Development of Security and Resilience for 6G Potential Cryptography Based on Quantum Key Distribution (QKD) and Quantum Error Correction (QECC): QuTech-6G

Khoirul Anwar

Director, The University Center of Excellence for Advanced Intelligent Communications (AICOMS), Telkom University, Bandung, Indonesia
Vice-Chair of Asia-Pacific Wireless Group (AWG), Bangkok, Thailand 2018—2025
Research Collaboration of Quantum Technology (PKR Kuantum 2.0)
Beyond 5.5G Laboratory
E-mail: anwarkhoirul@telkomuniversity.ac.id

Presented at ASEAN IVO FORUM 2024
Phnom Penh, Cambodia, 6 November 2024

Project Title: Development of Security and Resilience for 6G Potential Cryptography Based on Quantum Key Distribution (QKD) and Quantum Error Correction (QECC): QuTech-6G

Background :

- The current telecommunication generation is towards 5G-Advanced and 6G
- On June 7, 2024, the United Nations proclaimed 2025 as the International Year of Quantum Science and Technology (IYQ).
- Many future possible applications, which are not supported by the classical technology.

unesco

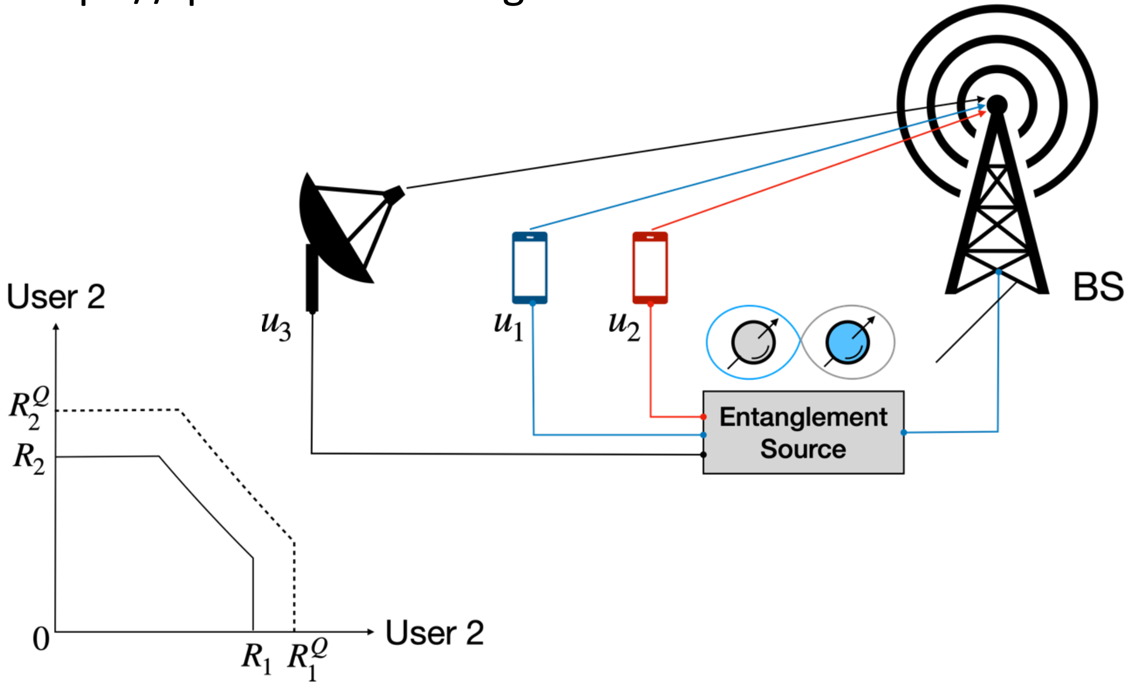
INTERNATIONAL YEAR OF
Quantum Science
and Technology

100 years of quantum is just the beginning...

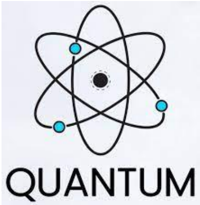
https://quantum2025.org

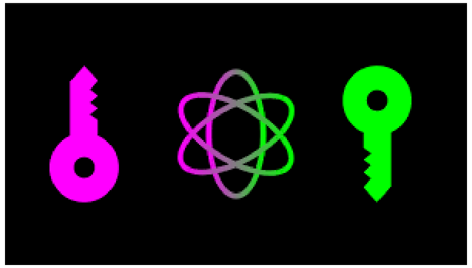
Targets:

- This project continues on the development of PATRIOT-Net with focus on the emerging technology of quantum for 5G-Advanced and 6G
- Patent and publications for prototyping real-field parameters in high reputed IEEE magazines or similar.
  - Conference: 3,
  - Patent: 2
  - Journal: 3



Roadmap of Quantum Technology for 6G





ASEAN IVO Y5-Y6 (Expected):
MCRBS V (AI+Quantum) Becomes 6G

ASEAN IVO Y4 (Expected):
MCRBS IV (AI+Quantum) and UAV with Autonomous System for logistics

ASEAN IVO Y3 (Expected):
MCRBS III (AI) and UAV with Autonomous System

ASEAN IVO Y2:
MCRBS II and UAV over Cellular

ASEAN IVO Y1:
Coding and MCRBS

2019-2020

2021-2022

2023-2025

2026-2028

2028-2030

5G

5G ADVANCED

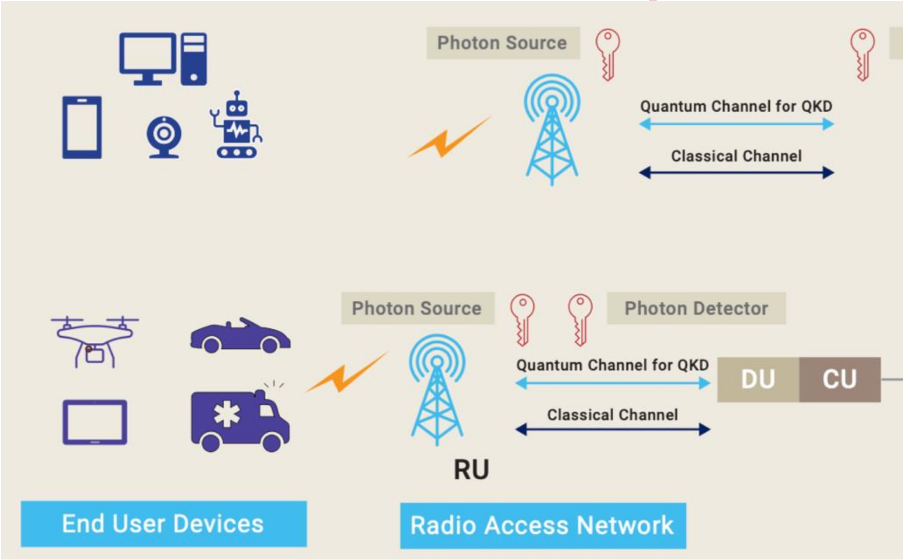


image: NEXTG Alliance, 2022.

Roadmap of Quantum Technology for 6G

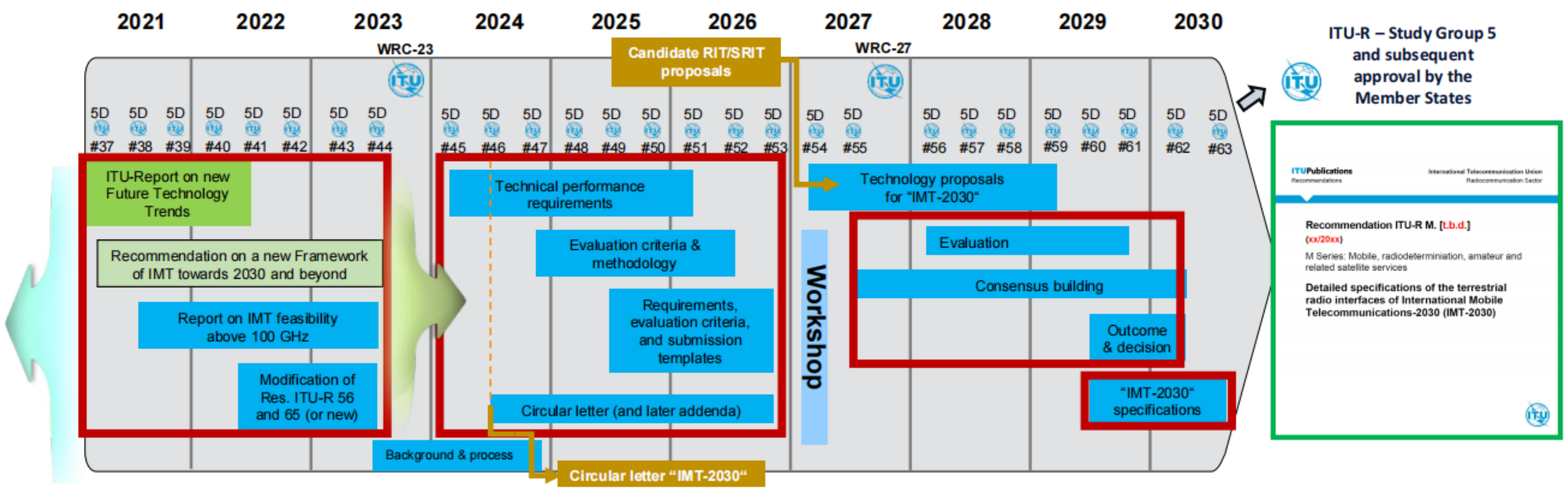
ASEAN IVO

⟨PKR|KUANTUM⟩
Pusat Kolaborasi Riset
Teknologi Kuantum 2.0
(Research Collaboration Center for Quantum Technology 2.0)

BADAN RISET DAN INOVASI NASIONAL – INSTITUT TEKNOLOGI BANDUNG – TELKOM UNIVERSITY

BRIN · Telkom University

2022	2023	2024	2025	2026	2027
PKR Year 1	PKR Year 2	PKR Year 3	PKR Year 4 ASEAN IVO Year 1	PKR Year 5 ASEAN IVO Year 2	PKR year 6 ASEAN IVO Year 3
QECC 5 qubits QECC 12 qubits Quantum Machine Learning	QKD BB84	QKD E91 QML High order modulation	Lab Prototype	Outdoor Experiment	Balloon/HAPS Experiment



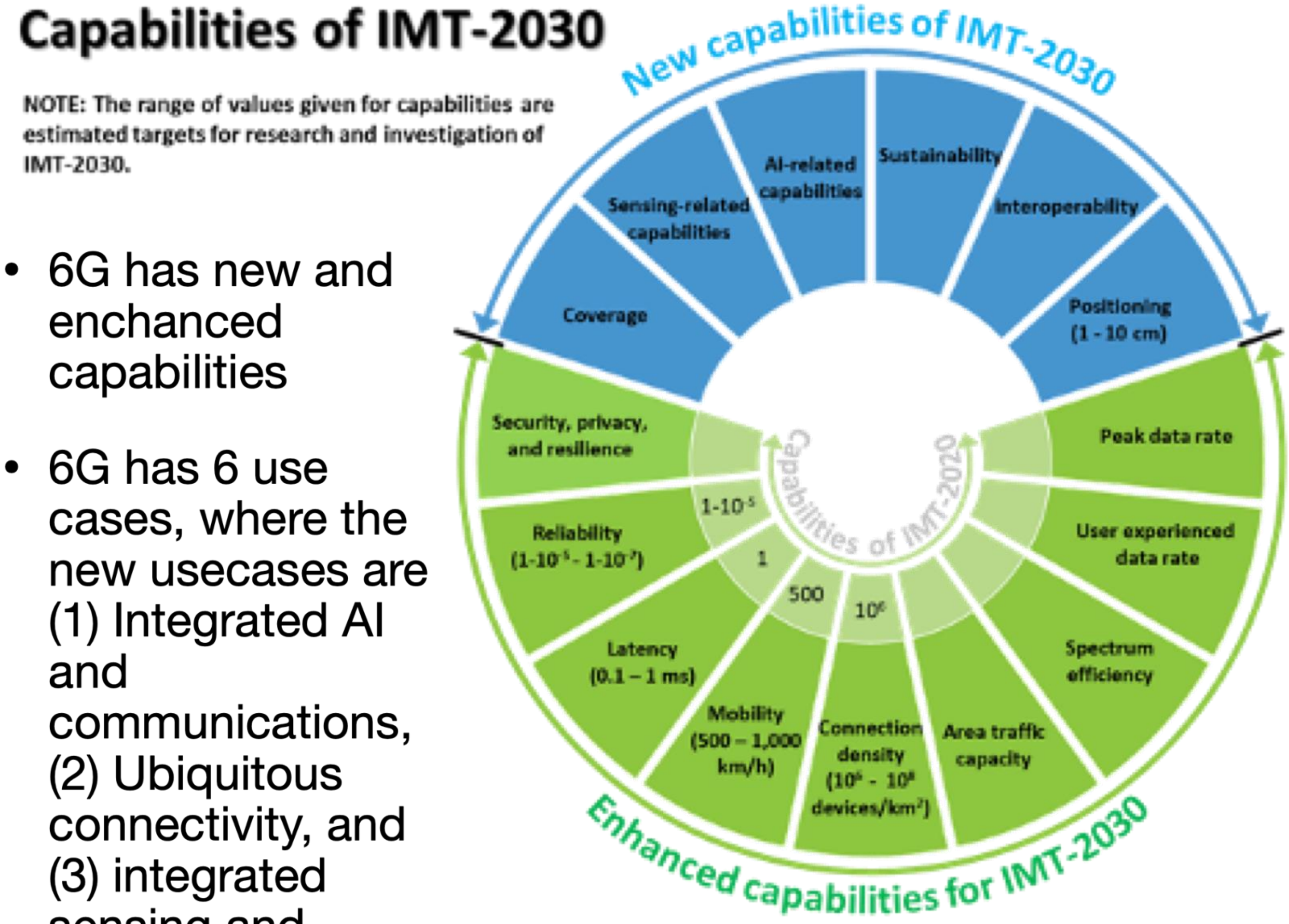
Note 1: WP 5D #59 will additionally organize a workshop involving the Proponents and registered Independent Evaluation Groups (IEGs) to support the evaluation process

Note 2: While not expected to change, details may be adjusted if warranted. Content of deliverables to be defined by responsible WP 5D groups

Framework → **Requirements and Evaluation criteria** → **Evaluation and Consensus building** → **Specification** → **Approval**

- The work on quantum technology for 6G was started in 2022 with funding from Indonesia PKR.
- Started from 2025, we expect larger funding with more significant results.
- The results are expected inline with the timeline of ITU standardization.

New Capabilities and Use Scenario in 6G



- 6G has new and enchanced capabilities
- 6G has 6 use cases, where the new usecases are (1) Integrated AI and communications, (2) Ubiquitous connectivity, and (3) integrated sensing and communications.

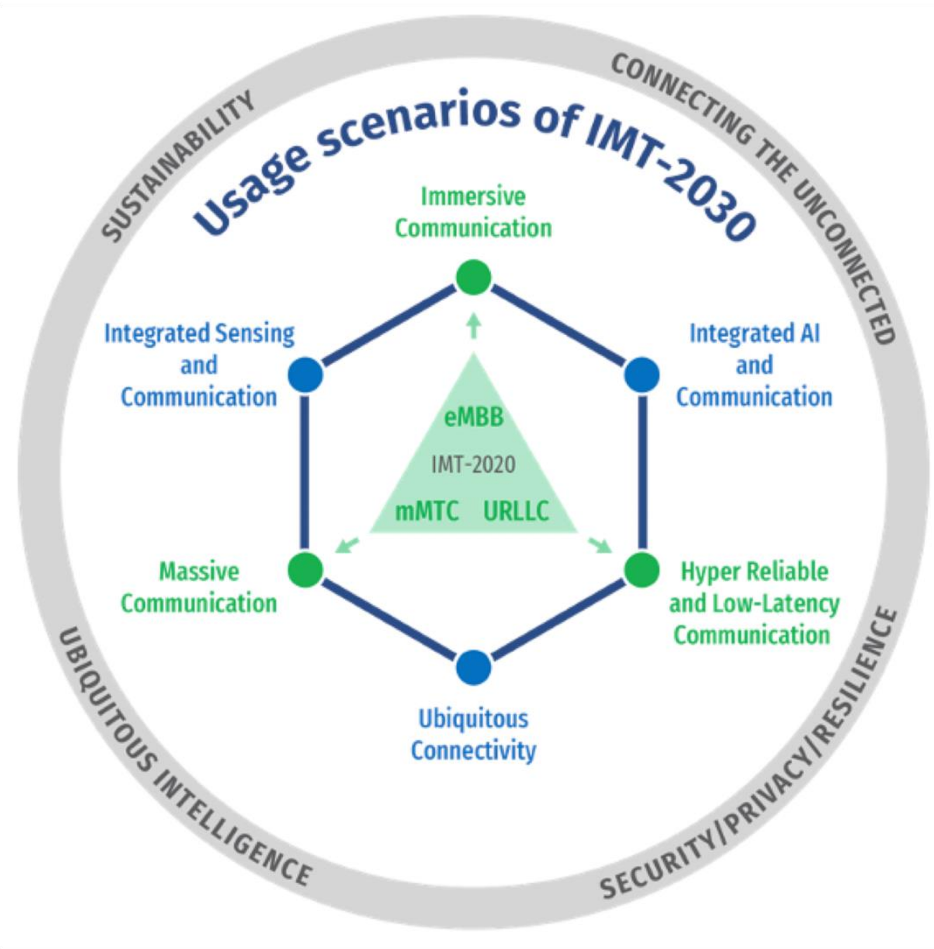
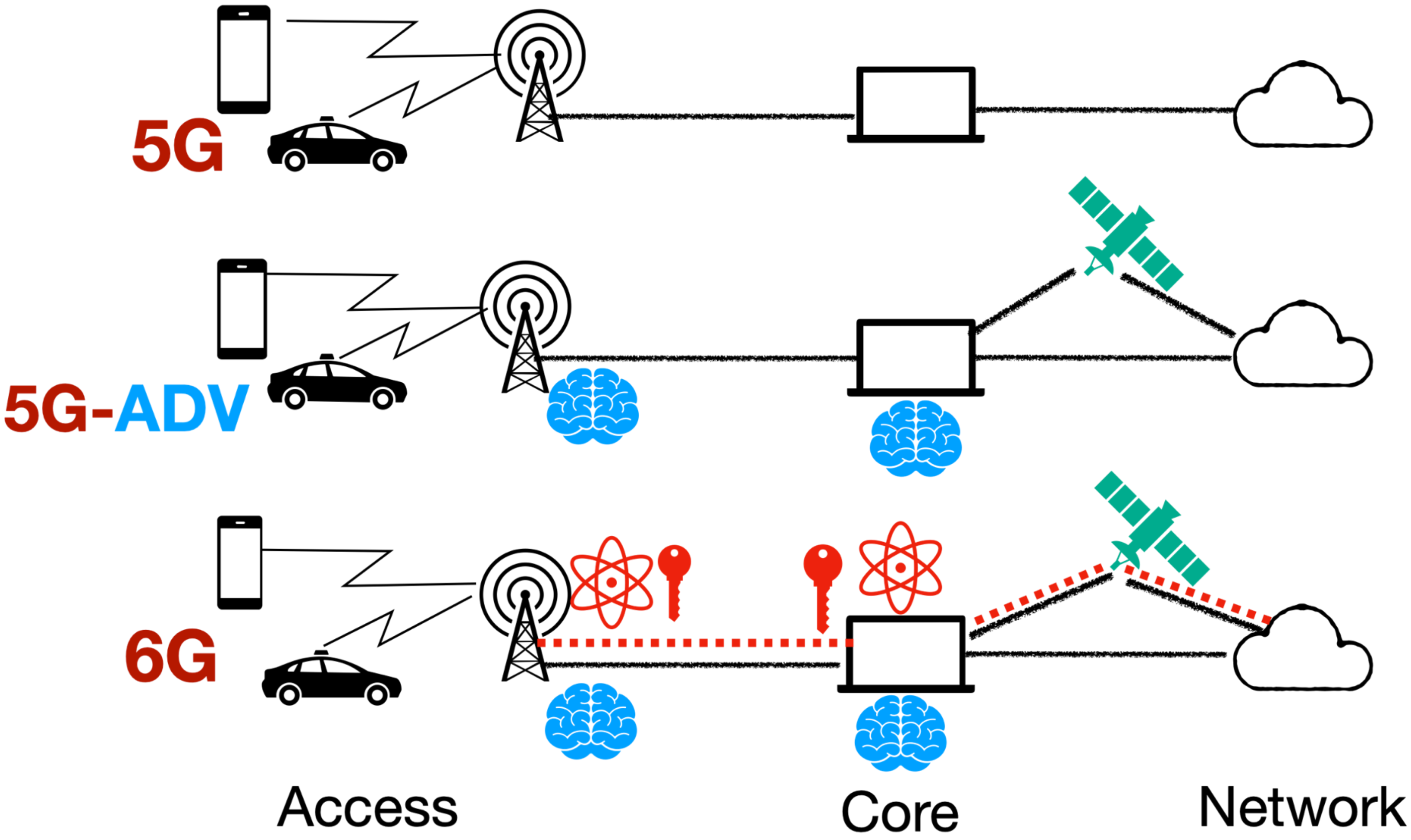


Image: ITU, WP5D

Evolution of 5G to 6G and Quantum Technology with Respect to RAN

- 5G-Advanced has uniqueness on the artificial intelligence (AI)
- 6G has uniqueness on the AI and Quantum cryptography.
- Quantum Technology with respect to RAN:
  - Physical layer processing of the user data plane in the RAN (quantum Fourier transform and quantum linear solver)
  - Clustering for automatic anomaly detection in network design optimization (quantum K-means algorithm)
  - Prediction of the quality of user experience for video streaming based on device and network level metrics (quantum support vector machine)
  - Database search at the data management layer (Grover's algorithm)



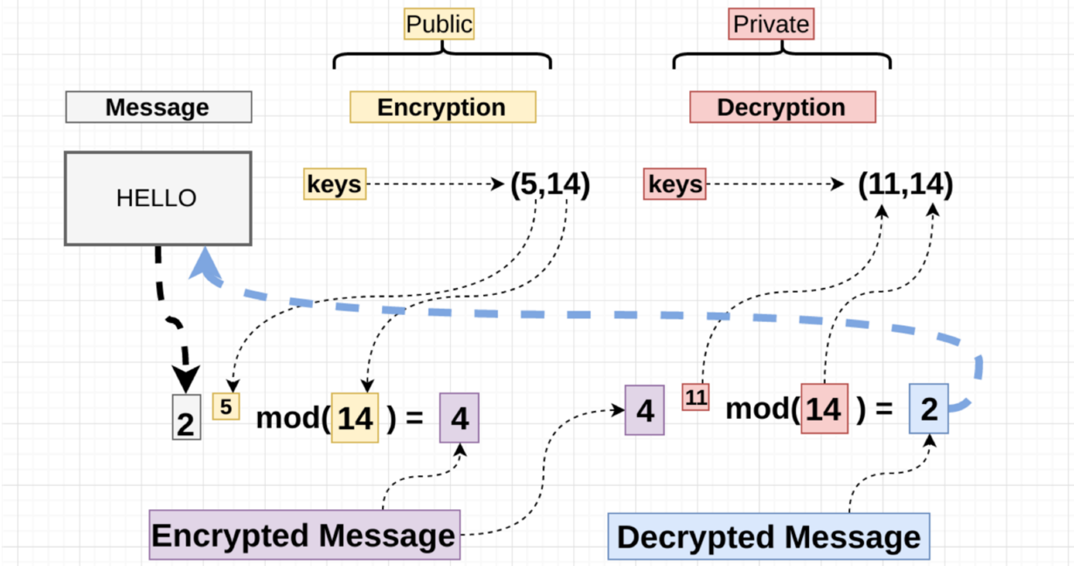
The Important of Quantum Security

Method	$n = 128$	$n = 128$	$n = 1024$	$n = 1024$
BF	$1.8 \cdot 10^{7}$ s	0.58 year	$1.3 \cdot 10^{142}$ s	$4 \cdot 10^{134}$ year
BC	$6 \cdot 10^{-4}$ s	$1.9 \cdot 10^{-11}$ year	$3.5 \cdot 10^{8}$ s	11.29 year
G	$4 \cdot 10^{-3}$ s	$1.3 \cdot 10^{-10}$ year	$1.1 \cdot 10^{65}$ s	$3.7 \cdot 10^{57}$ year
S	$2 \cdot 10^{-5}$ s	$6.6 \cdot 10^{-14}$ year	**0.01** s	$3.4 \cdot 10^{-11}$ year

Name	function	pre-quantum security level	post-quantum security level
Symmetric cryptography			
AES-128 [1]	block cipher	128	64 (Grover)
AES-256 [1]	block cipher	256	128 (Grover)
Salsa20 [2]	stream cipher	256	128 (Grover)
GMAC [3]	MAC	128	128 (no impact)
Poly1305 [4]	MAC	128	128 (no impact)
SHA-256 [5]	hash function	256	128 (Grover)
SHA-3 [6]	hash function	256	128 (Grover)
Public-key cryptography			
RSA-3072 [7]	encryption	128	broken (Shor)
RSA-3072 [7]	signature	128	broken (Shor)
DH-3072 [8]	key exchange	128	broken (Shor)
DSA-3072 [9, 10]	signature	128	broken (Shor)
256-bit ECDH [11, 12, 13]	key exchange	128	broken (Shor)
256-bit ECDSA [14, 15]	signature	128	broken (Shor)

Image: D. J. Bernstein, "Post-Quantum Cryptography", 2021.

- For breaking the cryptography of RSA or related technique, the Grover's algorithm requires only $\frac{\pi}{4}\sqrt{\sqrt{N}} \approx 25$ iterations. However, Shor's Algorithm does better.

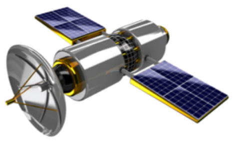


5–25 years

10 years

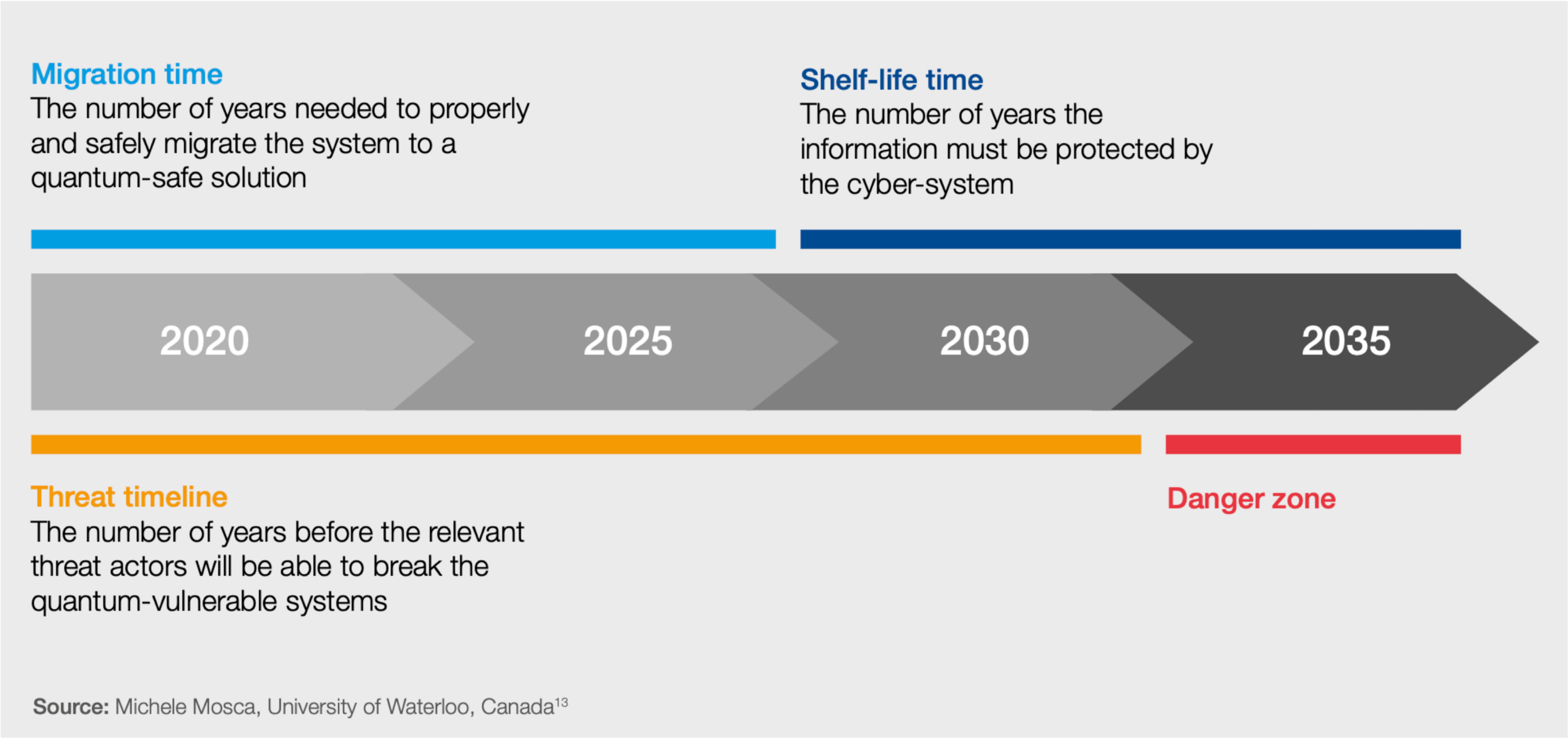
10–30 years

> 20 years



Some devices are hard to update

The Important of Quantum Security



The Proposed Quantum QKD Testing in Bandung: Expecting more collaboration

⟨PKR|KUANTUM⟩

Pusat Kolaborasi Riset

Teknologi Kuantum 2.0

(Research Collaboration Center for Quantum Technology 2.0)

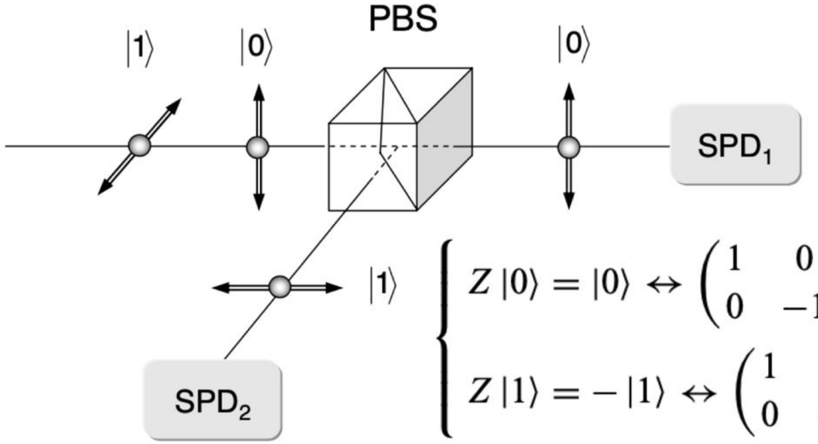
BADAN RISET DAN INOVASI NASIONAL – INSTITUT TEKNOLOGI BANDUNG – TELKOM UNIVERSITY

BRIN BADAN RISET DAN INOVASI NASIONAL

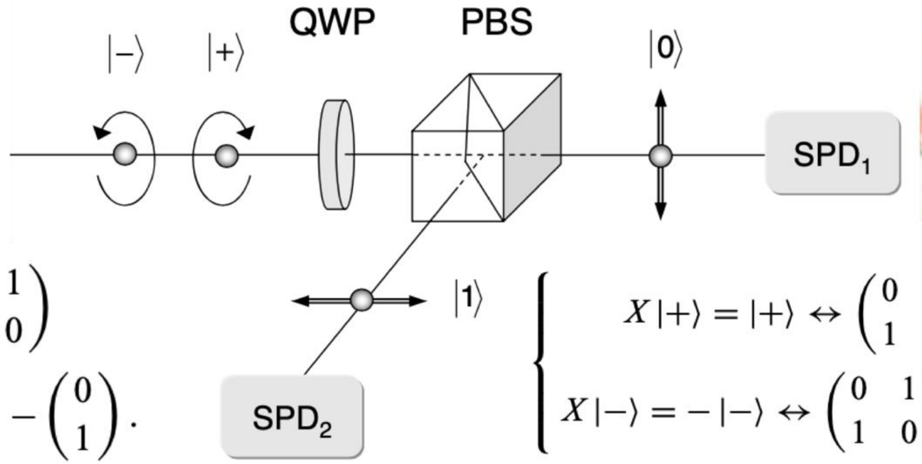
Telkom University

JL. GANESHA NO. 10, LABTEK V, BANDUNG 40132, INDONESIA

Collaboration with ITB and BRIN



$$\begin{cases} Z|0\rangle = |0\rangle \leftrightarrow \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} \\ Z|1\rangle = -|1\rangle \leftrightarrow \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = -\begin{pmatrix}0\\1\end{pmatrix}. \end{cases}$$



$$\begin{cases} X|+\rangle = |+\rangle \leftrightarrow \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \\ X|-\rangle = -|-\rangle \leftrightarrow \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = -\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}. \end{cases}$$

The Proposed Quantum QKD Testing in Bandung: Expecting more collaboration

- QKD is still growing with many new ideas
- We have categorized them into 8 groups
- We can start from the simple one and practical one.
- Collaborations are required.

Table 2: Some QKD techniques for possible application in 6G.

QKD	Principle	Strength
BB84	(Bennett and Brassard, 1984) [17] is based on quantum states of single photons using two sets of bases (rectilinear and diagonal) and relies on the no-cloning theorem.	High security; fundamental basis for most QKD systems
E91	(Ekert, 1991) [18] is based on quantum entanglement, where the security is guaranteed by the violation of Bell's inequality.	Strong security based on entanglement and Bell's theorem.
B92	(Bennett, 1992) [19] is a simplified version of BB84 by using only two non-orthogonal quantum states relying on the inability of an eavesdropper to perfectly distinguish between the two non-orthogonal states.	Simpler with fewer states, still highly secure.
SARG04	(Scarani, Acin, Ribordy, and Gisin, 2004) [20] improves security against photon-number-splitting (PNS) attacks on weak coherent states.	Improved security over long distances and against PNS attacks.
Decoy-State	Decoy State Protocol (2004) [21] [22] detects and counteract PNS attacks by randomly sending weaker states mixed with the actual key to prevents eavesdroppers from gaining full knowledge of the key from weak pulses.	Enhanced security against PNS with practical implementations.
CV-QKD	(Continuous Variable QKD, 2002) [23] encodes key in the continuous quadratures (amplitude and phase) of light using homodyne or heterodyne detection techniques.	Efficient integration with telecom systems, continuous variable encoding.
MDI-QKD	(Measurement Device-Independent QKD, 2012) [24] eliminates vulnerabilities in the detectors by using an untrusted third party who measures them but cannot gain information about the key.	Immunity to all detection-based attacks, more practical for real-world.
Twin-Field	Twin-Field QKD (2018) [25] is a recent breakthrough in QKD that significantly extends the transmission distance by combining the principles of phase-matching and MDI-QKD allowing longer distances.	Extended transmission distance, practical for long-range QKD networks.

K. Anwar, "Quantum Error Correction, Quantum Cryptography, and Quantum Machine Learning Towards IMT-2030 (6G)", ICPTAM 2024, Bali, Indonesia, Oct. 2024

Types of Error in Quantum Computing and Communications

Explicitly, **I** is an identity operator, or merely a repeat gate, which leaves the state $|\psi\rangle$ intact, as shown below:

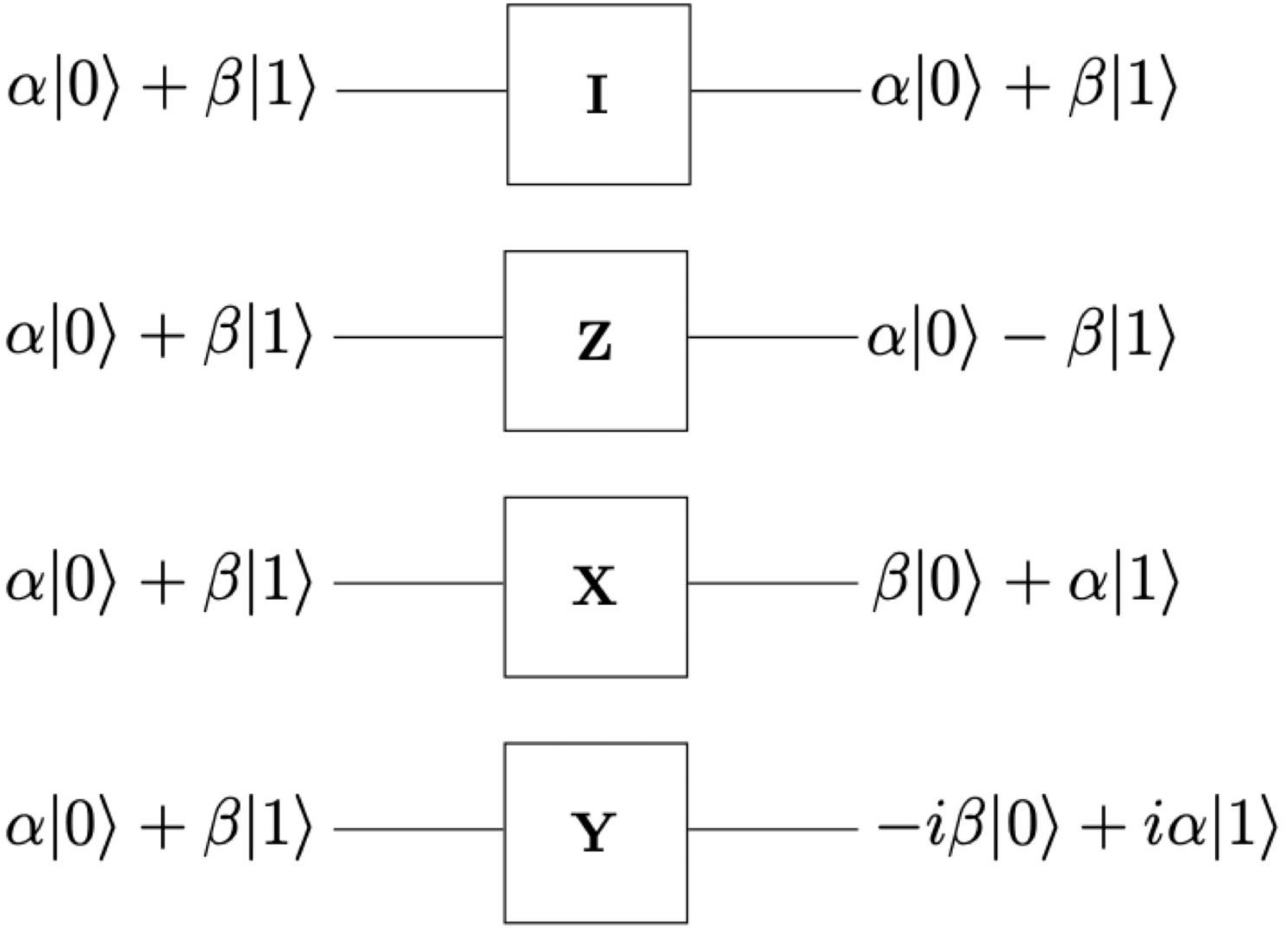
$$\mathbf{I}|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \equiv \alpha|0\rangle + \beta|1\rangle. \quad (20)$$

The operator **Z** is a phase-flip operator, which acts as:

$$\mathbf{Z}|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} \equiv \alpha|0\rangle - \beta|1\rangle, \quad (21)$$

while **X** is a bit-flip operator analogous to the classical NOT gate, which yields:

$$\mathbf{X}|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \equiv \beta|0\rangle + \alpha|1\rangle. \quad (22)$$



The Proposed Quantum Error Correction Codes

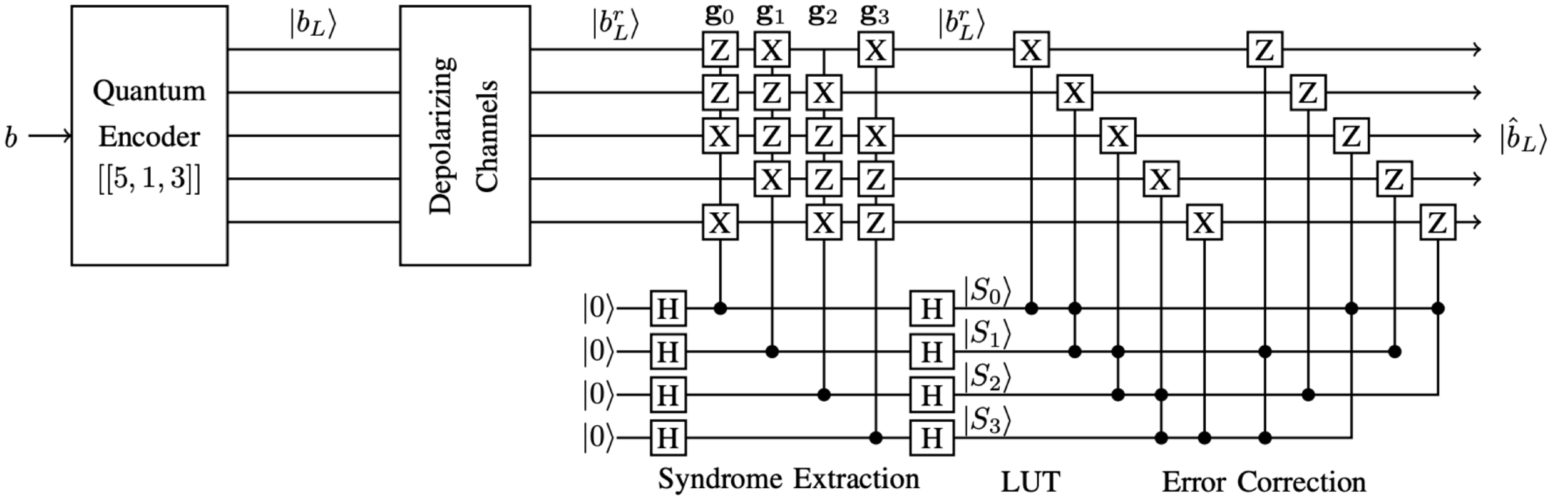
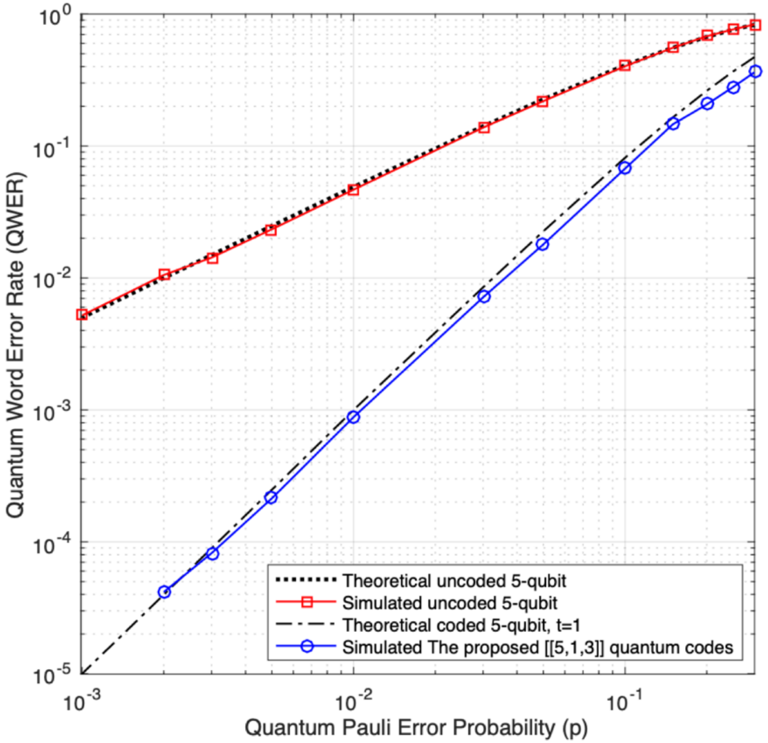


Fig. 3. The quantum circuit of the proposed perfect [[5, 1, 3]] quantum accumulate codes.



The Smallest Perfect Quantum Accumulate Codes

Khoirul Anwar and Mujib Ramadhan
The University Center of Excellence for Advanced Intelligent Communications (AICOMS),
School of Electrical Engineering, Telkom University
Jl. Telekomunikasi No. 1, Terusan Buah Batu, Bandung, 40257 INDONESIA
E-mail: {anwarkhoirul@, mujibramadhan@student.}telkomuniversity.ac.id

***Abstract*—Quantum has many unique characteristics for future applications, e.g., secure communications using quantum key distribution (QKD) in the sixth telecommunication generation (6G) 2030 based on the non-cloning principle and quantum teleportation. However, quantum communications are still vulner-**

Decoherence appears due to the interaction of qubits with environments that blur the superposition states. The decoherence introduces errors three types of Pauli errors. It suggests that the quantum states should be sufficiently isolated from

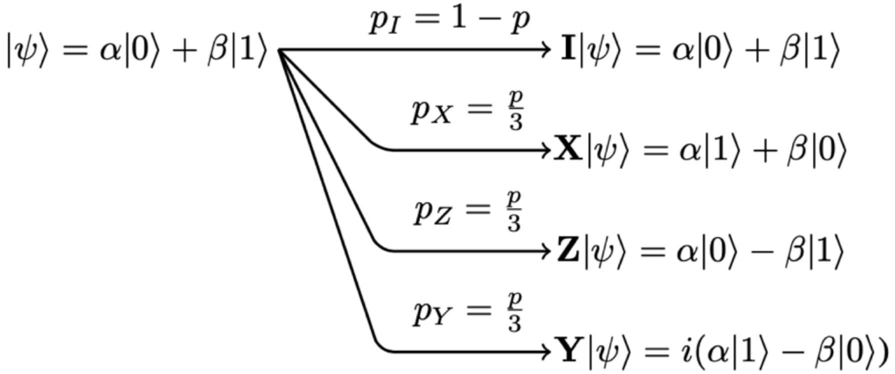
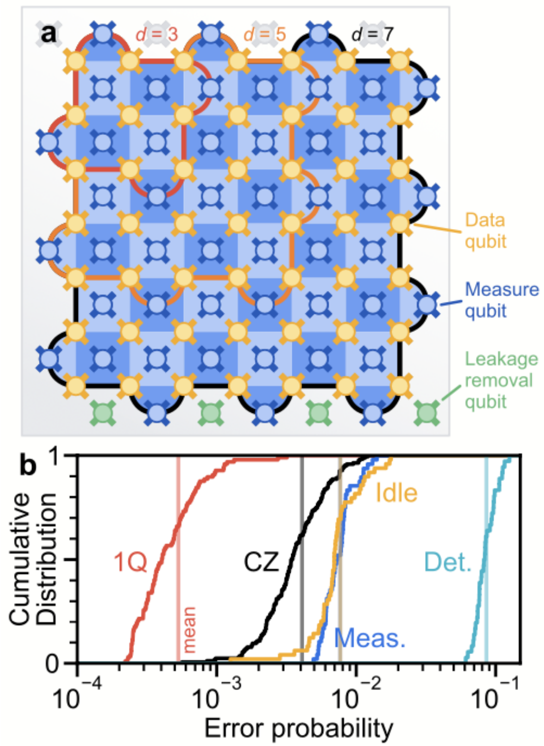
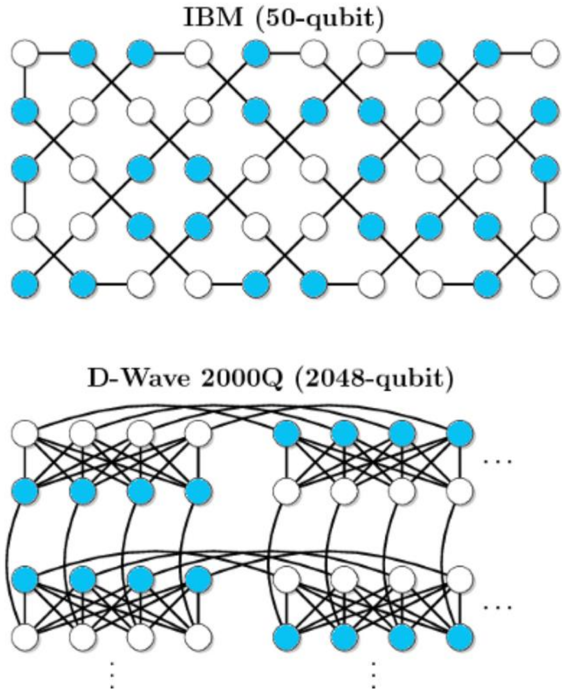


image: K. Anwar, invited paper in IEEE APCC 2021.

The Challenges on Quantum Error Correction Codes

- Google Quantum AI demonstrated (in 2024) a quantum memory (with the help of QEC) can operates below the threshold.
- The surface code is one of the most promising error correction codes for quantum computing, known to have a threshold around 1%. (It is said effective if the system experiences errors at a rate lower than 1%).
- The QECC helps the quantum memory of logical qubits last 2.4 times longer than any physical qubit.
- Distance d=5, 72 qubits, error suppression factor
- Distance d=7, 105 qubits,
- **Challenge: d=27, 1457 qubits, BER of 10^{-6}.**





Quantum error correction below the surface code threshold

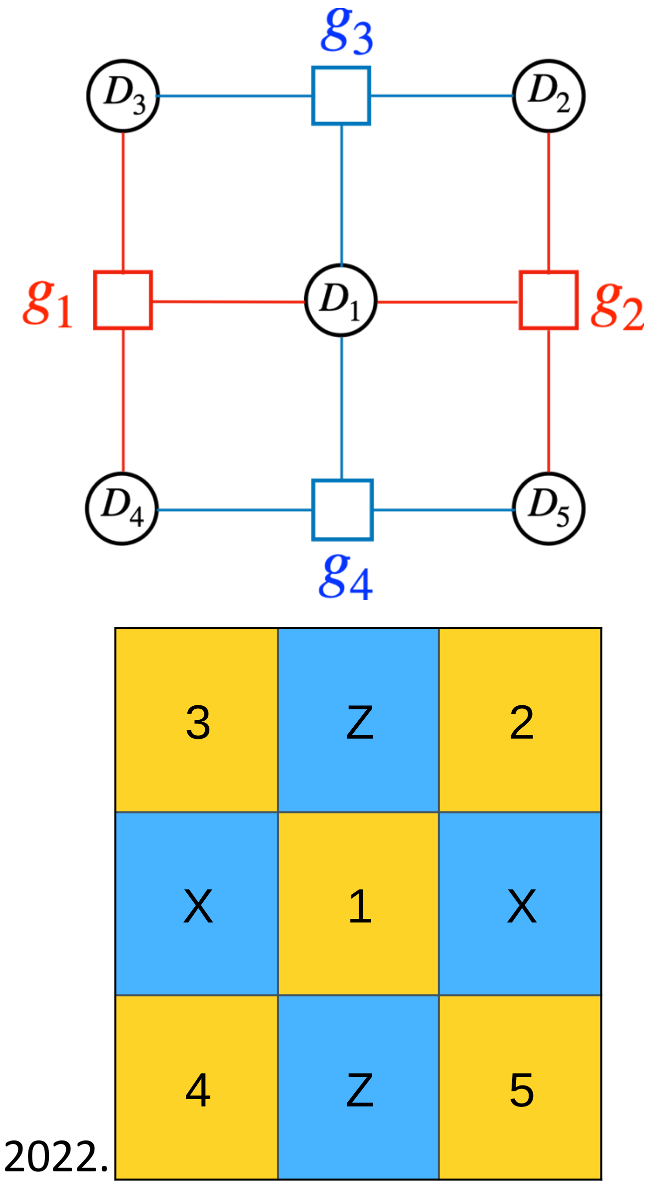
Google Quantum AI and Collaborators
(Dated: August 27, 2024)

Quantum error correction [1–4] provides a path to reach practical quantum computing by combining multiple physical qubits into a logical qubit, where the logical error rate is suppressed exponentially as more qubits are added. However, this exponential suppression only occurs if the physical error rate is below a critical threshold. In this work, we present two surface code memories operating below this threshold: a distance-7 code and a distance-5 code integrated with a real-time decoder. The logical error rate of our larger quantum memory is suppressed by a factor of $\Lambda = 2.14 \pm 0.02$ when increasing the code distance by two, culminating in a 101-qubit distance-7 code with $0.143\% \pm 0.003\%$ error per cycle of error correction. This logical memory is also beyond break-even, exceeding

Image: Google AI

Proposed WP

WP1: Coordination
WP2: QKD Development
WP3: Quantum RAN Algorithm: QECC Surface Codes
WP4: Quantum RAN Algorithm: QECC Non-Surface Codes
WP5: Quantum RAN Algorithm: QML Demodulation
WP6: Lab Experiment for QKD, QECC, QML
WP7: Dissemination and Workshop



Conclusions

- Quantum technology is emerging technology that provide many aspects, which are unavailable in classical technology.
- The proposed improvement is on:
  - Upgrade to 6G with:
    - QKD and
    - Quantum Error Correction:
      - Surface codes
      - Non-Surface Codes
    - Quantum Machine Learning
- We need your contributions.

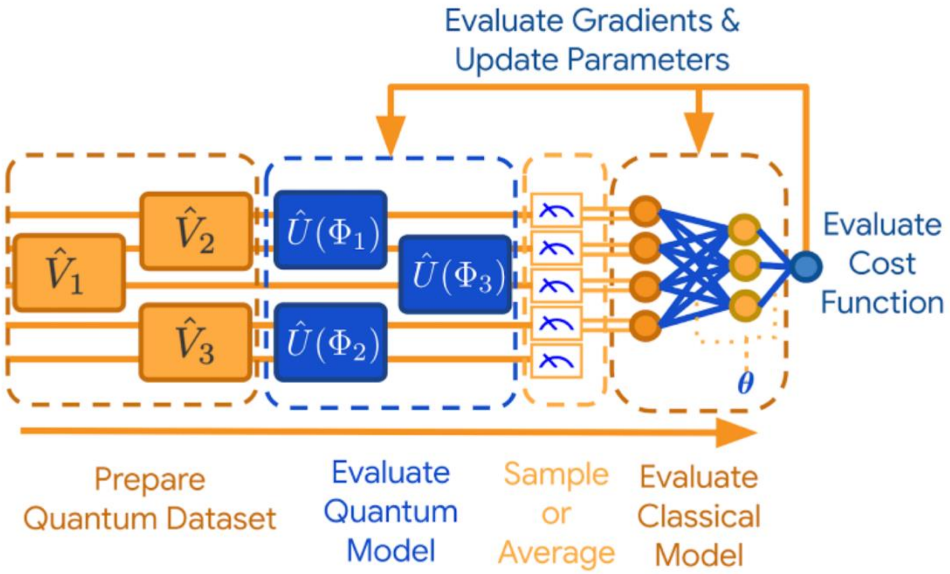


image: Walmsley, IC London

Drug discovery

Drug discovery

Logistics

Logistics