High Entropy Quantum Communication Framework for Secure Key Distribution and Secure Messaging.

Rohit De
Email: de.rohit01@gmail.com
Del Norte High School,
San Diego, California 92127, USA

IARIA INFOCOMP 2022, The Twelfth International Conference on Advanced Communications and Computation
June 26, 2022 to June 30, 2022 - Porto, Portugal

Presenter Biography

Rohit De, is an upcoming Senior student at Del Norte High School, San Diego, California, USA. He is an enthusiastic high schooler interested in computer science, cybersecurity, computational science, engineering, and music (vocal singing). He has continuously pursued various activities on his interests. Some of his achievements are:

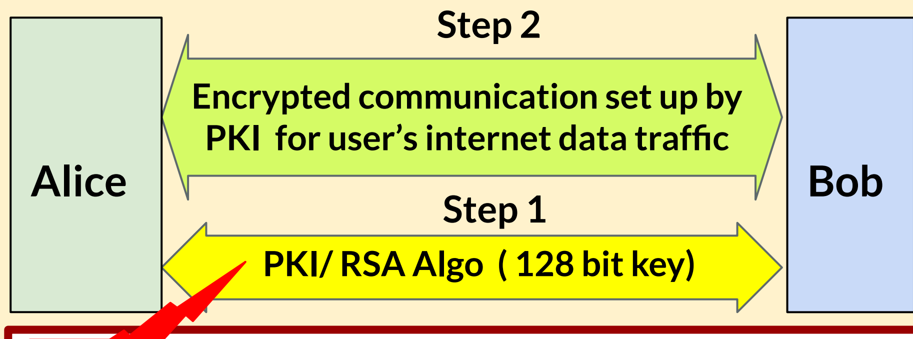
- First Award in Computational Biology at Greater San Diego Science and Engineering Fair, 2022, and “Honorary mention” (5th place) at the California Science and Engineering fair 2022 in Computational Systems category.
- First Award in Computer Science at Greater San Diego Science and Engineering Fair 2021, then selected to present at the California Science and Engineering fair 2021.
- Finalists in the top 500 for 2021 National Cyber Scholarship Competition.
- Consistently in top 1% in North America for Cyberpatriot 2022, 2021, 2020, and 2019, a cybersecurity competition for High School students.
- Presented a poster at 2021 IEEE International Conference on Quantum Computing and Engineering (IEEE QCE21).
- Co-authored a paper in IARIA ICQNM 2020.
- Distinction award in ABRSM level-8 performance grade on vocal singing

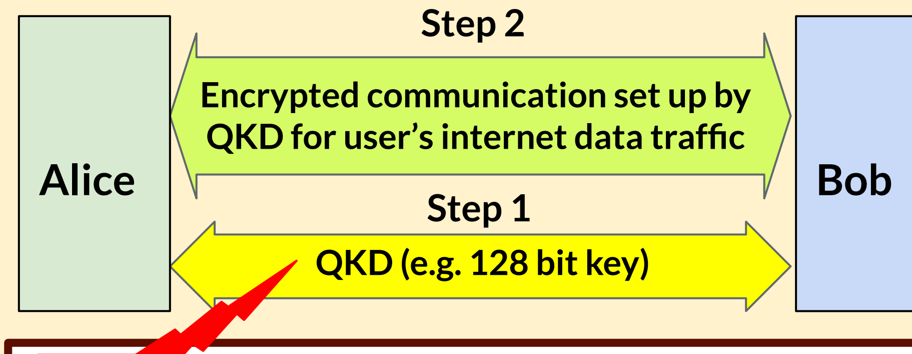
Rohit is interested to pursue college in Engineering and Computer Science after completing high school

Outline of the presentation

- Introduction: Impact of quantum computing and communications on Cybersecurity
- Prior research works used as foundation for this work
- The new method in this paper called HRB (Hopping, Reorder, Basis)
- Simulation Results
- Conclusion and Future work

Cyber attack scenario in the context of quantum computing & communication.



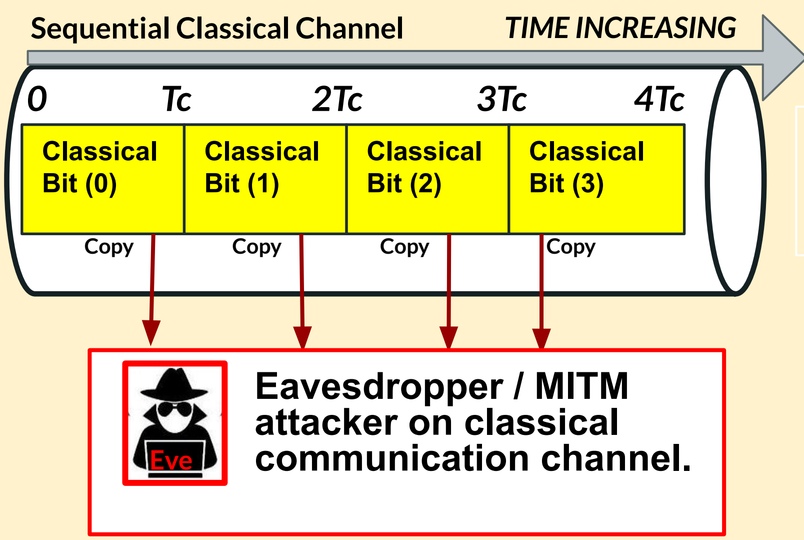


Eve

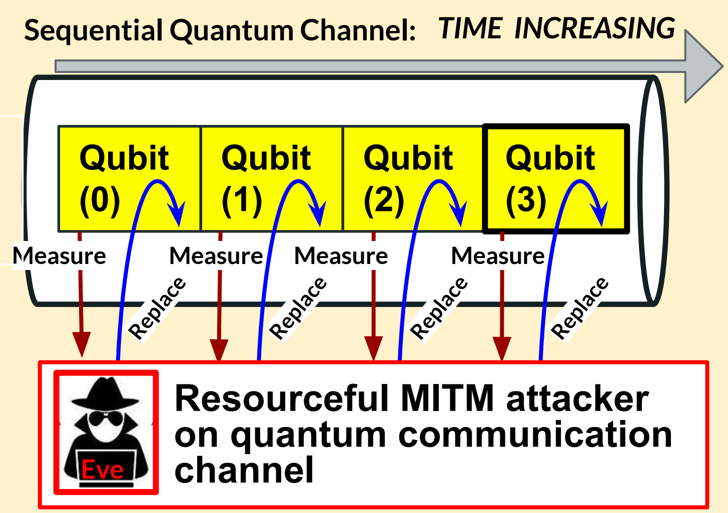
MITM attacker or eavesdropper can stealthily read, copy and store the transmitted bits and then do offline brute force analysis. Computation power of quantum computing is exploited to break classical security schemes such as Public Key Infrastructure (PKI) using Shor's algorithm to find the prime factors for RSA encryption many orders faster.

Eve

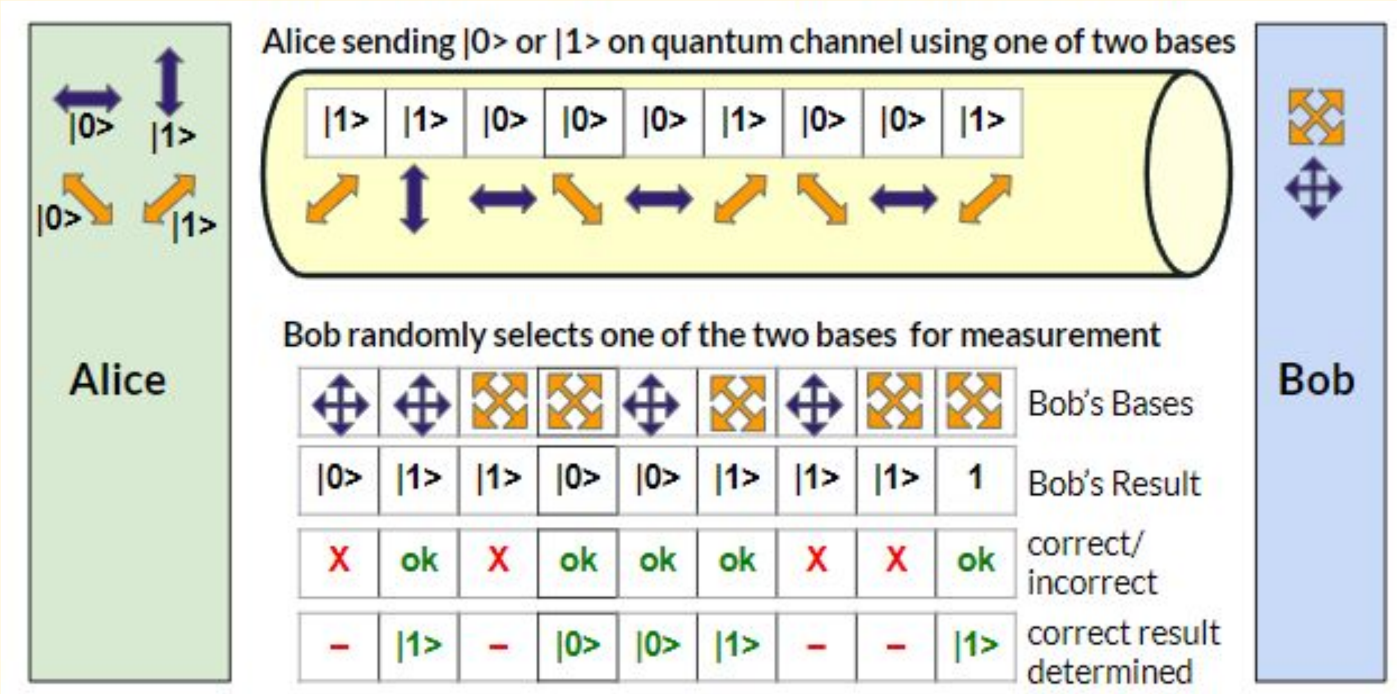
Quantum key distribution (QKD) leverages the 'no-cloning' property and lets Bob/Alice detect an eavesdropper or a MITM attacker as qubits collapse from superposition when measured / read. While improving security compared to classical communication, QKD can still be vulnerable from very sophisticated MITM attacks on the quantum channel like intercept/resend faked states, quantum cloning, etc



- **Tq:** qubit time in quantum channel
- **Tc:** bit time in classical channel



Basics of BB84 and DJ-algorithm for Quantum Key Distribution (QKD)

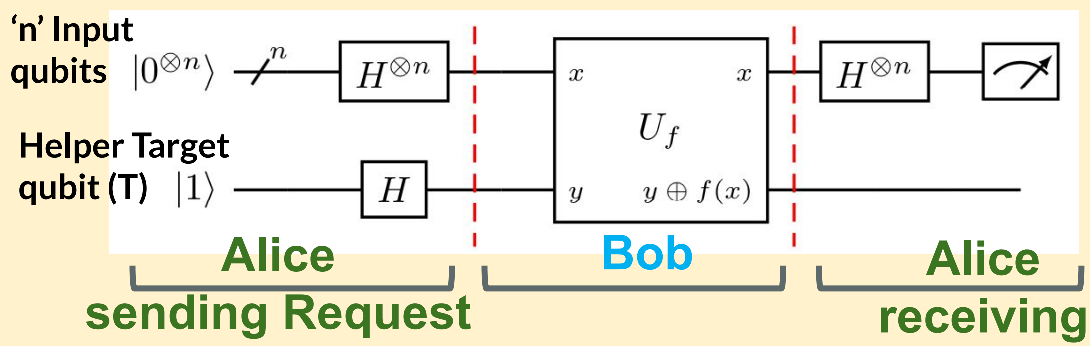


BB84

- Alice randomly selects one of the two different bases (rectangular or diagonal) to transmit |0> or |1>.
- Bob randomly uses one of the two bases for measurement.
- After qubit transmission they share the bases they used (Alice for sending, Bob for measurement).
- If Bob measures a qubit in the same base that Alice sent, the reception is correct.

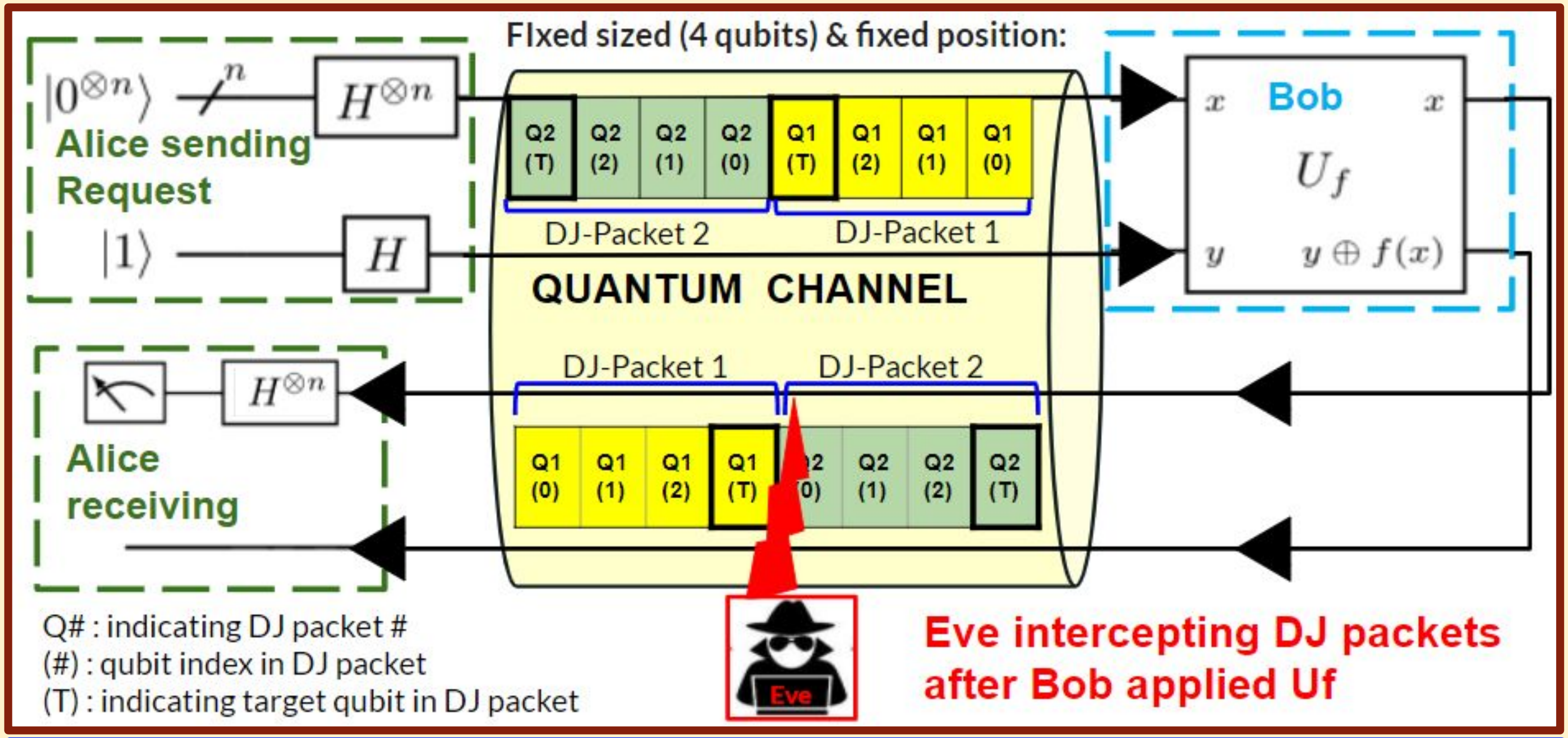
DJ-algorithm finds if an unknown function *'Uf'* is:

- **constant**: for all input possibilities the output is always |0> or always |1>.
- **balanced**: for one half of the inputs the output is |0> and for the other half of the inputs the output is |1>

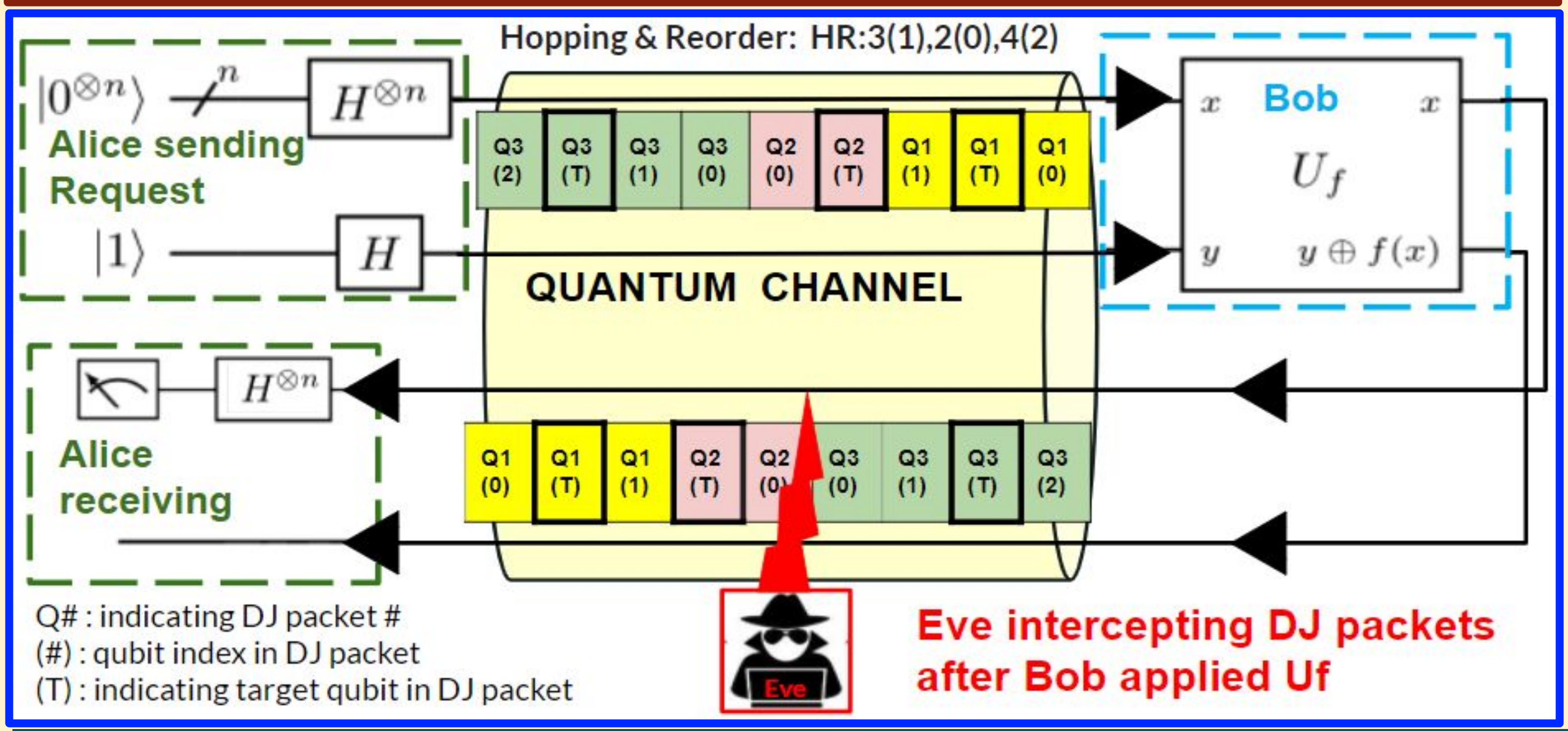


For QKD the DJ-algorithm is split into 3 steps:
(1) **Alice sends request with** |0> initialized 'n' input qubits & |1> initialized helper target qubit (T), that are all superposed, forming a DJ-packet.
(2) **Bob applies *Uf*** (constant or balanced) that updates the DJ-packet and sends back to Alice.
(3) **Alice receives** and measures the DJ-packet to determine type of *Uf* that was applied. This in essence communicates a secret binary value, interpreted as: constant = 0, balanced = 1

Past work on QKD based on DJ-algorithm



Fixed sized DJ-packets with no target qubit reordering.
Throughput = 1/4 secret bit per qubit.
Secrecy = VERY LOW
Easy for Eve to predictively intercept the entire DJ-packet, identify the qubits, determine Uf, and then replace with fresh qubits.
Ref: K. Nagata and T. Nakamura, doi:10.4236/oalib.1101798

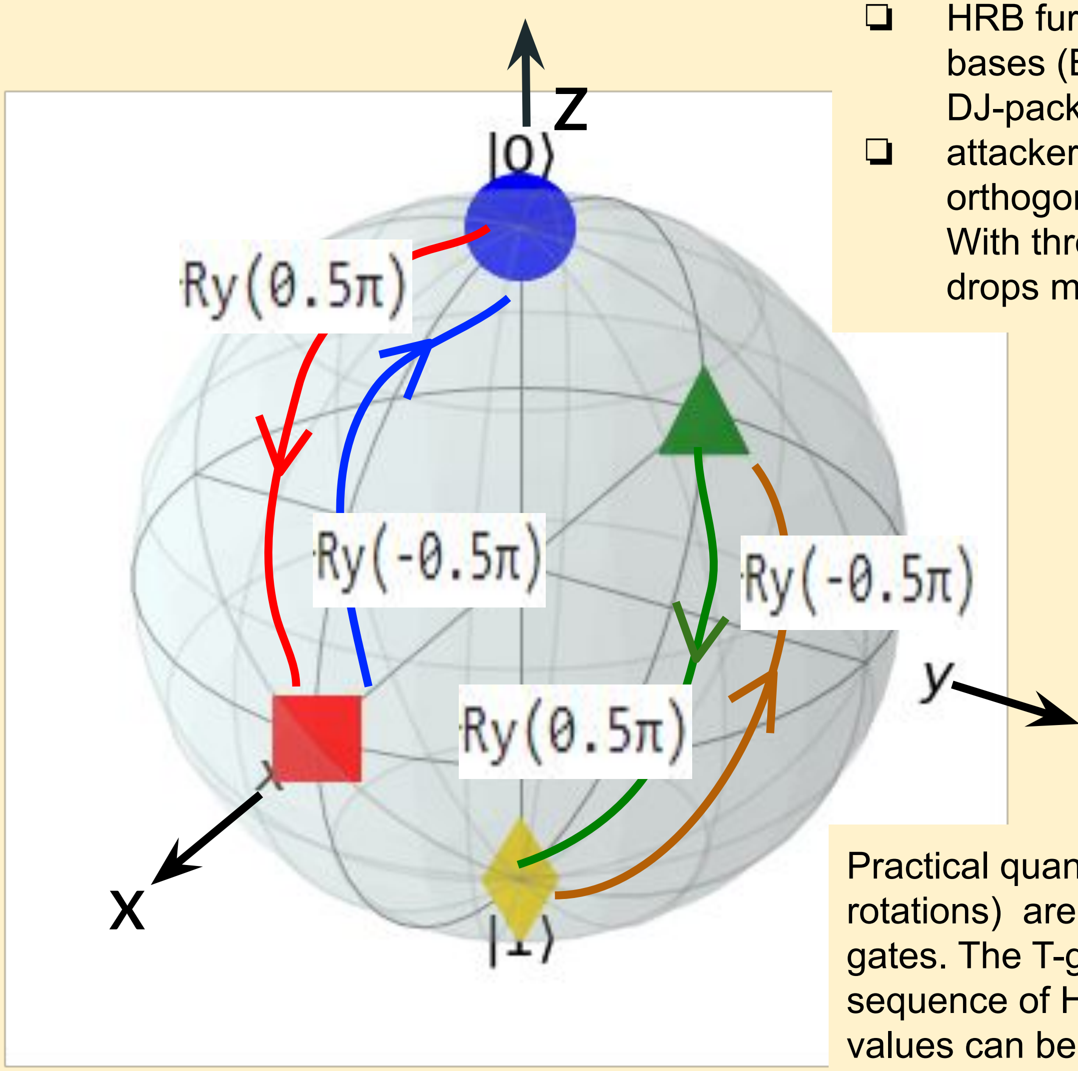


Size Hopping and reordering of target qubit for DJ-Packets.

Throughput = 3/(3+2+4) = 1/3 secret bit per qubit.
Secrecy = HIGH
Ref: R. De, R. Moberly, C. Beery, J. Juybari and K. Sundqvist, IEEE QCE21

The new work: The HRB (Hopping, Reorder, Basis) scheme

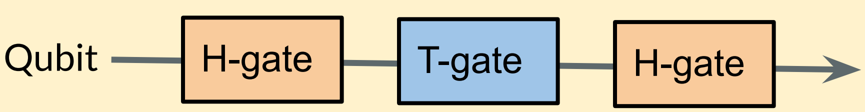
- HRB is an enhancement on the past work by R. De, R. Moberly, C. Beery, J. Juybari and K. Sundqvist, IEEE QCE21

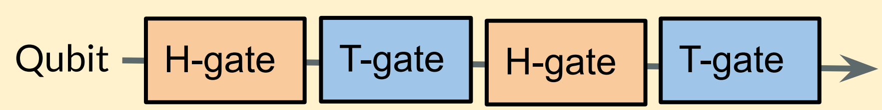


- ❑ HRB further increases the entropy by using multiple orthogonal bases (B) e.g., Z-basis, X-basis, for the different qubits in a DJ-packet, during communication over the quantum channel.
- ❑ attacker's interception success drops 200-times when using two orthogonal bases vs. 12-times in the past work in IEEE QCE21. With three orthogonal bases the attacker's interception success drops more than 1000-times, and Secrecy increases upto 99.98%

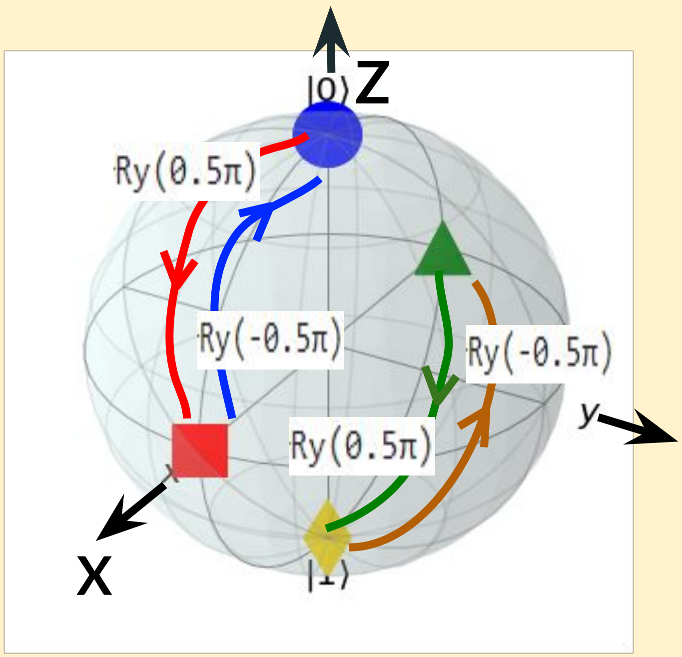
- ❑ |0> and |1> in Z-basis upon rotation about the Y-axis by 0.5*pi radians (90 degree) become the |+> and the |-> in the X-basis.
- ❑ To recover the qubits into Z-basis values a rotation of the qubits by -0.5*pi radians (-90 degree) about the Y-axis is needed.

Practical quantum hardware realization for the basis change (through rotations) are possible using a combination of Hadamard (H) and T gates. The T-gate is a rotation around the z-axis by pi/4 radians. With a sequence of H and T gates, a single-qubit gate rotation of various angle values can be set-up around an arbitrary axis in the Bloch sphere





The new work: The HRB scheme options and details



***Option (i)*: Uses same basis for all the qubits in the same DJ-packet, but different DJ-packets in the same hopping sequence can use different basis.**

Q1 (0, B0)	**Q1 (T, B0)**	**Q1 (1,B0)**	**Q2 (0, B1)**	**Q2 (1, B1)**	**Q2 (2, B1)**	**Q2 (T, B1)**	**Q2 (3,B1)**

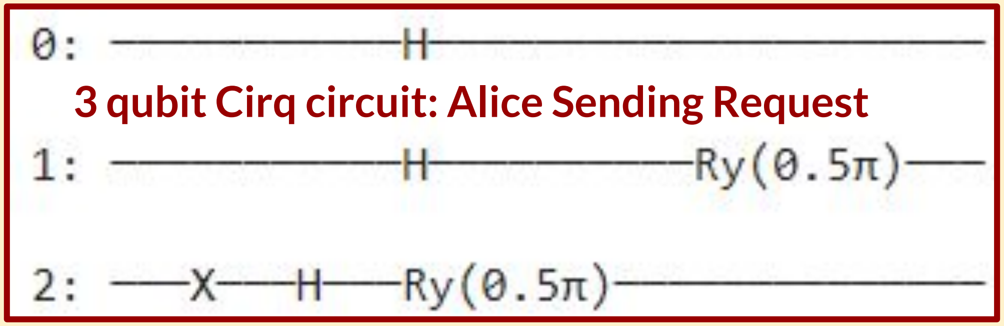
Hopping Sequence HRB:3(1,B0),5(3,B1): the first DJ-packet (Q1) using basis B0, and the second DJ-packet (Q2) using basis B1.
Where, B0 = standard basis/Z-basis, B1= X-basis

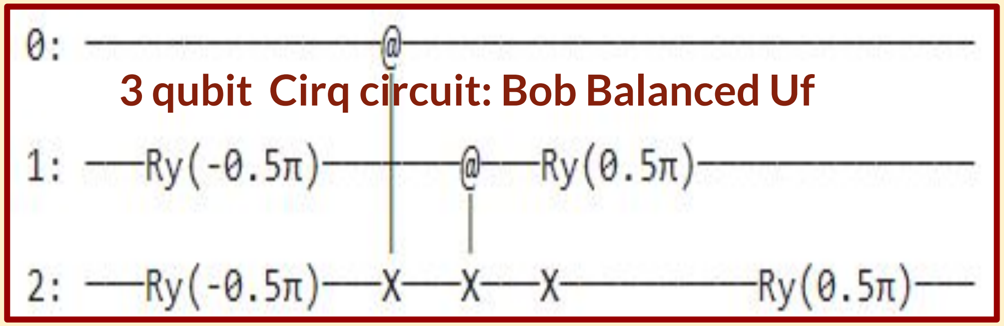
***Option (ii)*: individual qubits within a DJ-packet can use different basis (B0, B1)**

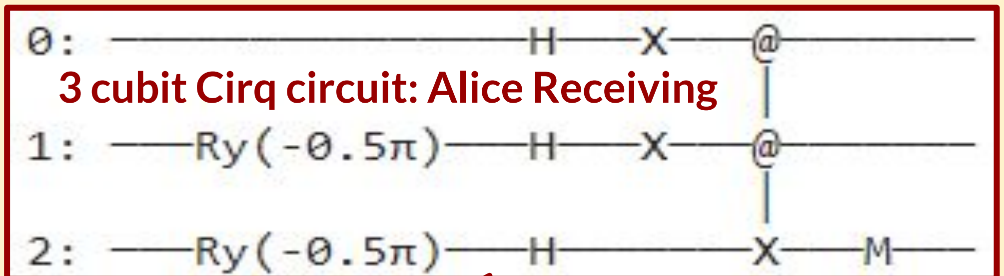
Q1 (0, B0)	**Q1 (T, B1)**	**Q1 (1,B1)**	**Q2 (0, B1)**	**Q2 (1, B0)**	**Q2 (2, B1)**	**Q2 (T, B0)**	**Q2 (3,B0)**

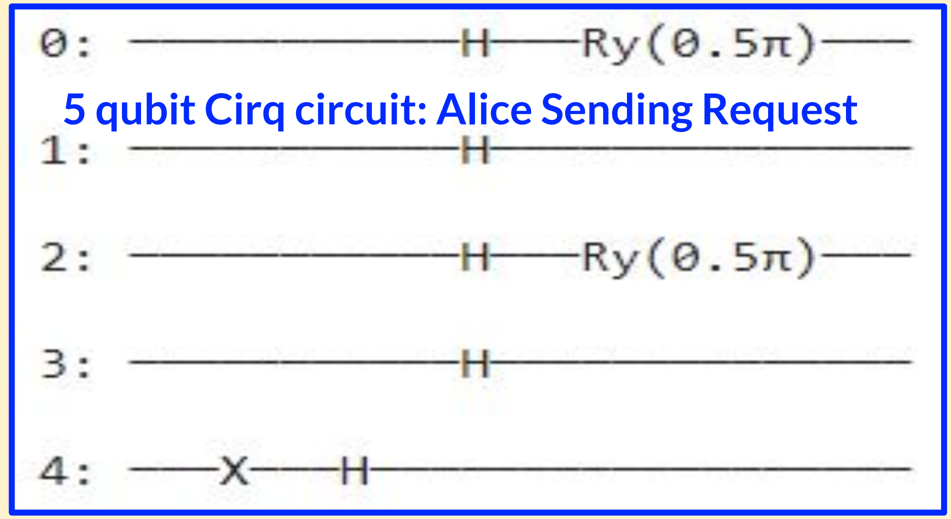
Hopping Sequence HRB:3(1, B0, B1, B1),5(3,B1, B0,B1,B0,B0) where basis can be different for individual qubits in a DJ-packets Q1 and Q2. *Where, B0 = standard basis/Z-basis, B1= X-basis*

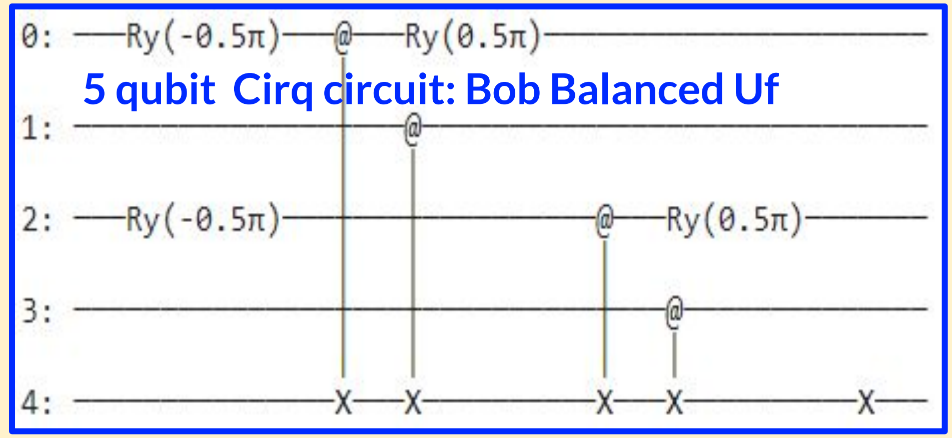
The new work: Example Cirq circuit for Alice and Bob in the HRB scheme

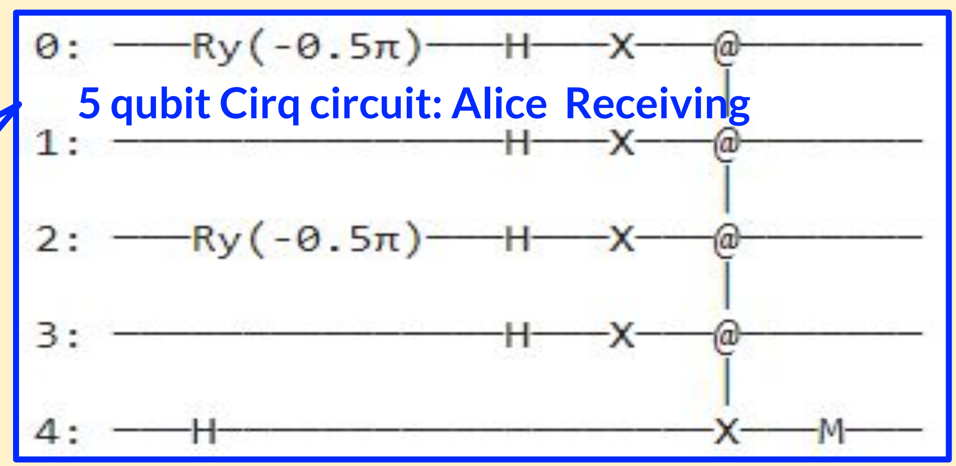










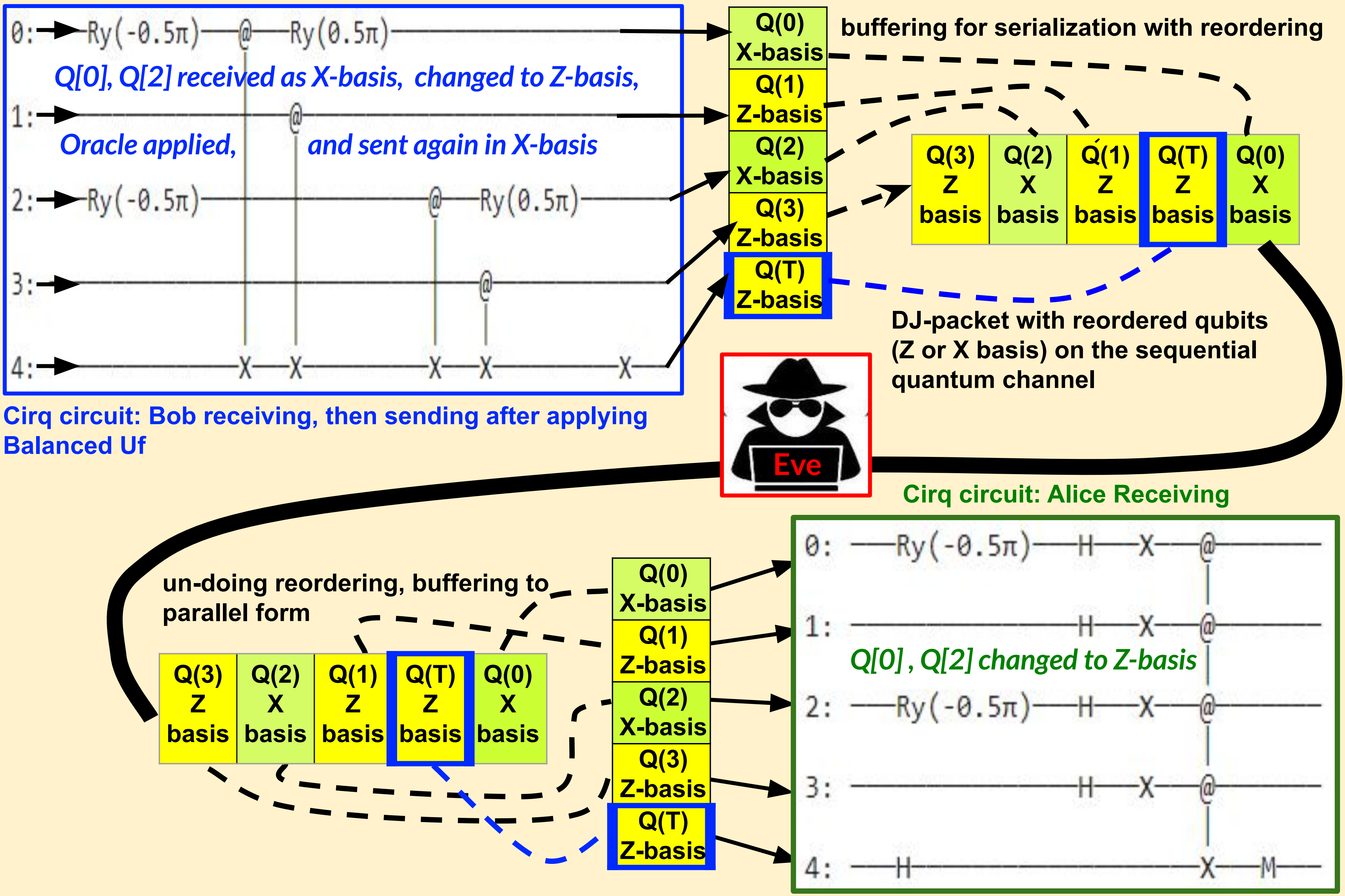


Circuit for
HRB : 3 (2, B0, B1, B1), 5 (4,B1, B0,B1,B0,B0)

Q[0] (Z-basis)	Q[1] (X-basis)	Q[2] (X-basis)

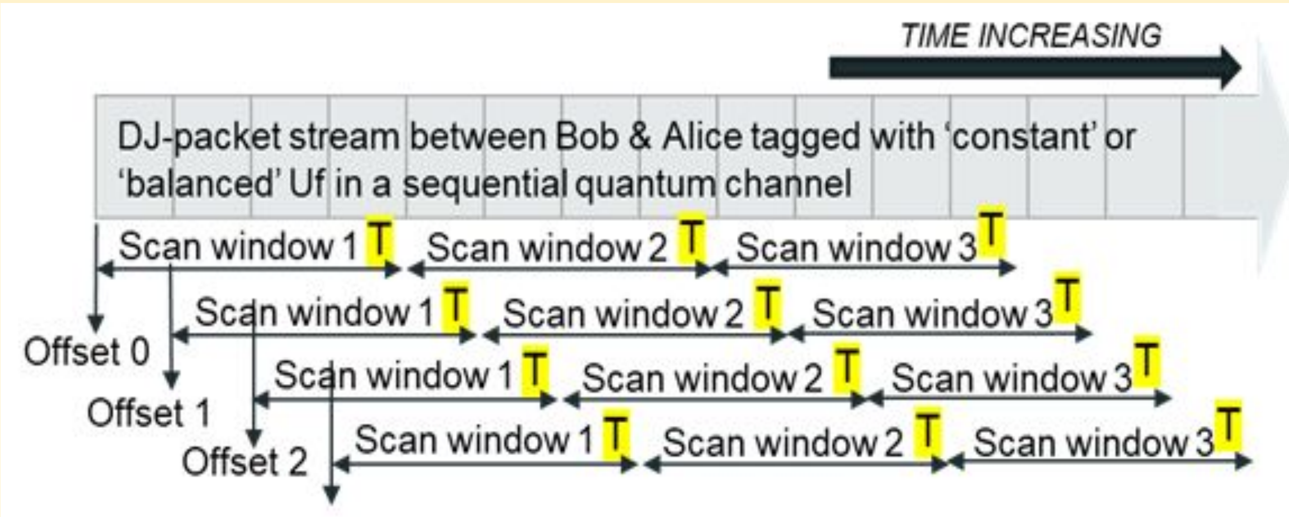
Q[0] (X-basis)	Q[1] (Z-basis)	Q[2] (X-basis)	Q[3] (Z-basis)	Q[4] (Z-basis)

The new work: Example circuit showing buffering, serialization, reordering from Bob to Alice in the HRB scheme a 5-qubit DJ-packet



Cirq simulation, attack model simulation in Python & theoretical probabilities

1. **Cirq simulation** uses quantum gates (e.g., Hadamard, Pauli X, CNOT) to implement Alice, Bob & Eve with DJ-packet qubits as inputs. Separate simulator instances for Alice, Bob, & Eve as they are on different quantum devices.
2. **Python simulation** with Eve attack model and DJ-packet stream set up with various HRB schemes and randomly selected (balanced, constant) oracles. Is much faster than the detailed Cirq simulation involving quantum operations.



Eve attack Model assumes a fixed DJ-packet size (M = 4) & target qubit (T) at the last index (index = 3). Scanning starts with different offsets.

Hopping Sequences have at least one DJ-packet of size M. Assumes qubits can be using either of the two basis Z-basis or X-basis

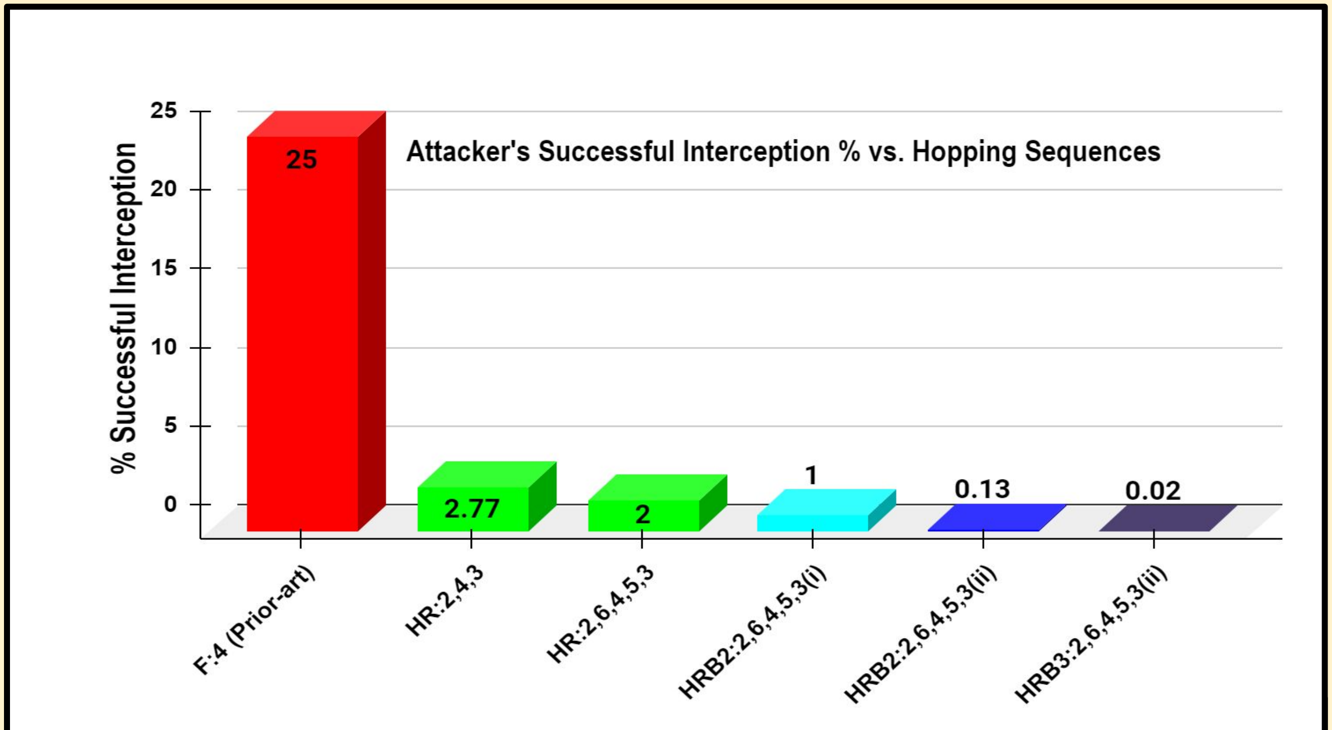
Computing theoretical probabilities of interception for the various schemes:

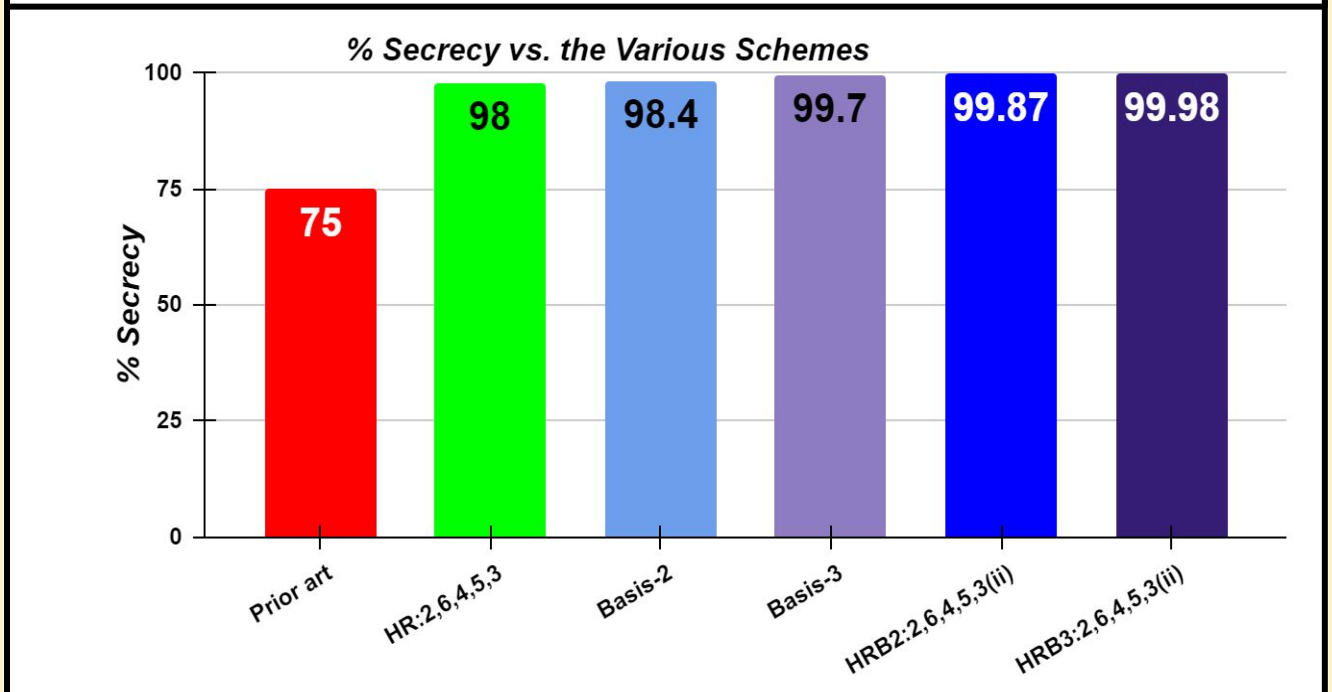
- ❏ Fixed DJ-packet size is **N = 4;** Eve Scan window is **M = 4**
- ❏ Total Size of Hopping Sequence in qubits is **H = 20** for HRB:2,6,**4**,5,3; (20=2+6+4+5+3)
- ❏ Number of DJ-packets in Hopping Sequence with same size as Eve Scan Window is **P = 1**;
- ❏ Number of Bases used **B = 2**

The theoretical probability of successful Interception for:

- **Fixed** *for F:4* Interception = **1/M** = 1 / 4 ⇒ **25%**
- **Fixed Reorder** *for FR:4* Interception = (1/M)*(1/M) = **1/(M*M)** = 1/16 ⇒ **6.25%**
- **Hopping** *for H:2,6,4,5,3* Interception = **P*(1/H) = P/H** = 1/20 = **5%**
- **Hopping Reorder** *for HR:2,6,4,5,3* Interception = (P/H)*(1/M) = **P/(H*M)** = 1/(20*4) = **1.25%**
- **Hopping Reorder Bases** *for HRB:2,6,4,5,3* Interception=(P/H)*(1/M)*(1/B)-pow-M = 1/(20*4*16) = **0.078%**

The simulation results





The first bar (F:4) represents work by K. Nagata & T. Nakamura, with fixed size DJ-packets where attacker's **interception success is 25%.**

The second & third bars (HR) show prior work by R. De, R. Moberly, C. Beery, J. Juybari & K. Sundqvist, IEEE QCE21. where **attacker's interception success dropped to 2.77% and 2.0%**, respectively, i.e., a **12.5-times drop compared to F:4.**

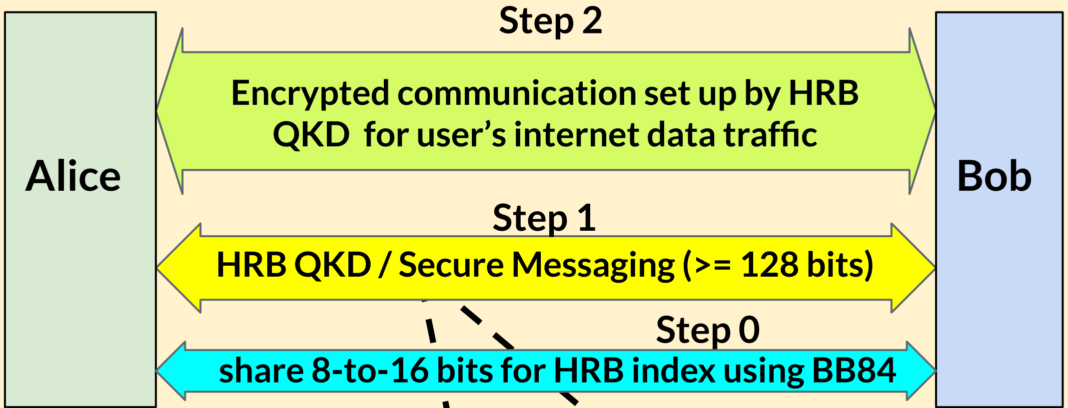
The fourth, fifth and the sixth bars show the new HRB scheme.

- The fourth bar uses two basis and option-1 with 1% successful interception.
- The fifth bar also uses two bases but with option-2 has **0.13% interception success,** which is **200-times lower than F:4**.
- The sixth bar uses three bases with option-2 with **0.02% successful interception** which >**1000-times lower than F:4.**

Secrecy improves from 75% for one basis, to 98.4% for two basis, and to 99.7% for three basis.

The **best secrecy (99.98%)** is achieved when three orthogonal basis is used with DJ-packet size-diversity, and target qubit reordering as in HBR3:2,6,4,5,3(ii)

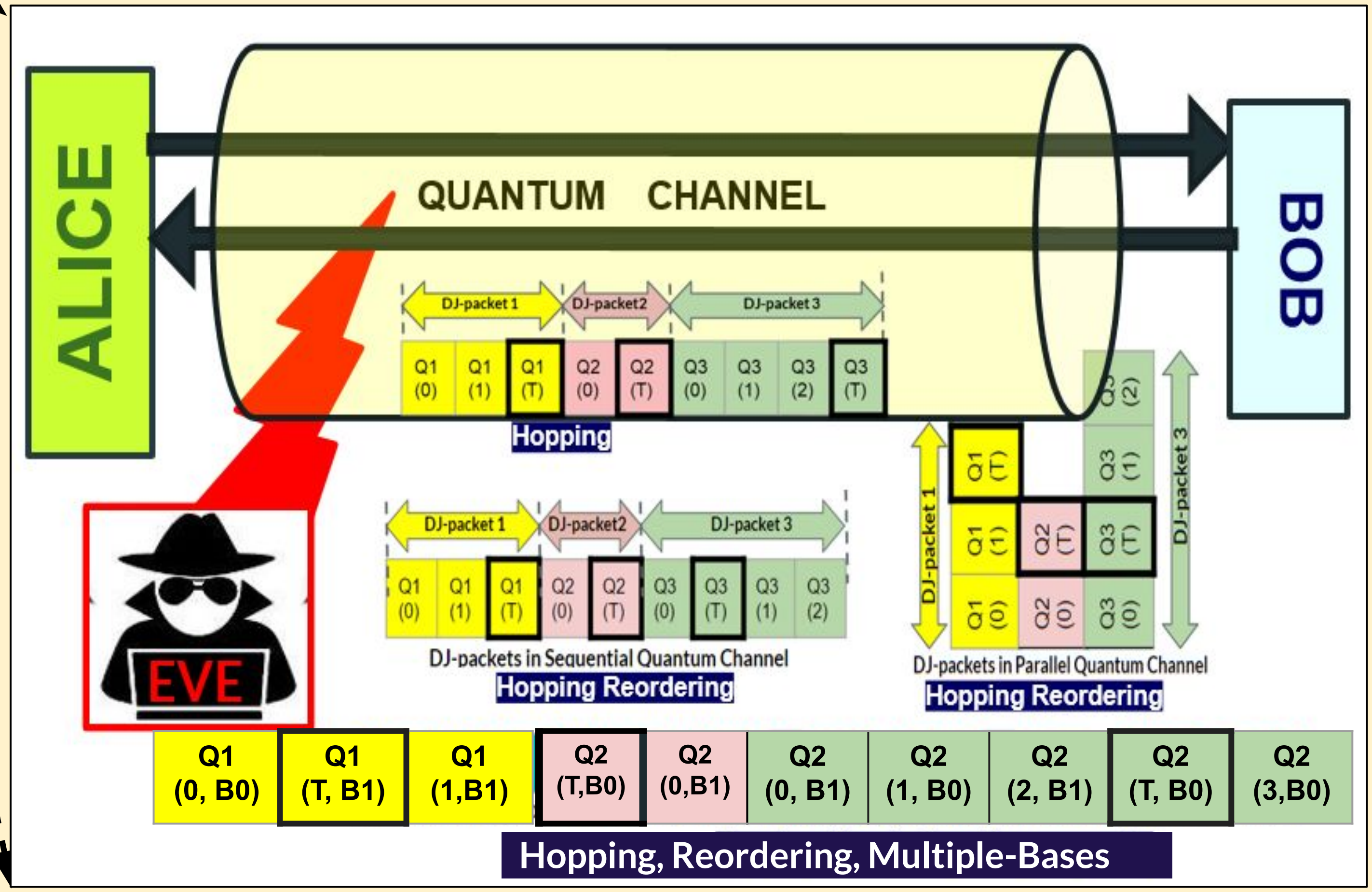
The high entropy quantum communication framework: overall system diagram



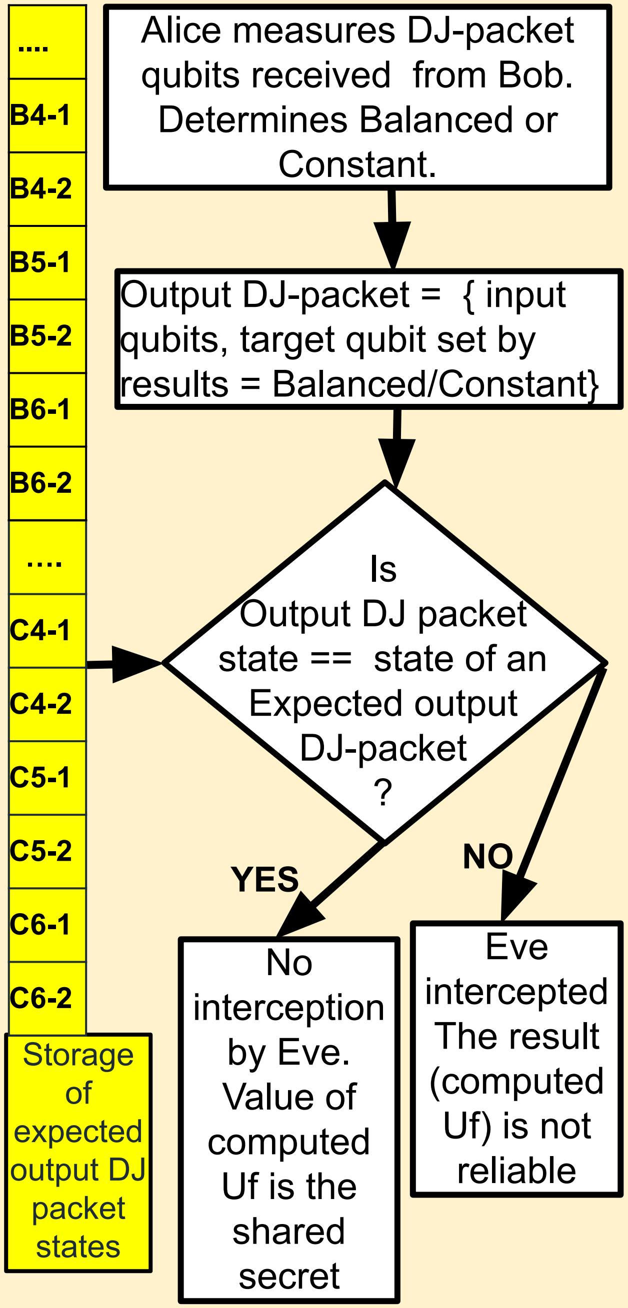
Alice and Bob has the list of all predefined HRS schemes, kept indexed using 8-16 bits (number of entries between 256 to 65,000)

Alice and Bob uses the BB84 scheme to communicate the index of the HRB scheme to use. Then they use the specific HRB scheme for the actual QKD, or instead of QKD Alice and Bob performs Short Secure messaging using the HRB scheme to encode the message bits

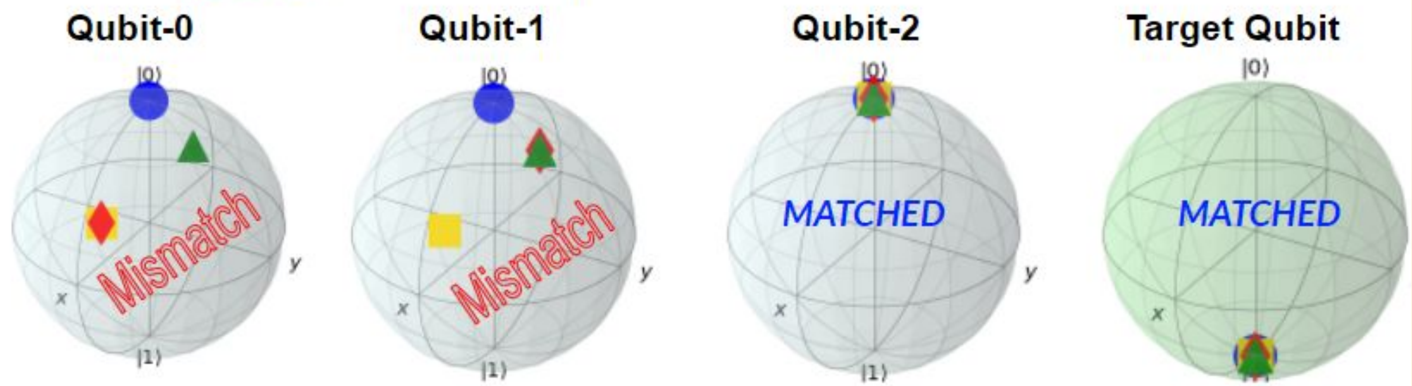
Item	HRB Scheme Description
1	**F**:4(3)
2	**FR**:4(3),4(2)
3	**FR**:4(3),4(2),4(0)
4	**H**:2(1),4(3)
5	**HR**:2(0),4(3)
8	**H**:2(1),4(3)
9	**HR**:2(0),4(3)
...	......
11	**HR**:2(1),4(3),3(0)
...	......
17	**HR**:4(3),2(0),6(2),5(3)
...	......
27	**HR**:2(0),6(3),4(3),5(2),3(1)
...	......



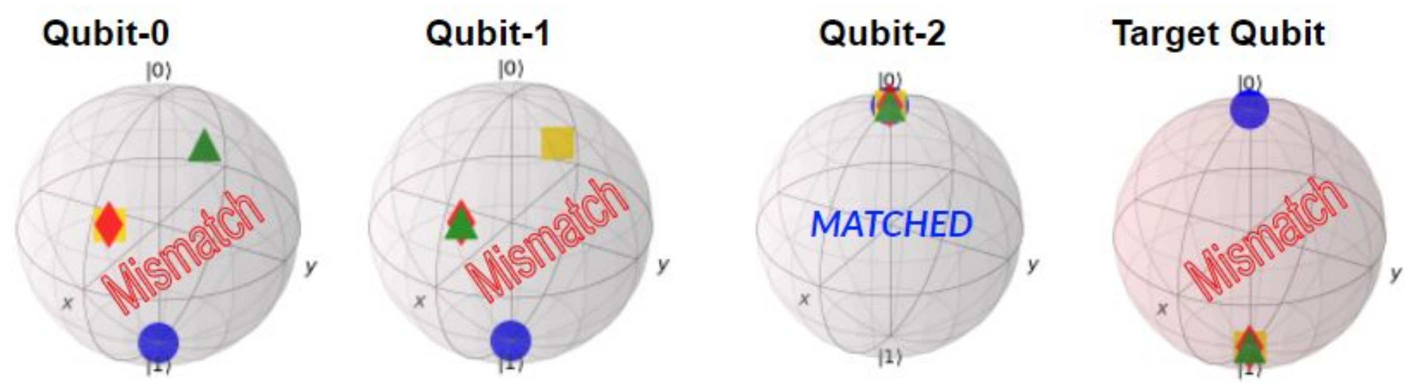
Detecting MITM attack by determining qubit state mismatches in DJ-packets



A Bloch Sphere represents a DJ-packet qubit. The expected (●) state and the actual (◆ ▲ ■) state of the qubits for three different test runs are shown



Balanced Uf: The actual states of Qubit-0 and Qubit-1 t do not meet the respective expected states, indicating an interception by Eve.



Constant Uf: The actual states of Qubit-0, Qubit-1 and Target Qubit do not meet the respective expected states, indicating an interception by Eve.

Conclusion

A novel way to **increase the entropy** of the DJ-packets communicated over the quantum channel is developed by **employing different orthogonal basis** for the qubits in the DJ-packets and combined with the past research that introduced DJ-packet size variation and target qubit reordering.

- Simulations showed that attacker's successful interception rate drops **200-times** when using **two orthogonal base**s, and more than **1000-times** when using **three orthogonal bases** vs. past research.
- The method can be used both for **QKD** and also for **secure messaging** due to very **high secrecy (e.g., 99.98%**) that can be achieved.

Worldwide, there is an increasing focus on **quantum technology to strengthen cybersecurity:**

- ❖ **US Department of Energy** (DoE) in 2020 announced a blueprint for a "***superfast and almost unhackable national quantum Internet***".
- ❖ Various research labs in **USA and Europe** have set up **QKD networks** for experiments and trial runs.
- ❖ **China launched a satellite** (Micius) that **demonstrated QKD** to set up secure communication.
- ❖ Various research teams worldwide are working on **Quantum Emulation hardware** that can make transition to quantum less risky and more accessible.
- ❖ Many **companies** are also working to bring quantum computing in the forefront. While **PKI can be compromised** in a number of ways, **QKD provides companies and government agencies** the means to share confidential, mission-critical data in an ultra-secure, almost unhackable way.

Possible Future Works:

- ➢ Evaluate different HRB schemes on real quantum hardware (it's difficult to get access) and perform trade-offs on HRB quantum circuit size vs. secrecy requirements for the quantum channel.
- ➢ Explore ways to prevent DoS that can happen when the attacker is continuously trying to intercept.
- ➢ Test robustness against quantum decoherence and noisy channels/hardware that can lead to false positives.

This research can also provide a foundation for interested readers to learn more about how quantum computing and quantum communications impact cybersecurity.

THANK YOU

High Entropy Quantum Communication Framework for Secure Key Distribution and Secure Messaging.

Rohit De

Email: de.rohit01@gmail.com

Del Norte High School, San Diego, California 92127, USA

ACKNOWLEDGEMENTS:

The author would like to immensely thank

- Mr Jeremy Juybari, Mr. Colton Beery, and late Dr. Raymond Moberly of Faster Logic LLC, USA;
- Dr. Kyle Sundqvist of the Physics Department at San Diego State University, USA;

for their support on the early research foundations for this project.

Much thanks to Ms. Jo Buehler, Rohit's High School Calculus teacher, for her encouragement and support.

INFOCOMP 2022, The Twelfth International Conference on Advanced Communications and Computation

June 26, 2022 to June 30, 2022 - Porto, Portugal