UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

DETECTING A SPY WITH QUANTUM COMPUTING

MAURICIO SOLAR – FELIPE CISTERNAS – JEAN-PIERRE VILLACURA – LIUBA DOMBROVSKAIA

(Universidad Técnica Federico Santa María, 2024)

CONTENT

- Conceptual Foundations
- State of Art
- Implementation
- Conclusions

CONCEPTUAL FOUNDATIONS – QUANTUM COMPUTING

A Quantum Computer(Qc):

- Solve problems out of reach for Classical Computing.
- Use Qubits and follows the next principles:
  - Superposition
  - Entanglement
  - Decoherence
- Actual State: Noisy Intermedite Scale Quantum (NISQ).
- Utility: Optimization, machine learning, cryptography and more.

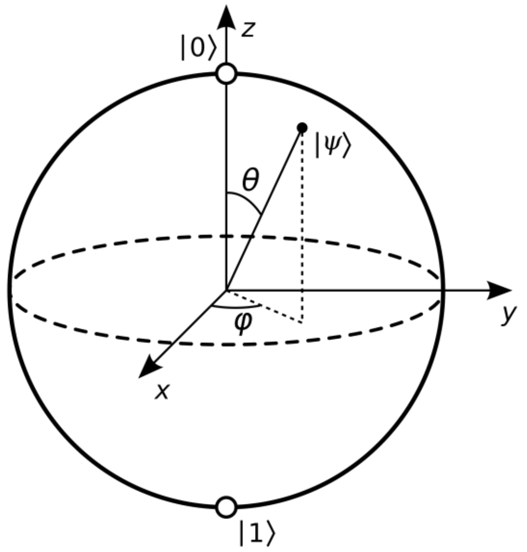
CONCEPTUAL FOUNDATIONS

- Quantum's states Representation:
  - 1 Qubit
  - 2 Qubits Superposition

$$|a\rangle = v_0|0\rangle + v_1|1\rangle \to \begin{bmatrix} v_0 \\ v_1 \end{bmatrix} \quad |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$$

- Bloch's Sphere.
- Quantum Gates
  - NOT $X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\quad X|0\rangle = |1\rangle \quad X|1\rangle = |0\rangle$
  - Pauli-Y $Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ $\quad Y|0\rangle = i|1\rangle \quad Y|1\rangle = -i|0\rangle$
  - Pauli-Z $Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\quad Z|0\rangle = |0\rangle \quad Z|1\rangle = -|1\rangle$
  - CNOT $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
  - Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $\quad H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- Noise
- Quantum Error Correction(QEC)



(Esfera de Bloch, 2024)

STATE OF ART

Date	**Main Advances**
1970	James Park articulates The Non-Cloning Theorem (20).
1973	A. Holevo articulates the Holevo and Bennet theorem's revealing that the computing can be done in a reversible manner.
1980	Paul Beinoff describes the first model of QC Computer (21), Tomasso Toffoli presents the Toffoli's Gate (22).
1985	David Deutsch describes the first QC universal.
1992	D. Deutsch and R. Jozsa propose computational problem that can be solved efficiently in a QC.
1993	Dan Simon invents an oracle problem, for which a QC would be exponentially faster than an algorithm in a QC.
1994	Peter Shor publishes Shor's algorithm.
1995	Shor propose the first schemes for QEC (23).
1996	Lov Grover invents the quantum DB search algorithm.
2000	Pati and Braunstein proved the quantum non-elimination theorem.
2001	First execution of Shor's Algorithm
2003	Implementation of the Deutsch-Jozsa algorithm in a QC.

STATE OF ART

Fecha	Principales avances
2006	First QC of 12 Qubits.
2007	D-Wave system shows the use of a 28 Qubit annealing QC.
2009	Creation of the first electronic quantum processor.
2010	Development of the single-electron Qubit.
2014	Scientists transfer data by quantum teleportation over a distance of 3 meters with an error rate of 0% (24)
2017	IBM introduces the QC of 17 Qubits.
2018	Google announces the creation of a 72 Qubits quantum chip.
2019	IBM unveils its largest QC of 53 Qubits.
2020	Google reports the largest chemical simulation in a QC.
2021	IBM claims to have created a 127 Qubits processor.
2022	Google team creates a traversable wormhole in a QC.
2023	Researchers from Innsbruck entwined two ions at more than 230 meters.

STATE OF ART

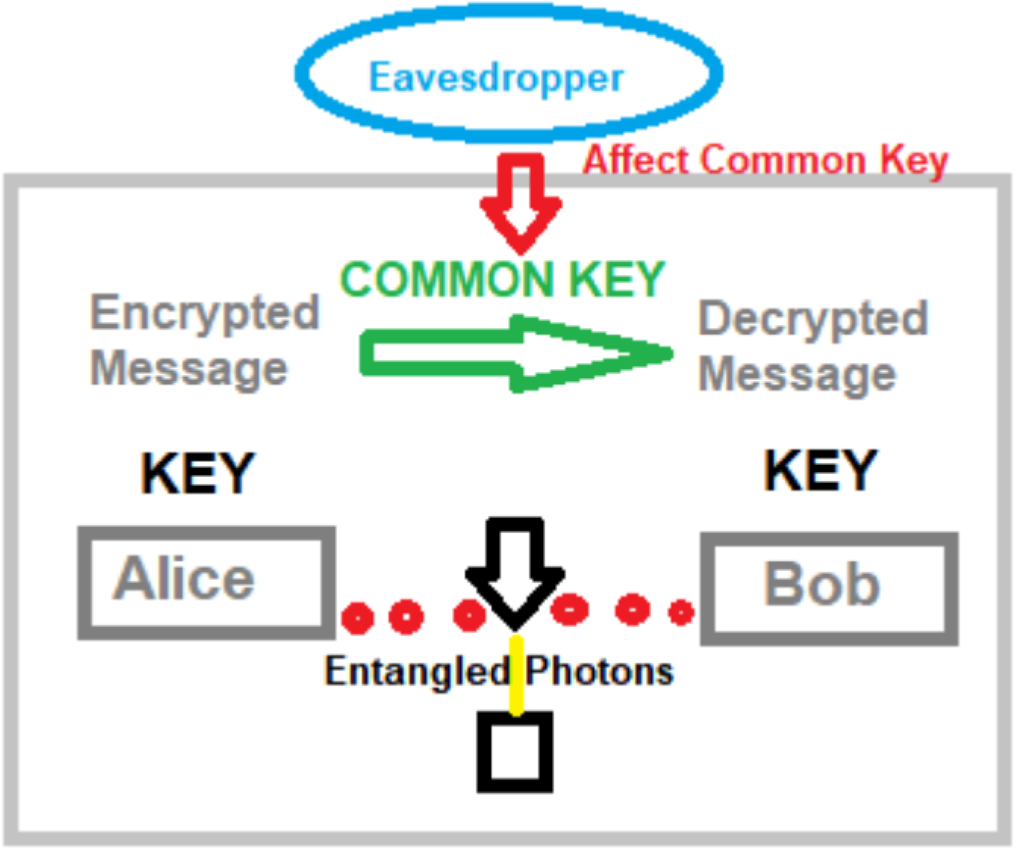
Ref	Contribución Realizada	Ventaja Comparativa
(25)	Propose of AES algorithm with more security using Quantum Random Walk	Post-Quantum propose of AES Algorithm
(26)	Quantum Key Distribution and experiments with eavesdropper.	State of Art of QKD and experiments with eavesdropper and quantity of photons.
(27)	Descripción general de QC en Ciberseguridad presentando varias soluciones.	Estado del arte sobre ataques con QC en contexto de Ciberseguridad
(28)	Propone parámetros y cambios a RSA en QC para hacerlos factibles en la actualidad.	Propone GEECM, versión cuántica de Lenstra Elliptic-Curve Factorization (ECM) y experimentación con escuchas de espías.

IMPLEMENTATION

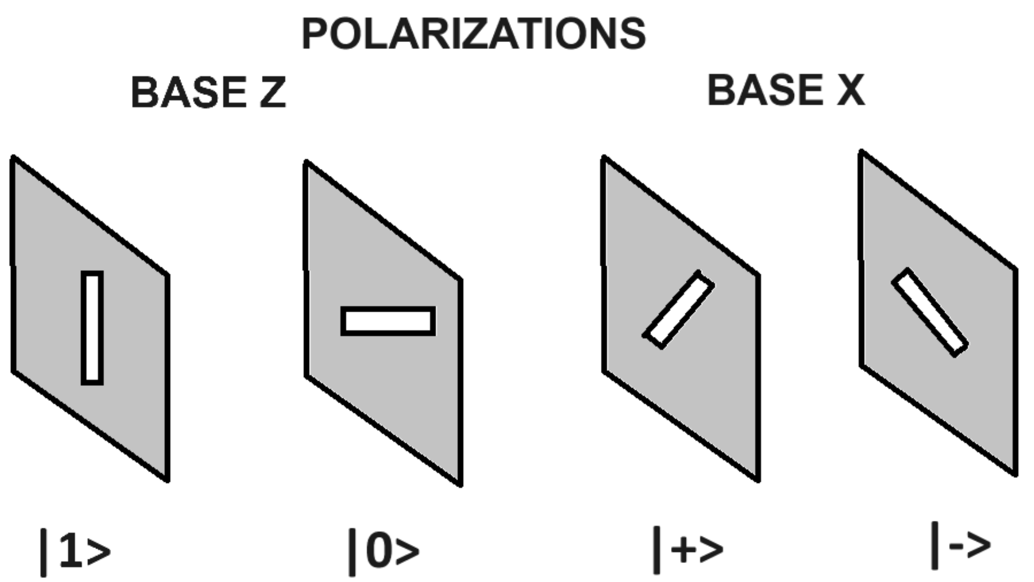
- **Purpose**: Send the next message to Bob:" 1 2 3 2 2 1" using Quantum Key Distribution and Quantum Circuit.
- **Libraries**: Qiskit, Cryptography Fernet.
- **Aim**: Send the next message with the creation of a Shared Key using Quantum simulation.
    - 1 2 3 2 2 1

      Binary: 0b01101110100 1
- **Situations**:
    - 1) No presence of a Spy.
    - 2) Presence of a Spy and detection.
- **Supositions**:
    - 1) No noise in the canal.

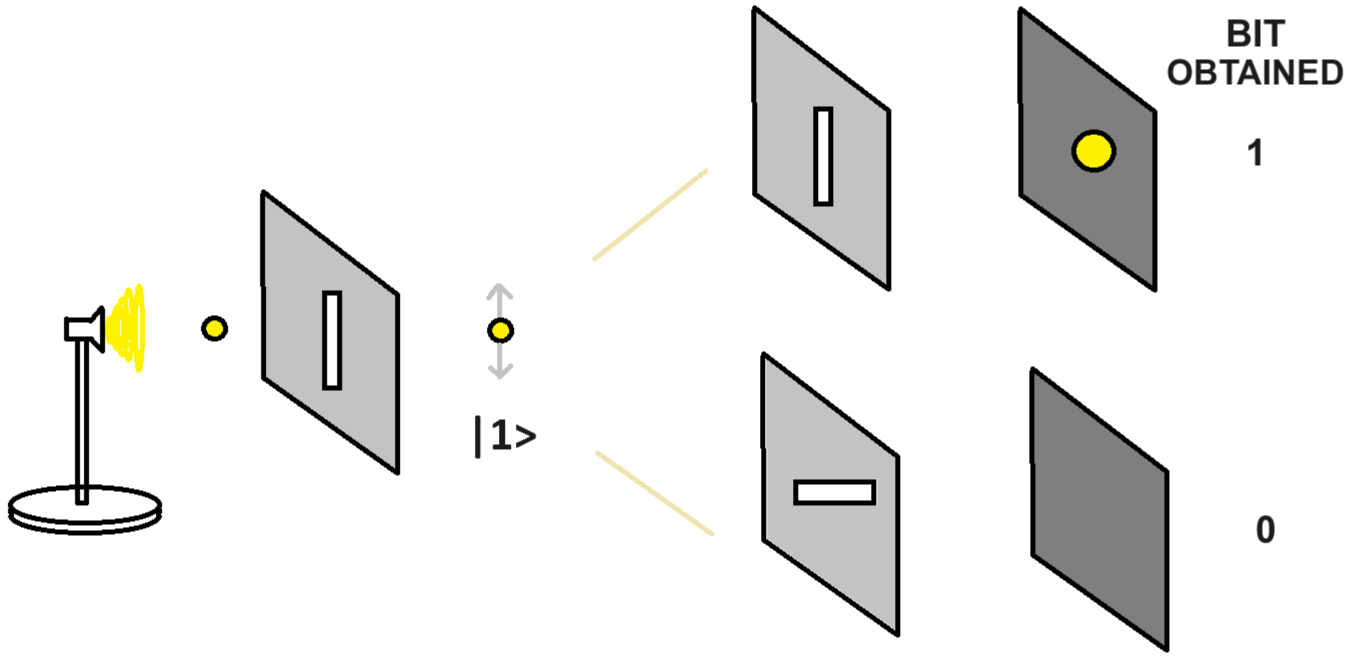
IMPLEMENTATION

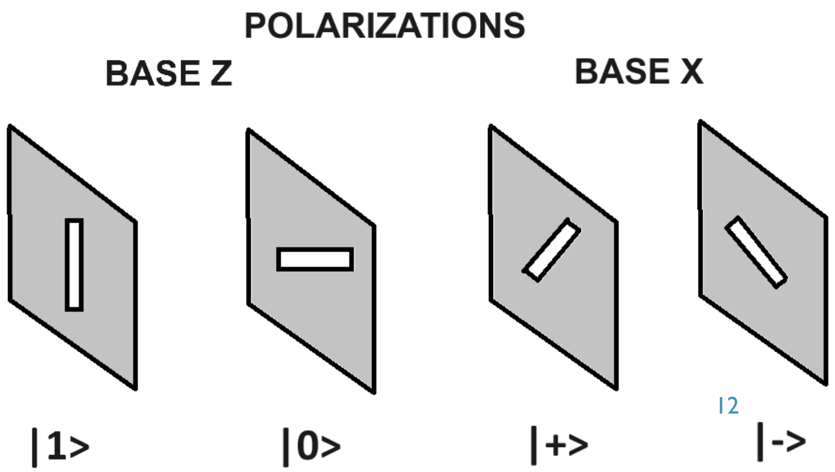


IMPLEMENTATION



IMPLEMENTATION

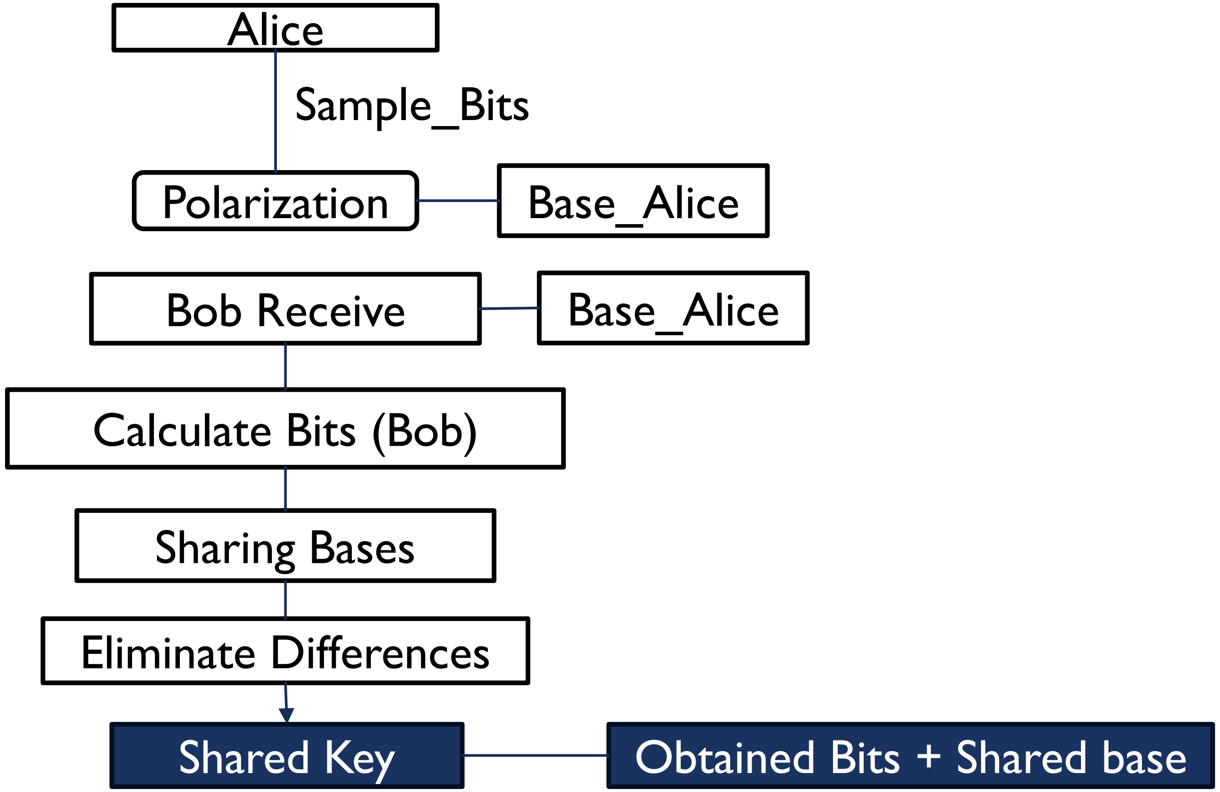




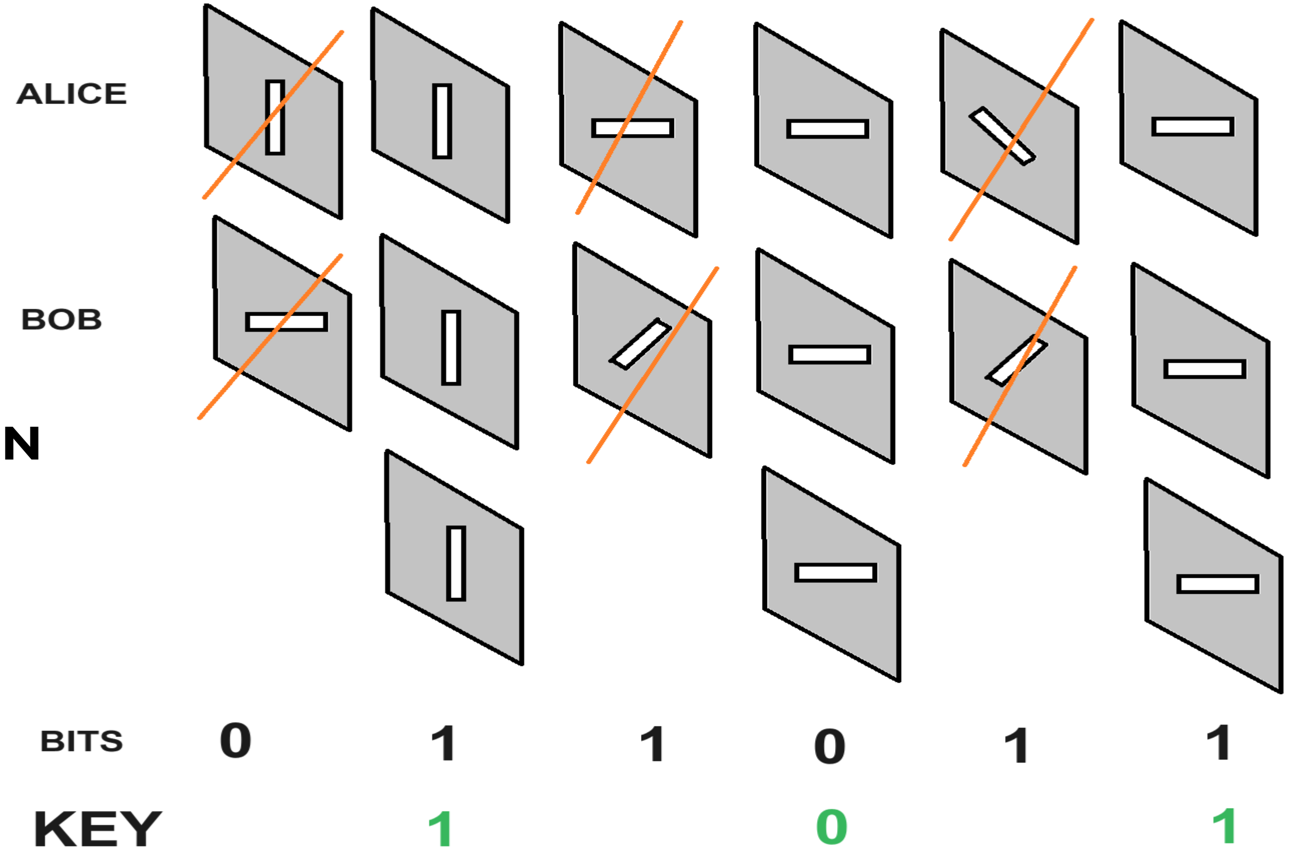
IMPLEMENTATION

- Situation 1) **No spy**:
  - **Generation of Bit String**(not message) **and arbitrary election of Basis:**

Random Generation:
Sample_Bits
Base_Alice
Base_Bob



- **SHARING BASES** (not Bits obtained)

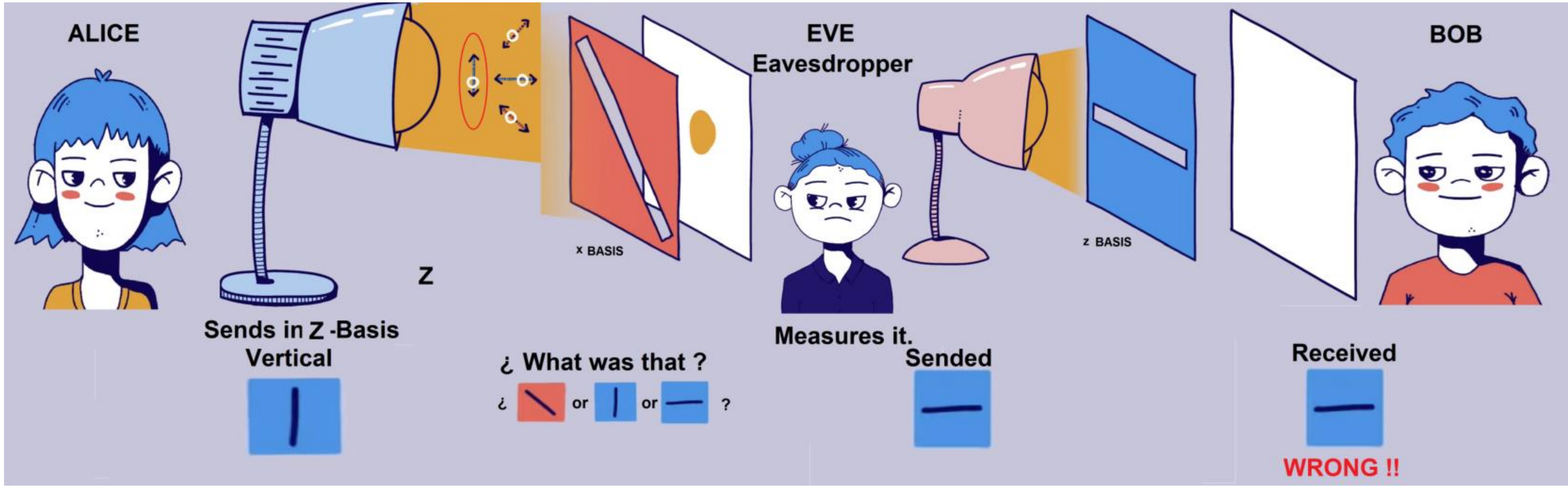


- **KEY OBTENTION**

- One Time Pad
- Cifrado simétrico
- MAC

IMPLEMENTATION

- **Situation 2:** Sending the message with Spy and Detecting.



Spy (EVE) can't know with 100% certainty the base used to replicate to Bob. Bob will realize that key generated is not working and it is reasonable think that the canal is compromised.

FUNCTIONS - IMPLEMENTATION

encode_message(bits, bases**)** , **measure_message(**message, bases**)** , **remove_no_coincidences(**a_bases, b_bases, bits**)**

```
def encode_message(bits, bases):
  message = []
  n=len(bases)
  for i in range(n):
     qc = QuantumCircuit(1,1)
     if str(bases[i]) == '0':
        if str(bits[i]) == '0':
           pass
        elif str(bits[i]) == '1':
           qc.x(0)
     else:
        if str(bits[i]) == '0':
           qc.h(0)
        elif str(bits[i]) == '1':
           qc.x(0)
           qc.h(0)
        qc.barrier()
     message.append(qc)
  return message
```

```
def measure_message(message, bases):
  backend = Aer.get_backend('aer_simulator')
  measurements = []
  n=len(bases)
  for q in range(n):
     if str(bases[q]) == '0': # base Z
        message[q].measure(0,0)
     if str(bases[q]) == '1': # base X
        message[q].h(0)
        message[q].measure(0,0)
     aer_sim = Aer.get_backend('aer_simulator')
     result = aer_sim.run(message[q], shots=1, memory=True).result()
     measured_bit = int(result.get_memory()[0])
     measurements.append(measured_bit)
  return measurements
```

```
def remove_no_coincidences(a_bases, b_bases, bits):
  good_bits = []
  n=len(bits)
  for q in range(n):
     if str(a_bases[q]) == str(b_bases[q]):
        good_bits.append(bits[q])
  return good_bits
```

IMPLEMENTATION

- **Results**

```
Bases
Alice_Base: [0 0 1 0 0 1 1 0 1 1 0 1 0 1 0 0 1 0 0 0 0 0 0 1 1 1 1 0 0 0]
Eva_Base:    [1 1 1 0 1 1 1 0 0 1 0 0 1 1 1 0 1 1 1 1 0 1 1 1 1 1 1 0 0 0]
Bob_Base:    [0 1 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 0 1 0 1 0 0 0 1 1 0 1 0]
```

```
Alice_Key_with_interception: 11101001010001101110
Bob_Key_with_interception:    01111011100111110110
```

```
ERROR. Used key is not correct.
POSIBLE PRESENCIA DE UN ESPIA
  Clave: 01111011100111110110
```

CONCLUSIONS

- Implementation of Quantum Key Distribution Based on BB84 in Python using Quantum Circuits simulator Qiskit.
  - Useful to make a secret shared key with the capacity to detect Spies in the communication.
  - We observe that the apparition of a Spy causes an unmatched shared Key, which is a sign of compromised communication.
    - State's Superposition is a important principle here, only on Quantum Computing.
  - While larger is the Key, better are the chances to detect an Spy in the communication in this context.

REFERENCES

- Wikipedia, "Universidad Técnica Federico Santa María," *Wikipedia, La enciclopedia libre,* https://es.wikipedia.org/w/index.php?title=Universidad_T%C3%A9cnica_Federico_Santa_Mar%C3%ADa&oldid=158781397 (descargado 13 de marzo de 2024).
- Wikipedia, "Esfera de Bloch," *Wikipedia, La enciclopedia libre,* https://es.wikipedia.org/w/index.php?title=Esfera_de_Bloch&oldid=160642043 (descargado 9 de junio de 2024).

REFERENCES

[1] Feynman, R. P. (1982). Simulating physics with computers. Int. J. Theor. Phys. 21, 467–488

[2] Whitfield, J. D., Yang, J., Wang, W., Heath, J. T., Harrison, B. (2022). Quantum computing 2022.

[3] Pogorelov, I. and Feldker, T. and Marciniak, Ch. D. and Postler, L. and Jacob, G. and Krieglsteiner, O. and Podlesnic, V. and Meth, M. and Negnevitsky, V. and Stadler, M. and Höfer, B. and Wächter, C. and Lakhmanskiy, K. and Blatt, R. and Schindler, P. and Monz, T. (2021): Compact Ion-Trap Quantum Computing Demonstrator. PRX Quantum, vol. 2, 2, pp. 020343, https://link.aps.org/doi/10.1103/PRXQuantum.2.020343

[4] Sangil Kwon, Akiyoshi Tomonaga, Gopika Lakshmi Bhai, Simon J. Devitt, Jaw-Shen Tsai (2021): Gate-based superconducting quantum computing. J. Appl. Phys. 129(4): 041102. https://doi.org/10.1063/5.0029735

[5] June Sang Lee, Nikolaos Farmakidis, C. David Wright and Harish Bhaskaran (2022): Polarization-selective reconfigurability in hybridized-active-dielectric nanowires. Science Advances, 8eabn9459. DOI:10.1126/sciadv.abn9459

[6] Wurtz, J. et al. (2023): Aquila: Quera's 256-qubit neutral-atom quantum computer. https://arxiv.org/abs/2306.11727.

[7] Kornjača, M., Samajdar, R., Macrì, T. et al. (2023): Trimer quantum spin liquid in a honeycomb array of Rydberg atoms. Commun Phys 6, 358 (2023). https://doi.org/10.1038/s42005-023-01470-z

[8] Steven H. Adachi, Maxwell P. Henderson (2015): Application of Quantum Annealing to Training of Deep Neural Networks. https://arxiv.org/abs/1510.06356

[9] Cao, Yudong, Romero, Jonathan, Olson, Jonathan P., Degroote, Matthias, Johnson, Peter D., Kieferová, Mária, Kivlichan, Ian D., Menke, Tim, Peropadre, Borja, Sawaya, Nicolas P.D., Sim, Sukin, Veis, Libor, Aspuru-Guzik, Alán (2019): Quantum Chemistry in the Age of Quantum Computing. Chemical Reviews, Vol. 119, No. 19, pp. 10856–10915, https://doi.org/10.1021/acs.chemrev.8b00803

10] Ma, H., Govoni, M. Galli, G. (2020): Quantum simulations of materials on near-term quantum computers. npj Comput Mater 6, 85. https://doi.org/10.1038/s41524-020-00353-z

11] Sivarajah, Ilamaran. (2022): What is Quantum Control Theory?. AZoQuantum. Retrieved on March 06, 2024 from https://www.azoquantum.com/Article.aspx?ArticleID=335

REFERENCES

[12] Riccardo Bassoli, Holger Boche, Christian Deppe, Roberto Ferrara, Frank H. P. Fitzek, Gisbert Janssen, Sajad Saeedinaeeni (2021): Quantum Communication Networks. Foundations in Signal Processing, Communications and Networking. Springer. https://doi.org/10.1007/978-3-030-62938-0

[13] Len, Y.L., Gefen, T., Retzker, A. et al. (2022): Quantum metrology with imperfect measurements. Nat Commun 13, 6971. https://doi.org/10.1038/s41467-022-33563-8

[14] Díaz, A., Rodriguez, M., Piattini, M. (2024): Towards a set of metrics for hybrid (quantum/-classical) systems maintainability. Journal of Universal Computer Science, vol. 30, no. 1, pp. 25-48

[15] S, N., Singh, H., N, A. U. (2022). An extensive review on quantum computers. Advances in Engineering Software, 174, 103337. https://doi.org/10.1016/j.advengsoft.2022.103337

[16] Preskill, J. (2018). Quantum Computing in the NISQ era and beyond. Quantum, 2, 79. doi:10.22331/q-2018-08-06-79

[17] Brooks, M. (2019). Beyond quantum supremacy: the hunt for useful quantum computers. Nature, 574(7776), 19-21. doi:10.1038/d41586-019-02936-3

[18] Bennett, C. H. (1973). Logical reversibility of computation. IBM Journal of Research and Development, 17(6), 525-532. doi:10.1147/rd.176.0525

[19] Raussendorf, R. (2012). Key ideas in quantum error correction. Philo- sophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences , 370 (1975), 4541-4565. doi:10.1098/rsta.2011.0494

[20] Park, J. L. (1970). The concept of transition in quantum mechanics. Foundations of Physics, 1, 23-33.

[21] Benioff, P. (1980). The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. Journal of Statistical Physics, 22(5), 563-591. doi:10.1007/BF01011339

[22] Toffoli, T. (1980). Reversible computing. In J. de Bakker J. van Leeuwen (Eds.), Automata, languages and programming (pp. 632–644). Berlin, Heidelberg: Springer Berlin Heidelberg.

[23] Shor, P. W. (1995). Scheme for reducing decoherence in quantum computer memory, 52(4), R2493-R2496. doi:10.1103/PhysRevA.52.R2493

[24] Pfaff, W., Hensen, B. J., Bernien, H., van Dam, S. B., Blok, M. S., Taminiau, T. H., . . . Hanson, R. (2014). Unconditional quantum teleportation between distant solid-state quantum bits. Science, 345(6196), 532–535. doi:10.1126/science.1253512

[25] Ko, K.-K., Jung, E.-S. (2021). Development of cybersecurity technology and algorithm based on quantum computing. Applied Sciences, 11(19). doi:10.3390/app11199085

[26] Tianqi Zhou, X. L., Jian Shen. (2018). Quantum cryptography for the future internet and the security analysis. Security and Communication Networks. https://doi.org/10.1155/2018/8214619

[27] Uttam Ghosh, P. C., Debashis Das. (2023). A comprenhensive tutorial on cybersecurity in quantum computing paradigm. TechRxiv. https://doi.org/10.36227/techrxiv.22277251.v1

[28] Bernstein, D. J., Heninger, N., Lou, P., Valenta, L. (2017). Post-quantum rsa. Cryptology ePrint Archive, Paper 2017/351. https://eprint.iacr.org/2017/351