A Multi-Dimensional Parity-Switched Packet Protocol for Qubit Retention and Mitigating Eavesdropping in Quantum Key Distribution Algorithms

Pranav Sitaraman
Edison Academy Magnet School
Edison, NJ 08837, United States
sitaraman.pranav@gmail.com

Ishan Mungikar
Montgomery High School
Skillman, NJ 08558, United States
imungikar@gmail.com

***Abstract*—Research in quantum cryptography has sought solutions to efficient quantum algorithms poised to break most modern encryption techniques. This paper seeks to increase the security of quantum key distribution (QKD) protocols with the novel proposition of utilizing non-orthogonal basis states in multiple dimensions. It then introduces the framework for a parity-switched packet protocol (PSPP) to be applied to common QKD algorithms such as BB84 and E91 to preserve higher qubit retention while mitigating eavesdropping. These ideas culminate with the creation and optimality of E91-Parity, the application of PSPP to E91 over non-coincident triangular and tetrahedral basis schemas.**

***Keywords*—quantum key distribution, BB84, E91, basis states**

I. Introduction

Quantum cryptography protocols have been at the forefront of research and development for the next-generation of quantum computers. With quantum supremacy having already been shown on certain computers [1], efficient quantum algorithms such as Shor's algorithm [2] have the potential to break the known methods of classical cryptography.

As a result, quantum cryptographers have looked to create quantum protocols that can send information across a quantum channel without the risk of an eavesdropper abstracting information from this channel. Quantum key distribution (QKD) algorithms, such as BB84 and E91, were devised to deal with the problem of sending information in a secure manner across quantum channels. Current quantum cryptography research is focused on qubit retention, with today's quantum computers still limited by qubit number [3].

This paper aims to test the viability of multi-dimensional basis states for quantum key distribution and builds off of similar research endeavors, such as the six-state protocol (SSP) [4], to demonstrate the improvements in performing QKD protocols with tetrahedral basis states.

This paper then presents a novel Parity-Switched Packet Protocol (PSPP), which argues for the use of repeatedly shuffled basis schemas according to the parity of bits in the constructed key. The protocol seeks to demonstrate higher qubit retention rates compared to traditional implementations of the BB84 algorithm while maintaining viable security compared to E91.

Finally, this paper proposes and proves the optimal nature of the E91-Parity algorithm, which involves the application of PSPP to E91 over a combination of triangular and tetrahedral basis schemas.

II. Preliminaries

A. BB84

BB84 is a protocol in which a unidirectional quantum channel, often represented by a stream of photons, is used to send a private key from one party, Alice, to another party, Bob [5]. Prior to transmission, Alice and Bob both agree upon a coordinate system and a set of bases with which to measure the polarization of the photons. For each bit, Alice polarizes a photon along a random basis state and then sends it to Bob. Bob then randomly picks a basis state that is not necessarily the same as Alice's and measures the photon using this basis.

At the end of the key generation process, Alice and Bob share their chosen basis states for each qubit over a bidirectional classical channel. They then discard any qubits where their basis states fail to match before comparing the values of their measurements on half of the bits with matching basis states to determine the presence of an intruder. If their corresponding measurements all match, Alice and Bob can generate a key with the bits from the remaining half of the matching basis states.

Alice and Bob are able to detect an intruder if they notice a difference in measurements within any of their pairs of compared bits. This is because if an intruder, Eve, is interfering, she will pick her measuring basis from

979-8-3503-0965-2/23/$31.00 © 2023 IEEE

the same set of bases as Alice and Bob to maximize her chances of being able to eavesdrop on the bits. However, because measuring a quantum state causes its underlying wave function to collapse and thus be destroyed, Eve must send a new photon to Bob in an effort to cover up her eavesdropping. Eve is unable to know either Alice's or Bob's basis state. As such, the best she can do is send Bob the same qubit she has read in the same basis state she has measured from, meaning that Bob may not always measure the same value as Alice. Differing measurements for a bit with matching basis states are therefore indicative of interference in the key generation process.

B. E91

The E91 algorithm relies on a similar set of mechanics as BB84 with a few key differences. Firstly, Alice and Bob each receive one photon from a pair of entangled photons produced by an external source. They both randomly pick a basis state from the set of agreed-upon bases and independently measure the polarization of their photon.

The second primary difference is in the method of detecting interference that E91 employs. E91 compares bits with non-matching rather than matching bases to detect when Eve intrudes on the quantum channel. This enables E91 to transmit fewer bits to achieve a key of the same length while still ensuring channel security.

In the same manner as before, Eve will pick her measuring basis from the same set of bases as Alice and Bob and then send Bob the same qubit she has read with the photon polarized in the same basis state she has measured from. When Bob receives the bits, he publicly communicates his bases with Alice as in BB84. He sends his bits with non-matching basis states to Alice, who compares them against her corresponding bits.

When Alice compares her bits with Bob's bits, she will notice that some bits match while others are different. As shown in [6], the proportions of matching bits will be different depending on if the channel is secure or if Eve is interfering, where Eve's intrusion will increase the probability of finding matching bits. If this increased probability is observed, Alice and Bob end the communication and key distribution process. If not, Alice and Bob discard the shared bits and keep the private bits found from the matching bases as part of the key.

C. Useful Lemmas and Definitions

Definition 1. *Basis Schema: A set of basis states that Alice and Bob choose from when measuring the state of a qubit (polarization of a photon).*

Definition 2. *Usable Bit: A bit that can potentially be in Alice and Bob's private key without being publicly revealed.*

Definition 3. *Eavesdropped Bit: A bit used in the key where Alice, Bob, and Eve all measure the same value.*

Definition 4. *Checked Bit: A bit whose value Alice and Bob compare over the classical channel.*

Definition 5. *Incorrect Bit: A bit used in the key where Alice and Bob do not record the same value.*

Definition 6. $\theta_{i,j}$ *is the central angle between basis states* i *and* j *on the Bloch sphere.*

Lemma 1. *The probability of measuring a qubit of value* $|0\rangle$ *in basis* β *that has a value of* $|0\rangle$ *in basis* α *is* $\cos\left(\frac{\theta_{\alpha,\beta}}{2}\right)^2$.

Proof. WLOG, let basis α be $|0\rangle = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ and fix β on the real plane of the Bloch sphere. Measuring in basis β is thus equivalent to applying the rotation gate RY, giving,

$$RY(\theta_{\alpha,\beta}) = \left(\begin{smallmatrix}\cos(\theta_{\alpha,\beta}/2) & -\sin(\theta_{\alpha,\beta}/2)\\ \sin(\theta_{\alpha,\beta}/2) & \cos(\theta_{\alpha,\beta}/2)\end{smallmatrix}\right)$$

$$\beta = \left(\begin{smallmatrix}\cos(\theta_{\alpha,\beta}/2) & -\sin(\theta_{\alpha,\beta}/2)\\ \sin(\theta_{\alpha,\beta}/2) & \cos(\theta_{\alpha,\beta}/2)\end{smallmatrix}\right)\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) = \left(\begin{smallmatrix}\cos(\theta_{\alpha,\beta}/2)\\ \sin(\theta_{\alpha,\beta}/2)\end{smallmatrix}\right) =$$

$$\cos(\theta_{\alpha,\beta}/2)\,|0\rangle + \sin(\theta_{\alpha,\beta}/2)\,|1\rangle$$

The probability of observing $|0\rangle$ is therefore $\cos(\theta_{\alpha,\beta}/2)^2$. □

III. Multi-Dimensional Basis States

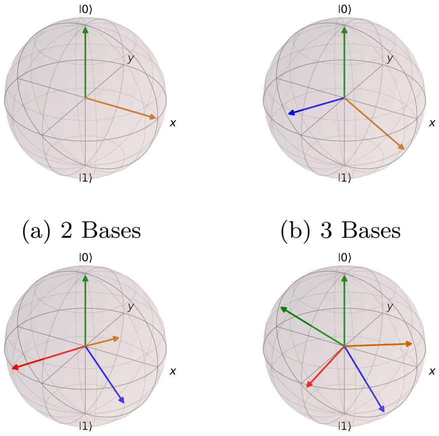
A. Motivation

With the advent of protocols such as the six-state protocol [4], creating basis schemas that function in three dimensions becomes a valid tool for increasing overall qubit-by-qubit security. Advances in technology allow quantum computers to manipulate increasing numbers of qubits in three dimensions [3], meaning that such multi-dimensional quantum key distribution protocols can be implemented.

The following analysis shows that increasing the number of basis states from the traditional E91 or BB84 protocols decreases the probability of a eavesdropped qubit, allowing for the system's security to be substantially improved. Arrangements of these higher-order basis schemas in three dimensions can be represented as polyhedra inscribed in the Bloch sphere. This novel approach provides some valuable intuition for what such a polyhedron should entail.

1) The orientation of the qubit should be a non-factor in probabilistic outcomes. For this to be true, the symmetry group of the polyhedron must be transitive on the vertices, edges, and faces, leaving only the platonic solids.
2) Any basis should not be coincident with any another basis or the reflection of another basis through the center, as this reduces its probabilistic effectiveness. For a platonic solid, this means that it must not be mapped to itself by point inversion.

The only polyhedron that satisfies these conditions is the tetrahedron. Other special properties of the tetrahedron that make it an ideal set of bases include the fact that it has congruent vertex-center-vertex angles for all pairs of vertices and is the only possible arrangement of four equidistant points in three-dimensional space. Following the usage of the tetrahedron, the lack of platonic solids with 5 vertices makes it apparent that a 5-basis schema must be accomplished with a regular pentagon in 2 dimensions. These arrangements are shown in Fig. 1.



(a) 2 Bases

(b) 3 Bases

(c) 4 Bases

(d) 5 Bases

Fig. 1: Multi-dimensional basis states on the Bloch sphere.

B. *Algorithm Metrics*

Table I outlines the metrics for the proposed extensions to the BB84 algorithm, while Table II displays the corresponding metrics for the E91 algorithm. The derivations for these metrics for BB84 and E91 can be found in Appendix A and Appendix B respectively.

Analyzing the eavesdropping rates across all demonstrated basis schemas shows that a tetrahedral arrangement is optimized against an intruder's ability to eavesdrop on a key. The calculation of the proportion of the key eavesdropped displays a significant improvement in the security of the tetrahedral basis schema as compared to others. The results of this paper help to illuminate the viability of various higher-order basis schemas in constructing secure quantum key distribution protocols.

IV. Parity-Switched Packet Protocol

Tetrahedral-arranged basis states provide new applications for quantum security protocols, but the low qubit retention rates when applied to standard methods make the implementation of the algorithm less feasible in regards to key generation. In order to mitigate the issues of wasted qubits in the tetrahedral basis schemas, a novel Parity-Switched Packet Protocol (PSPP) is proposed to increase qubit retention rates while maintaining the security given by this specific geometric arrangement of basis states.

PSPP relies on the superimposition of two basis schemas within one Bloch sphere so that no two bases are coincident. The remainder of this paper discusses PSPP using the triangular 3-Basis and tetrahedral 4-Basis schemas superimposed as shown in Fig. 2.

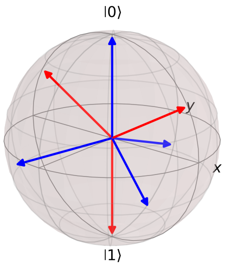


Fig. 2: Superimposition of 3-Basis and 4-Basis schemas on the Bloch sphere to produce the Parity-Basis.

A. *Mechanisms for PSPP*

Prior to communication, Alice and Bob agree to break an intended-length key into packets of length n bits. They also decide together to arbitrarily give each of the 3-Basis states a unique label 0, 1, or 2 and each of the 4-Basis states a unique label 0, 1, 2, or 3. Alice and Bob then start communication by making measurements for the first packet with the 3-Basis schema. Alice and Bob both measure a series of n quantum bits according to either the BB84 or E91 protocol and record the basis states they use for each measurement. Bob then classically shares his bases as a list of integers in the form $3k + b_j$ (the coefficient of 3 is given by the number of states in the basis schema of choice), where k is a sufficiently large integer and b_j is Bob's measurement base.

Alice reads these integers that Bob has shared classically. As Alice is also using the 3-Basis schema, she takes each of the integers she sees modulo 3, arriving at the value of the basis that Bob measured with. Alice now knows both her own and Bob's bases, and so she uses either the BB84 algorithm or the E91 algorithm to check for interference by Eve. If interference is detected, Alice and Bob terminate the communication as the channel is compromised and a key cannot be shared safely. If interference is not detected,

TABLE I: Metrics of Modifications to the BB84 Algorithm

Metric	BB84-2	BB84-3	BB84-4	BB84-5	BB84-Parity
Proportion of Usable Bits	0.250	0.167	0.125	0.100	0.146
Proportion of Key Eavesdropped	0.625	0.375	0.333	0.375	0.344
Proportion of Checked Bits that Match (No Interference)	1.000	1.000	1.000	1.000	1.000
Proportion of Checked Bits that Match (With Interference)	0.750	0.750	0.667	0.750	0.687
Proportion of Key Incorrect	0.250	0.250	0.333	0.250	0.313

TABLE II: Metrics of Modifications to the E91 Algorithm

Metric	E91-2	E91-3	E91-4	E91-5	E91-Parity
Proportion of Usable Bits	0.500	0.333	0.250	0.200	0.292
Proportion of Key Eavesdropped	0.625	0.375	0.333	0.375	0.344
Proportion of Checked Bits that Match (No Interference)	0.500	0.250	0.333	0.375	0.292
Proportion of Checked Bits that Match (With Interference)	0.500	0.375	0.444	0.437	0.420
Proportion of Key Incorrect	0.250	0.250	0.333	0.250	0.313

Alice adds the remaining bits, as determined by the choice of algorithm, from the packet to an initially empty key and informs Bob to do the same.

Now, Bob and Alice both independently look at their entire key so far, composed of bits from all previous packets sent over the quantum channel. They count the number of 1's that appear in this total key and find the parity of this number (whether it is even or odd). They independently choose the basis schema for their next packet, using the 4-Basis if they observe an even parity and the 3-Basis if they observe an odd parity. Their parities should always match if there is no interference and should mostly match if Eve is interfering. This basis is used to send the next packet through the same process, with the exception that a shared consensus of using the 4-Basis requires Bob to encode his basis state as $4k + b_j$ and Alice to take this integer modulo 4 to uncover Bob's measurement basis. Packets continue to be sent in this manner until a key of desired length is achieved or interference is detected, upon which the communication terminates.

B. Interference in PSPP

The protocol's robustness is shown when an eavesdropper, Eve, tries to breach the system. The process for detecting interference by Eve remains the same as in the BB84-3 and E91-3 protocols using the 3-Basis schema or the BB84-4 and E91-4 protocols using the 4-Basis schema. The primary difference is in the changing of the basis schemas between the end of one packet and the start of the next. This change is made based on the parity of the number of 1's in the total key, which Eve cannot know; the values in the key themselves are never shared publicly and it is practically impossible for her to guess correctly every time. Furthermore, the encoding of the compared basis states as a large integer that can only be decoded with the knowledge of the current basis schema ensures that Eve cannot distinguish between the basis schemas with the information sent in the unsecured classical channel.

The metrics for BB84-Parity and E91-Parity are in Table I and Table II respectively and follow mostly similar formulas to the already derived proportions. The primary difference is that the parity protocols feature equal probabilities of each basis schema (regardless of the number of basis states, which are different between the two schemas) rather than equal probabilities of basis states. This unequal weighting must be taken into account when calculating the proportions observed in the tables. For reference, the Python code used for all calculations for the E91-Parity and BB84-Parity schemas can be found at [7].

C. Unsynchronization of Basis Schemas

There is a small but not insignificant probability that a bit in the transmitted key is incorrect (the corresponding bit is recorded differently by Alice and Bob) when Eve is interfering, which may cause Bob to have a different parity of the number of 1's in his key than Alice even if Eve is not caught. If this is the case, communication must terminate, as a lack of synchronization of the basis schemas used results in an inability for Alice and Bob to compare basis states and generate a viable key.

If the BB84-Parity protocol is used, this is relatively trivial. If Alice and Bob are not using the same basis schema for a packet, they incorrectly believe to be measuring with the same basis state when this is not the case (i.e. the 0 basis in the 3-Basis schema is not coincident with the 0 basis in the 4-Basis schema). Therefore, it is highly likely that there are some bits for which Bob measures a value different than Alice despite expecting to measure with the same basis. When this is observed in a checked bit, communication will be terminated as desired.

If the parity protocol of choice is E91-Parity, the situation is more complex. The proportion of checked bits that match is calculated similarly to when there is interference (as this lack of synchronization in the basis schemas could only be caused by Eve intruding on the channel). However, note that the value shown in the table is derived regardless of the basis schemas of Alice and Bob. The knowledge that Alice and Bob are using different basis schemas results in a proportion of 0.500 instead, which is significantly above the proportion of 0.292 with no interference. Therefore, an unsynchronization of the basis schemas results in a measurable increase in the proportion of matching bits that can prompt communication to be terminated.

V. Conclusions

The metrics generated above demonstrate the optimal nature of the E91-Parity schema and protocol. E91-Parity demonstrates substantial improvements when compared to all tested basis schemes of the BB84 protocol by requiring only $3.5N$ bits for a key of length N, compared to BB84's best-case performance requiring $4N$ bits. Additionally, E91-Parity demonstrates notable improvements to E91-2, E91-3, and E91-5 basis schemas with a proportion of eavesdropped qubits in the key being the lowest at 0.344 compared to the second-lowest of 0.375 among those basis schemas. Lastly, E91-Parity improves on E91-4 with a 0.313 proportion of incorrect bits in Alice and Bob's attempt to make a shared key, less than E91-4's proportion of 0.333. Together, these factors demonstrate the optimality of E91-Parity in comparison to the other tested basis schemas and highlight its practicality for quantum key distribution.

References

[1] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, and et al., "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, p. 505–510, 2019.

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, p. 1484–1509, Aug 1995.

[3] K. Padavic-Callaghan, "IBM unveils world's largest quantum computer at 433 qubits," Nov 2022. [Online]. Available: https://www.newscientist.com/article/2346074/

[4] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters*, vol. 81, no. 14, p. 3018–3021, 1998.

[5] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, p. 7–11, 2014.

[6] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical Review Letters*, vol. 67, no. 6, p. 661–663, 1991.

[7] PranavSitaraman, "PranavSitaraman/PSPP." [Online]. Available: https://github.com/PranavSitaraman/PSPP

Appendix

A. BB84 Derivations

1) Proportion of Usable Bits: Half of the bits for which Alice and Bob's basis states match are usable. WLOG, fix Alice's basis state. Bob's probability of using the same basis state is $\frac{1}{N}$, giving a proportion of $\frac{1}{2} \times \frac{1}{N} = \frac{1}{2N}$.

2) Proportion of Key Eavesdropped: If a bit is in the key, Alice and Bob's basis states are known to have matched. Any pair of Alice and Bob's bases occurs with probability $\frac{1}{N^2}$. Eve will know Alice and Bob's bit without being detected only if both her measurement and Bob's measurement do not flip the bits. This happens with probability $(\cos(\theta/2)^2)^2 = \cos(\theta/2)^4$. Therefore, the proportion of the key eavesdropped is $\sum_{i=1}^{N} \sum_{j=1}^{N} \frac{1}{N^2} \cos(\theta_{i,j}/2)^4$.

3) Proportion of Checked Bits that Match (No Interference): In BB84, the checked bits have the same basis states for Alice and Bob. If there is no interference, Alice and Bob measure along the same basis, and so Bob has a 100% chance of observing the same bit as Alice. This means that the proportion of checked bits that match must be 1.000.

4) Proportion of Checked Bits that Match (With Interference): In BB84, bits need to have the same bases for both Alice and Bob for them to be checked. If Eve is interfering, the checked bits will match only if her and Bob's measurements either both flip the bits or both do not flip the bits. Any pair of Bob and Eve's bases occurs with probability $\frac{1}{N^2}$. For each, the bits match with probability $(\cos(\theta/2)^2)^2 + (1 - \cos(\theta/2)^2)^2$. Therefore, the proportion of checked bits that match when there is interference is $\sum_{i=1}^{N} \sum_{j=1}^{N} \frac{1}{N^2}((\cos(\theta_{i,j}/2)^2)^2 + (1 - \cos(\theta_{i,j}/2)^2)^2)$.

5) Proportion of Key Incorrect (With Interference): As shown above, the proportion of checked bits that match when there is interference is $\sum_{i=1}^{N} \sum_{j=1}^{N} \frac{1}{N^2}((\cos(\theta_{i,j}/2)^2)^2 + (1 - \cos(\theta_{i,j}/2)^2)^2)$. Because the bits that are checked are taken randomly from the same sample of bits that are kept in the key, the proportion of the key that is shared between Alice and Bob is the same expression. Therefore, the proportion of the key with incorrect (unshared) bits is $1 - \sum_{i=1}^{N} \sum_{j=1}^{N} \frac{1}{N^2}((\cos(\theta_{i,j}/2)^2)^2 + (1 - \cos(\theta_{i,j}/2)^2)^2)$.

B. E91 Derivations

1) Proportion of Usable Bits: Unlike BB84, all of the bits in which Alice and Bob's basis states match are usable for the key. In the same process as before, fix Alice's basis state WLOG. The probability that Bob's basis state matches that of Alice is thus $\frac{1}{N}$.

2) Proportion of Key Eavesdropped: The proportion of the key eavesdropped is the same for E91 as in BB84. Every bit in the key is a result of Alice and Bob having matching basis states, which occurs with probability $\frac{1}{N^2}$. Just as in BB84, Eve can only successfully eavesdrop on the communication between Alice and Bob if both her measurement and Bob's measurement do not flip the bits. This happens with probability $(\cos(\theta/2)^2)^2 = \cos(\theta/2)^4$, giving that the proportion of the key eavesdropped is $\sum_{i=1}^{N} \sum_{j=1}^{N} \frac{1}{N^2} \cos(\theta_{i,j}/2)^4$.

3) Proportion of Checked Bits that Match (No Interference): Unlike in BB84, the bits that are checked in E91 are those for which Alice and Bob have different basis states. For a pair of different bases, if there is no interference, then the probability that Bob measures the same bit as Alice is simply $\cos(\theta/2)^2$. Because Bob's base must be different than Alice's, this proportion is $\sum_{i=1}^{N} \sum_{j=1, j \neq i}^{N} \frac{1}{(N)(N-1)} \cos(\theta_{i,j}/2)^2$.

4) Proportion of Checked Bits that Match (With Interference): Alice and Bob check bits when they have different basis states. Note that for their bits to match, Bob and Eve's measurements must either both flip the observed values or both not flip the state. This proportion is $\sum_{i=1}^{N} \sum_{j=1, j \neq i}^{N} \sum_{k=1}^{N} \frac{1}{(N^2)(N-1)}(\cos(\theta_{i,k}/2)^2 \times \cos(\theta_{k,j}/2)^2 + (1 - \cos(\theta_{i,k}/2)^2) \times (1 - \cos(\theta_{k,j}/2)^2))$.

5) Proportion of Key Incorrect (With Interference): As with BB84, the bits in the key are the ones for which Alice and Bob have matching basis states. It holds that the proportion of bits from matching basis states that are also equivalent when there is interference is $\sum_{i=1}^{N} \sum_{j=1}^{N} \frac{1}{N^2}((\cos(\theta_{i,j}/2)^2)^2 + (1 - \cos(\theta_{i,j}/2)^2)^2)$. Therefore, the proportion of the key with incorrect/non-matching bits is $1 - \sum_{i=1}^{N} \sum_{j=1}^{N} \frac{1}{N^2}((\cos(\theta_{i,j}/2)^2)^2 + (1 - \cos(\theta_{i,j}/2)^2)^2)$.