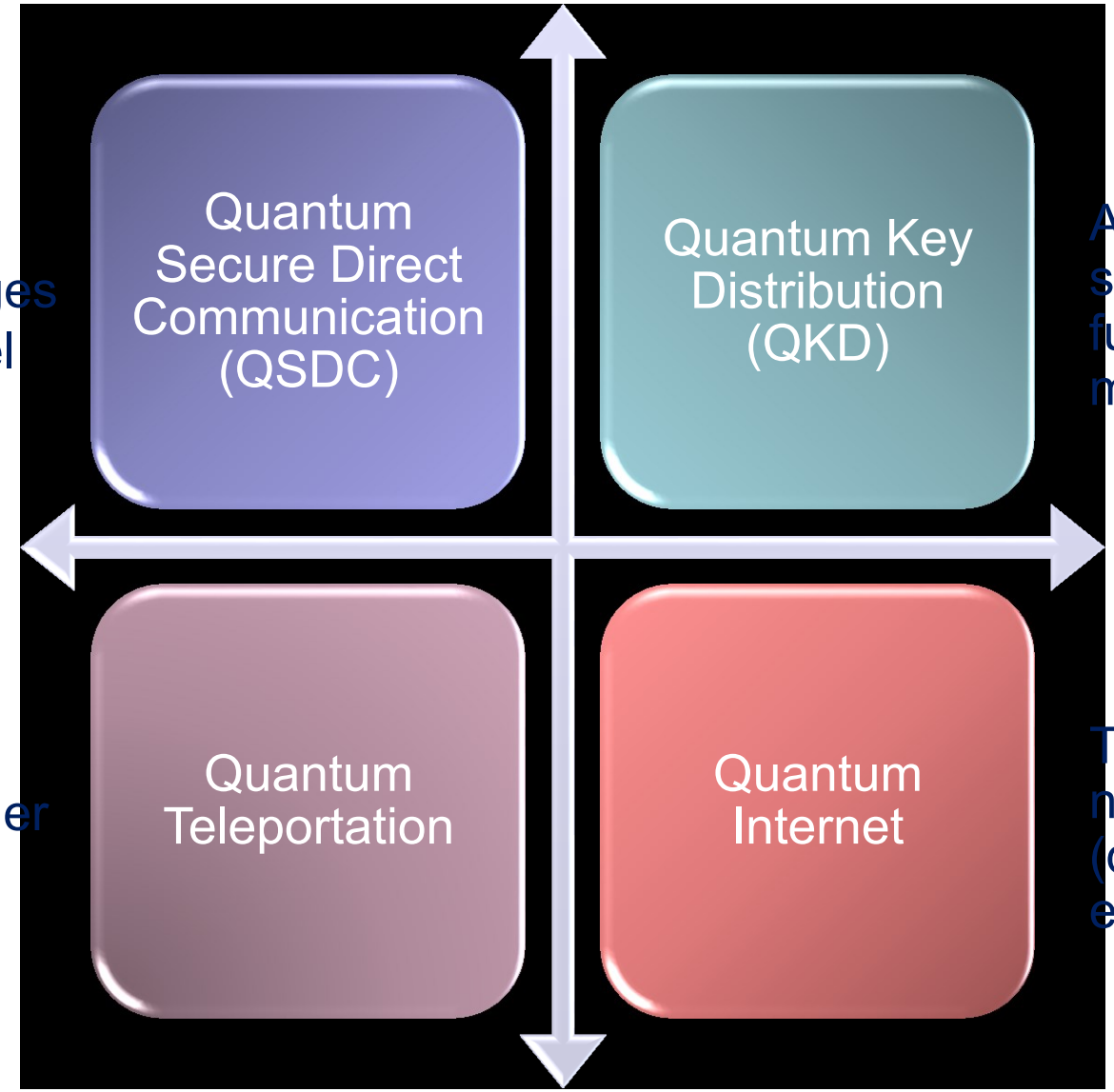
STARTUPS ANALYZED

Source: https://www.startus-insights.com/innovators-guide/quantum-technology-trends/


Top 10 Quantum Technology Trends in 2023
Quantum Technology
Quantum Sensors
Hybrid Quantum Applications
Quantum Communication
Novel Qubits
Advanced Materials
Post-Quantum Cryptography
Quantum Simulations
Quantum Machine Learning
Cloud Computing
Fault-Tolerance Computing
QDI systems
Quantum Technologies
seeqc
Xairos
Aliro
QC82
parityqc
C12
QustomDot
Terra Quantum
KUANO
QUANSCIENT
QUANTUM
QuantrolOx
Nord Quantique
ALICE & BOB
1 040
Startups & emerging companies analyzed
Data provided by
StartUs insights
November 2022

Quantum Communication: Technology Candidates

Direct and secure transmission of messages over a quantum channel



A method of key exchange with security guaranteed by the fundamental rules of quantum mechanics

Transfer of quantum information from a sender to a receiver

Transfer of qubits across a network of quantum devices (quantum computers, sensors, etc.)

Quantum Communication: The Need of the Hour

While quantum technologies will bring a paradigm shift in almost every aspect of life, access of such technologies to an adversary poses threat to existing data security and encryption technologies.

Intrusions remain undetectable

$f(x)$

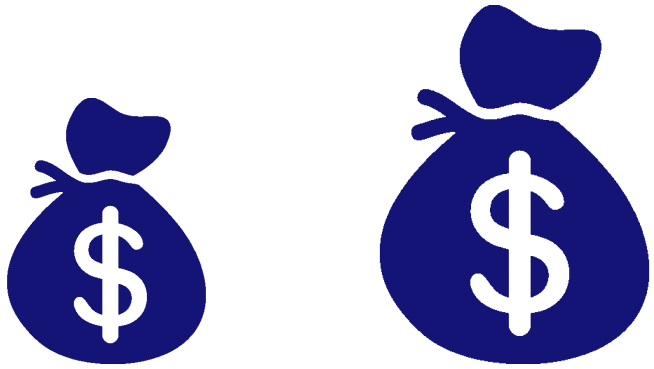
Security is based on belief and not unconditional; With advent of quantum computers, security stands compromised

Brute force attack on cryptographic keys are easy due to low frequency of key update

SLOW

Asymmetric cryptographies are 2-3 times slower than equivalent symmetric cryptographic algorithms

Should We Get Worried?



2020 3.86 million

2022 4.35 million

Average total cost of a data breach

IBM Security Report 2020 and 2022

News / Technology / News / Chinese researchers claim they can break 2048-bit RSA using quantum computers, entire tech world at risk

Chinese researchers claim they can break 2048-bit RSA using quantum computers, entire tech world at risk

In a startling claim, some Chinese researchers have claimed that they can break 2048-bit RSA encryption using existing quantum computers. If true, the claim will remake the entire tech world and internet as it will put at everything digital at a risk.

Source: https://www.indiatoday.in/ Date: 6 January 2023

Articles / Analysis

'Harvest Now, Decrypt Later' Concern Boosts Quantum Security Awareness

Nancy Liu | Editor
September 28, 2022 2:00 AM

Share this article:

Source: https://www.sdxcentral.com/articles/analysis/

Infamous hacker Kevin Mitnick sniffs fiber, reads email

Kevin Mitnick demonstrates how easy it is for a hacker to tap into your network and read your email messages, even if it's a fiber optic network.

Source: https://www.zdnet.com/article/

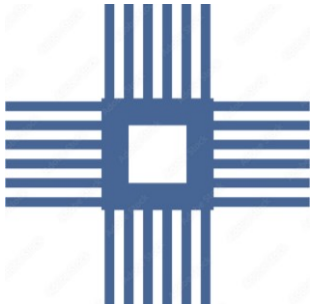
Quantum Communication: Applications

Quantum (enhanced) Classical Cryptography

- **Quantum Random Number Generator (QRNG)** can enhance the security of classical cryptography, one-time passwords, lotteries etc.

Quantum Cryptography

- **Secure communication** enabled by a quantum generated perfectly random and secure key shared between distant communicating partners—e.g., quantum key distribution (QKD)



Enhanced Quantum Computing/Internet

- **Distributed quantum processing**, where multiple quantum computers are connected to enhance computing power
- **Blind quantum computing**, where a remote quantum computer is accessed such that it learns nothing about the performed operation

Quantum Communication & C-DOT

सी-डॉट
C-DOT

- Indigenously developed solutions
- QKD system based on COW and DPS protocols
- PQC IP Encryptor based on NIST algorithm

QKD/PQC

- Alliance for collaborative development of quantum communication technologies
- Academia, start-ups, industries in India can apply

Quantum Alliance

- C-DOT welcomes proposals from academia, start-ups, industries, individual researchers in India to break the security of C-DOT QKD/PQC systems
- INR 10 Lakh award for each break , along with offer to join the C-DOT Quantum Alliance

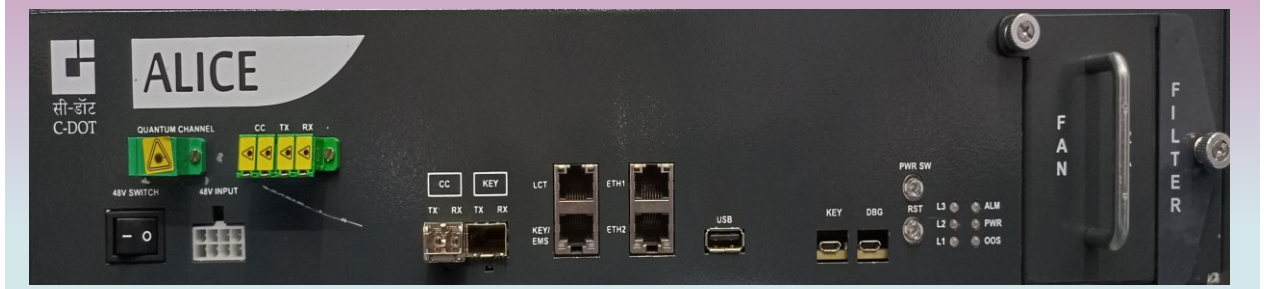
Quantum Hackathon

- C-DOT welcomes proposals for indigenous development of QKD / PQC protocols/algorithms for implementation in indigenous QKD/PQC systems
- Funding will be provided for the selected proposals

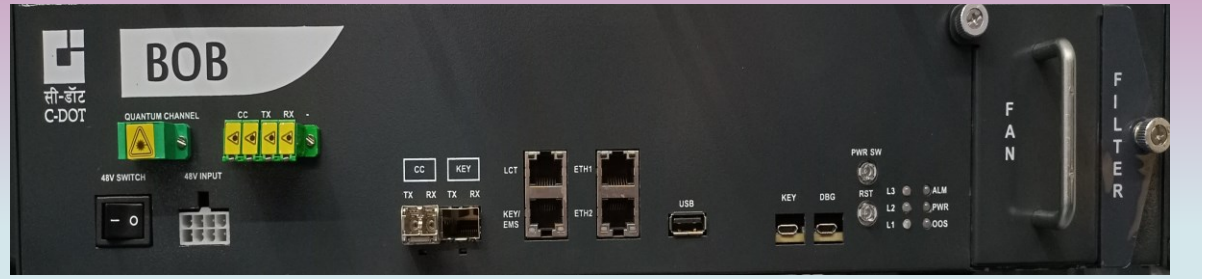
Quantum Protocols

C-DOT's QKD Solution

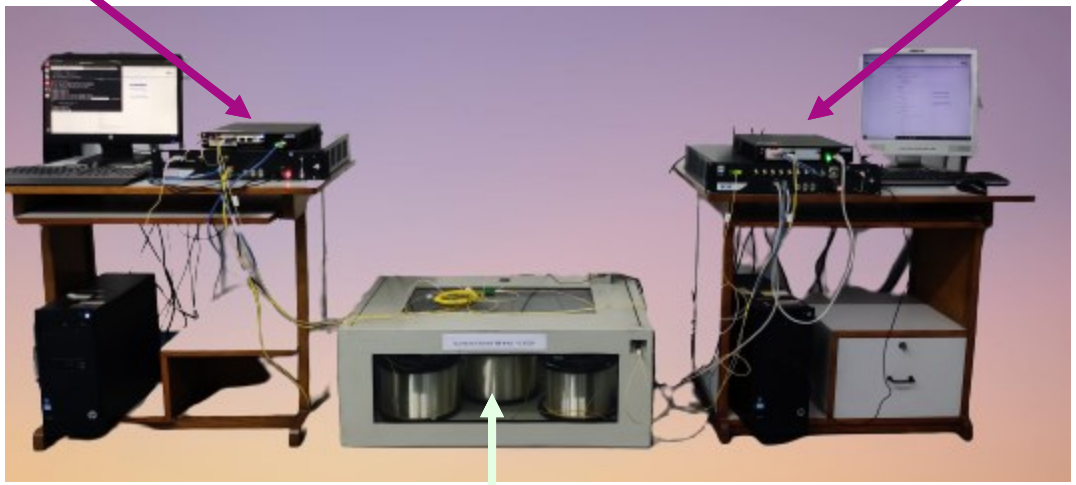
Alice (Transmitter)



Bob (Receiver)



Lab Set Up



Quantum Channel

DPS+COW QKD Protocols

C-DOT's PQC Solution

- PQC uses different hard-to-compute mathematical complex problems as foundation to cryptography so that it is resilient to Quantum Attacks

PQC-based IP-layer Encryptor

Phone

Summary

- The security of data being transported by telecom networks is under threat by rapid advancements in the area of Quantum Computing
- Large scale deployment of 5G Networks will further aggravate the security problem – with large number of devices getting connected to the network, industry automation etc. requiring foolproof security
- Quantum communication addresses the issue to provide “Information Theoretic” security
- There is plenty scope of development in terms of novel algorithms, standardised solutions allowing multi-vendor interoperability
- Global investment trends, market forecast and rapid technological development portray a bright future for quantum technologies in the years to come

सी-डॉट
C-DOT

THANK YOU

Centre for Development of Telematics
www.cdot.in

C-DOT Campus, Mandi Road
New Delhi-110030, India