A Symmetric Cryptosystem based on Superdense DNA coding technique

***Abstract*—In a world where data is the new oil, it has become a valuable resource for storage as well as for communication and transmission. The importance of better transmission rate and higher capacity, due to influx of redundant data, during communication, has increased like never before. In terms of security, DNA cryptography has revolutionized a new chapter in the field of cryptography by incorporating DNA and RNA operations such as transcription, translation and so on to ensure security of such data. At the same time, Quantum cryptography has also shown a new scope of Post Classical Cryptography, due to the rise and use of quantum computers and free online simulators such as *IBM Qiskit*. This paper proposes a symmetric cryptosystem, where a novel relationship has been built between DNA states and Bell States, in order to show a new prospective in the field of cryptography. *Superdense DNA coding* promises to increase classical capacity and communication security, despite being undermined by noisy quantum channels. By proposing and identifying a new symmetric cryptosystem, this paper aims to improve communication while ensuring the three security goals: *Confidentiality*, *Integrity* and *Availability*.**

***Index Terms*—Symmetric Cryptosystem, Watson Crick Complementary rule, Bell states, Superdense DNA coding, Bijection Attacks.**

I. Introduction

A. DNA Cryptography

A DNA strand contains a sequence of nucleotides. In a DNA double helix, Purines are complementary only with Pyrimidines, that is, *(Adenine)* A is always paired with *(Thymine)* T and *(Cytosine)* C is always paired with *(Guanine)* G in a DNA strand, according to the refined Watson-Crick complementary rules from Franklin Rosalind's findings. The principle of complementarity for DNA can be interpreted as a *"lock and key principle"*. This means that two strands of the nucleic acids needs to have an attributed structure that fits into one another like a *lock* and it's very *specific key*. A *DNA sense strand*, which can be considered as the *lock*, is the conventional form of a DNA sequence. For example, *5'-CGCTAT-3'* can also be written as *CGCTAT*, where the direction is assumed to be (5'→3'). A *DNA antisense strand*, considered as the *key*, is the complementary of *DNA sense strand*. For example, *3'-GCGATA-5'* can also be written as *GCGATA*, where the direction is assumed to be (3'←5'). These two complimentary DNA strands having opposite directions can also be referred to as *"anti-parallel"* in their nature. The *Watson-Crick complementary rule* cuts down the total combinations of the DNA states to just eight combinations as shown in Table I. This reduces the data redundancy and improves the coding efficiency compared to the use of DNA character coding, which is, using a codon table.

DNA Sense Combinations				DNA Antisense Combinations			
1	2	3	4	5	6	7	8
00-A	00-A	00-C	00-C	00-G	00-G	00-T	00-T
01-C	01-G	01-A	01-T	01-A	01-T	01-C	01-G
10-G	10-C	10-T	10-A	10-T	10-A	10-G	10-C
11-T	11-T	11-G	11-G	11-C	11-C	11-A	11-A

TABLE I: Eight encoding rules of the complementary rule showing DNA Sense and Antisense combinations.

Table I also shows the difference between *DNA Sense* strand and it's *DNA Antisense* strand combinations. Here, if we consider the left four combinations to be the sense strand combinations or *lock* combinations, then it's complementary antisense strand combinations are the right four combinations or *key* combinations; vice versa is also possible, depending on the mutual choice of Alice and Bob. For example, column 1 DNA sense combination has column 8 DNA antisense combination as it's complementary. Therefore, the lock and key combination are as follows: (column 1, column 8), (column 2, column 7), (column 3, column 6) and (column 4, column 5).

B. Quantum Cryptography

Contrary to traditional cryptography, which uses only mathematical methods to ensure the secrecy of information, Quantum cryptography focuses on both physics and it's mathematical methods or models, where information is carried using objects known as (*Qubits*) of quantum mechanics. Unlike bits in a classical computer, which only holds one information at a time (either 0 or 1), a qubit is always in a superposition of two states as shown below.

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

Here, α and β represents the amplitudes or coefficients of the basis vectors $|0\rangle$ and $|1\rangle$, also known as eigenvectors. We calculate the probability of getting the result 0 or 1 from the coefficients α and β as shown in eqn. (2).

$$Pr[0] = |\alpha|^2, Pr[1] = |\beta|^2 \tag{2}$$

where, α, $\beta \in \mathbb{C}$ and satisfies $|\alpha|^2$ + $|\beta|^2$ = 1. A complex number can be represented as a point in a two-dimensional *complex plane*, since a complex number consists of two real numbers and one imaginary number. Here, α and β can be viewed as *real numbers*, $\mathbb{R}$, because complex numbers, $\mathbb{C}$, can easily be simulated by $\mathbb{R}^2$ as well. This is done in order to

simplify the representation of the coefficients to a linear plane instead of a complex plane, without losing much information. Thus, a two qubit system can be represented in the following way,

$$\begin{aligned} |\Phi\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \lambda|1\rangle) \\ &= (\alpha\gamma|00\rangle + \alpha\lambda|01\rangle + \beta\gamma|10\rangle + \beta\lambda|11\rangle) \end{aligned} \tag{3}$$

where, α, β, γ, $\lambda \in \mathbb{C}$ and satisfies $|\alpha|^2$ + $|\beta|^2$ + $|\gamma|^2$ + $|\lambda|^2$ = 1. The computational basis, also known as the Z-basis, for a two qubit system is represented by $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. If we multiply the coefficients of $|00\rangle$ and $|11\rangle$, we get $\alpha\beta\gamma\lambda$ and also, if we multiply the coefficients of $|01\rangle$ and $|10\rangle$, we get $\alpha\beta\gamma\lambda$. If these two values are equal, where α = β = γ = λ = $\frac{1}{2}$ to satisfy the above constraint, then the qubits are in a product state (linear product) or they are tensor products. However, for entangled qubits, these values cannot be equal. This is because in entangled qubits, the pairs are separated as correlated, $|00\rangle$ and $|11\rangle$, and anti-correlated, $|01\rangle$ and $|10\rangle$ pairs. For correlated pairs, if the 1st qubit is 0, then the 2nd qubit must be 0 as well. Also, if the 1st qubit is 1, then the 2nd qubit must be 1 as well. For anti-correlated pairs, if the 1st qubit is 0, then the 2nd qubit is 1 and vice versa. In order to distinguish between correlated and anti-correlated pairs, the product of coefficients are meant to be not equal to each other, i.e. an arbitrary entangled qubit can only represent either correlated or anti-correlated pairs at a time and not together as shown in a two qubit system in eqn. 3.

Therefore, we can say that for correlated pairs, the first product is $\frac{1}{2}$ and the second product is 0. For anti-correlated pairs, it's vice versa. The coefficient is considered to be $\frac{1}{2}$, in order to show the equal probability of getting either $|00\rangle$ or $|11\rangle$ for correlated pairs and getting either $|01\rangle$ or $|10\rangle$ for anti-correlated pairs. This is also the case for maximally entangled qubits, defined in a later section. Thus, they are in an entangled state, which gives rise to the concept of *Entangled Systems* or *Entanglement* in quantum mechanics. One of the simplest case of an entangled quantum system is often known as the *Bell States* or *Einstein, Podolsky and Rosen* (EPR) pairs. These states or pairs are defined as follows,

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\beta_{00}\rangle \tag{4}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\beta_{01}\rangle \tag{5}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\beta_{10}\rangle \tag{6}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\beta_{11}\rangle \tag{7}$$

One of the basic techniques used in Quantum Communication with the help of Entanglement is called *Superdense Coding* (SDC) technique. Here, an entangled state is shared between two parties, who are trying to communicate from a long distance. Alice performs some local quantum gate operations on her half of the state, encodes the bits she wants to send to Bob, based on the gate outputs, through a quantum channel. Upon receiving, Bob measures the entire state, including his and Alice's half, to get the result that will indicate what bits Alice had sent. Based on this technique, there have been many quantum protocols proposed and one such protocol named *Quantum Secure Direct Communication* (QSDC) has become quite popular due to the advantage of transmitting secure information through quantum channels without the use of any keys.

The *objective* of this work is to propose a symmetric cryptosystem, based on a new SDC technique called *Superdense DNA coding* (S-DNA-C) technique and similar to QSDC, i.e. no keys are needed. DNA encoded Bell states messages are transmitted through noisy quantum channel, after Alice and Bob authenticates by sharing a single carrier Bell State encoded by a single DNA letter. This bell state will be based on the least frequent DNA state that appears in the DNA strand, prior to encrypting, in order to increase the complexity of the unitary gate operations required to encrypt the DNA qubits into DNA encoded Bell States being transmitted. Here, the coded message will be in a new *bell basis* known as the *DNA basis* represented by ($|C\rangle$, $|T\rangle$, $|A\rangle$, $|G\rangle$) encoding or masking the computational basis ($|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$) present in the bell states for secure communication.

The *motivation* of this work is to incorporate the strengths of DNA and Quantum Cryptography in order to fix the shortcomings of both the crypto techniques. Due to the concept of **no-cloning theorem** in Quantum Cryptography, one major security issue, eavesdropping is mitigated entirely. In DNA cryptography, a single DNA letter is used to encode two classical bits in order to reduce the data redundancy and also increasing the transmission rate. The benefit of using a single DNA letter to encode for two classical bits can also be incorporated for computational basis, as well, in order to reduce the number of qubits being transmitted as well as making the SDC circuit more efficient to further increase the transmission rate. Both DNA and Quantum cryptography advancements has shown us that they have huge computing power and massive storage capacity.

Contributions of this work: (i) A Symmetric Cryptosystem based on Superdense DNA Coding technique has been proposed. (ii) A new bell basis known as the DNA basis has been proposed and can be used in a similar way as a single DNA letter is used to encode two classical bits. (iii) The use of an authentic channel to maintain the authentication between two parties involved, thus covering another major security issue of Quantum Cryptography, without the use of keys. (iv) How a noisy message can be used to retrieve the original message, i.e. plaintext, by interchanging DNA letters as part of the cryptosystem.

The rest of the paper is organized as follows. In Section II, to identify the research gaps, some existing works have been discussed. In Section III, the proposed system and technique is explained in details along with the types of noises in one of the quantum channels. Section IV presents how this cryptosystem can be hacked with the intention of disrupting the coded message only. In Section V, we discuss the experimental results to show the effectiveness of the system. Finally, the paper is concluded with some future works of the cryptosystem in Section VI.

II. Literature Review

A. Related Works on DNA Cryptography

Shahriar et al. [1] proposed a hybrid encryption technique based on DNA encoding for both cryptography and steganography. They have compared their proposed method with other existing methods and have shown to be more efficient while providing a double layer of security to sensitive data. The authors in both [2] and [3] have used and discussed the DNA digital coding method and the Watson-Crick rule of complementary nucleotides, where the following complement rules are followed by the nucleotides (A with T, C with G). Furthermore, in [3], they have shown a comparative review of recent works based on DNA cryptography where they discussed which cryptographic techniques, DNA digital coding and other techniques were used. They also reviewed the applications and limitations of these works. Hammad et al. [4] discussed an overview of DNA symmetric and asymmetric cryptography. Here, they have also mentioned the types of attacks that can occur on DNA based cryptography such as brute force attack, which is going to be very expensive computational problem due the fact that the four base genes in DNA used for encoding lacks linguistic properties or redundancy as in human language. In study [5], the authors have discussed about the different types of attacks on a cryptosystem such as ciphertext-only attack (COA), known plaintext attack (KPA); Man in the middle attack is also known as known plaintext attack, where the attacker should have access to both plaintext and ciphertext. Lastly in [6], they mentioned how DNA encoding can be used in Quantum Cryptography as well. A plain text encrypted by DNA encoding can be sent through a quantum channel.

B. Related Works on Quantum Cryptography

A recent study [7] has shown the advantage of quantum cryptography over classical cryptography with theorems such as the no cloning theorem, which shows that it is impossible for an eavesdropper to copy a quantum state or make multiple copies of the state without disturbance or detection by the sender and receiver. It has also discussed the popularity of Quantum Key distribution (QKD) protocol and variants of it such as device dependent, independent and semi-dependent QKD protocols as well. This study had gone into details about the assumptions and security guarantees of quantum cryptography. There are two such assumptions that stood out: **Free randomness exists** - A free choice of measurement basis such as the computational or hadamard basis can be randomly chosen without being dependent on any quantum devices, and **Devices do not leak any unauthorized information** - it is assumed that the raw key stored in a classical computer is not leaked in any way possible. Lastly, it concludes by discussing some critique questions regarding QKD such as how authentication is still not guaranteed, how whether it is more vulnerable to denial of service attacks or not. In [8], the author proposes a new protocol by combining QKD and Quantum Direct Secure Communication (QDSC) called Quantum key Secure Communication (QKSC) using enhanced superdense coding technique. Here, they have upheld how QKD is much more vulnerable compared to QDSC. The two way branch used in the quantum channel in QDSC has also been seen as vulnerable, due to the practical implementations. Therefore, in QKSC they have removed the backward branch of QDSC and used their version of the superdense coding, where it stores the classical bits that may get lost in long distance communication. The concept of diffusion is shown in [9], where diffusion is the complexity of the relation between a plaintext and the ciphertext, such that by analyzing the ciphertext, it does not give much information about the plaintext properties. The authors of [10], [11] and [12] have all used superdense coding technique in QKD, QSDC and Quantum Public Key Distribution problems (QPKD) to show it's efficiency and simplicity. Lastly, some lecture tutorials turned papers such as [13] and [14] has shown that the problem of eavesdropping or intrusion detection is solved by quantum cryptography, however, just like classical cryptography, the problem of honest hosts or authentication still remains a major problem even though due to the addition of a more secure quantum channel mitigates this problem or opens a new way for authentication.

C. Methods combining DNA Cryptography and Quantum Cryptography

The authors of [15], [16] and [17], have proposed and demonstrated methods that blended DNA or Genomics problems and methods with Quantum Cryptography and Quantum Mechanics methods. It should be noted that due to the open access of cloud based quantum simulators such as *IBM Qiskit*, researches on hybrid methods of DNA and Quantum cryptography are being conducted and proposed more frequently. In both [15] and [17], they proposed some contemporary methods for testing encoded DNA sequences using Quantum simulators, where they have either used Huffman encoding or Hamming distance in developing classical-to-quantum data encoding methods. Kosoglu-Kind et al. [16] presented a method to analyze the similarity between two DNA or RNA sequences on a quantum computer, where a similarity score is used as an evaluation metric. This was done in order to utilize the computational power of quantum computers to compute the linear sequences of nucleotides, which are represented by letters ranging from thousands to billions.

DNA Sense Combinations				DNA Antisense Combinations			
1	2	3	4	5	6	7	8
$\|00\rangle$-$\|A\rangle$	$\|00\rangle$-$\|A\rangle$	$\|00\rangle$-$\|C\rangle$	$\|00\rangle$-$\|C\rangle$	$\|00\rangle$-$\|G\rangle$	$\|00\rangle$-$\|G\rangle$	$\|00\rangle$-$\|T\rangle$	$\|00\rangle$-$\|T\rangle$
$\|01\rangle$-$\|C\rangle$	$\|01\rangle$-$\|G\rangle$	$\|01\rangle$-$\|A\rangle$	$\|01\rangle$-$\|T\rangle$	$\|01\rangle$-$\|A\rangle$	$\|01\rangle$-$\|T\rangle$	$\|01\rangle$-$\|C\rangle$	$\|01\rangle$-$\|G\rangle$
$\|10\rangle$-$\|G\rangle$	$\|10\rangle$-$\|C\rangle$	$\|10\rangle$-$\|T\rangle$	$\|10\rangle$-$\|A\rangle$	$\|10\rangle$-$\|T\rangle$	$\|10\rangle$-$\|A\rangle$	$\|10\rangle$-$\|G\rangle$	$\|10\rangle$-$\|C\rangle$
$\|11\rangle$-$\|T\rangle$	$\|11\rangle$-$\|T\rangle$	$\|11\rangle$-$\|G\rangle$	$\|11\rangle$-$\|G\rangle$	$\|11\rangle$-$\|C\rangle$	$\|11\rangle$-$\|C\rangle$	$\|11\rangle$-$\|A\rangle$	$\|11\rangle$-$\|A\rangle$

TABLE II: Eight encoding rules of the complementary rule showing DNA Sense and Antisense combinations in Qubits

D. Novelty

The novelty of this study is that it provides a triple layer security by incorporating a relationship between the Watson-Crick complementary rules for DNA and Bell states to preserve both the biological functionality as well as the quantum mechanics principle of entanglement. This is the first of it's kind paper, where a relationship has been built between DNA strands and Bell States to propose a new Bell basis for quantum computation known as the ***DNA basis*** linked to the Z-basis or Computational basis. Using this new basis, the well-known SDC technique is also enhanced into S-DNA-C technique with it's own implications, different from the general SDC. This fills the gaps found in the literature discussed above for both DNA cryptography and Quantum Cryptography.

III. Proposed Approach

A. Preliminaries

Before Alice and Bob starts communicating, it is necessary for them to share and agree on some vital information for encoding and encrypting the plaintext, in order to reduce the amount of information being shared over the channels, i.e. to keep the cryptosystem blind, due to the possible presence of Eve and also to maintain a certain level of authentication, if not entirely. To start with, they will have to agree on the column they want to use from **Table II**, a lookup table that will set the encoding, encryption and decryption rules as well as the DNA encoded Bell States. This table is similar to Table I, showing the combinations, in terms of Qubits.

Let's say, they have mutually agreed on using the column shown in the table below.

Computational Basis	DNA Basis
$\|00\rangle$	$\|C\rangle$
$\|01\rangle$	$\|T\rangle$
$\|10\rangle$	$\|A\rangle$
$\|11\rangle$	$\|G\rangle$

TABLE III: Computational Basis encoding using single DNA qubit letter, Column 4 from Table II.

Similar to DNA cryptography, where two classical bits are encoded or masked by a single DNA letter, here, two qubits are being encoded by a single DNA qubit letter, as shown in Table III. This gives rise to the possibility of a new basis in quantum computation, known as ***DNA basis*** or D-basis, represented by $|C\rangle$, $|T\rangle$, $|A\rangle$, $|G\rangle$. A computational basis or the Z-basis, for *N* qubits is the only basis that has been adapted in the current quantum computers or simulators. X-basis known as the **Hadamard Basis** is also adapted in these simulators by the use of a Hadamard gate, shown later on. Therefore, using the two qubit system, eqn 3, the DNA system is represented in Qubits as shown below.

$$|\Phi\rangle = \frac{1}{3}|C\rangle + \frac{1}{2}|T\rangle + \frac{1}{2}|A\rangle + \frac{2}{3}|G\rangle \tag{8}$$

As discussed earlier, the coefficients can be considered as *real numbers*, $\mathbb{R}$, as well and therefore in eqn. 8, they are represented as fractions. In terms of biology, these fraction coefficients can be taken as the number of hydrogen bonds that binds the bases together, that is, C and G are bound by three hydrogen bonds, T and A are bound by two hydrogen bonds. Here, we can see that the product of the coefficients of $|C\rangle$ and $|G\rangle$ is not equal to the product of the coefficients of $|T\rangle$ and $|A\rangle$. As discussed earlier, they are not in a product state and thus can only be represented in an entangled system. Also, this system does not show us the exact bindings or pairings of C-G and T-A, rather it shows the probability of the DNA bases present in this arbitrary qubit state, $|\Phi\rangle$, based on the number of hydrogen bonds required to bind them, shown as coefficients. Therefore, in order to show the exact pairings, it is required to use the Bell states as shown below.

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|C\rangle + |G\rangle) = |\beta_C\rangle \tag{9}$$

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|T\rangle + |A\rangle) = |\beta_T\rangle \tag{10}$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|T\rangle - |A\rangle) = |\beta_A\rangle \tag{11}$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|C\rangle - |G\rangle) = |\beta_G\rangle \tag{12}$$

Here, the Watson-Crick complementary rule for DNA states and the Bell states which shows correlation and anti-correlation pairs, forms a relationship between themselves. If we consider C and G to be the correlated pairs in the bell states, then T and A are considered as the anti-correlated pairs in the bell states and can be vice versa as well, depending on the encoding rule initially chosen by the sender and receiver mutually from Table III. To simplify, if $|C\rangle$ = $|00\rangle$, then $|G\rangle$ must be equal to $|11\rangle$ to complete the correlation pairs of the Bell states and similarly, if $|T\rangle$ = $|01\rangle$, then $|A\rangle$ must be equal to $|10\rangle$ to complete the anti-correlation pairs of the Bell states.

We can say that the ***DNA basis*** is an orthonormal basis, similar to computational basis, as shown in Appendix A.

For every new communication, mutually or just Alice, they can choose randomly any rule they want, since Bob will be aware of Table II and III as well. The significance of the relationship discussed above is to maintain both the complementary rule, *biological functionality*, as well as to show the pairings, using the *entanglement property* of quantum mechanics. *Maximally Entangled States* are used for these pairings since they are so strongly correlated that measuring one state will reveal the state of the other. Therefore, the pre-information that Alice and Bob will share is shown in the table below.

Computational Basis	DNA Basis	Bell States	DNA Bell States
$\|00\rangle$	$\|C\rangle$	$\|\beta_{00}\rangle$	$\|\beta_C\rangle$
$\|01\rangle$	$\|T\rangle$	$\|\beta_{01}\rangle$	$\|\beta_T\rangle$
$\|10\rangle$	$\|A\rangle$	$\|\beta_{10}\rangle$	$\|\beta_A\rangle$
$\|11\rangle$	$\|G\rangle$	$\|\beta_{11}\rangle$	$\|\beta_G\rangle$

TABLE IV: Extension of Table III showing Bell States and corresponding DNA encoded Bell States

B. Encryption Phase - Sender End

The data encryption process for the quantum channel as well as the authentic channel starts with converting the plain text message containing letters, numbers and special characters into ASCII binary (8-bits). Then, we take each two binary digits from left to right, converting two bits into one DNA letter according to any 2-bit binary encoding rule from Table I, in this case column 4.

Algorithm 1: Encryption Procedure using S-DNA-C
Step 1: Convert the Plain text message (PBIN) into ASCII Binary.
Step 2: Convert the PBIN into DNA Sequence using 2-bit binary encoding.
Step 3: Encode the DNA sequence to it's equivalent DNA basis sequence, i.e. Table III and send the least frequent DNA basis to Bob through Quantum Channel 1.
Step 4: Based on the least frequent DNA basis, Bob will create the carrier DNA encoded Bell State in his lab and send to Alice over Quantum Channel 1.
Step 5: Once Alice authenticates that the Bell State received is the correct Bell state from Table IV, she will use the S-DNA-C technique to encrypt the DNA basis states into Bell States to create DNA encoded Bell states to be sent over Quantum Channel 2.

Let us assume, Alice's plaintext message is: "hello", which she wants to send to Bob securely. So, if we have P = hello, then the ASCII binary of P, PBIN = 01101000 01100101 01101100 01101100 01101111. We convert PBIN by substituting every two bits, from left to right, with its corresponding DNA base. Thus, we get MSense = TAAC TATT TAGC TAGC TAGG. MSense is the DNA sense strand in this case. Therefore, M Qubit Sense Strand will be,
MQSense = $|T\rangle|A\rangle|A\rangle|C\rangle$ $|T\rangle|A\rangle|T\rangle|T\rangle$ $|T\rangle|A\rangle|G\rangle|C\rangle$ $|T\rangle|A\rangle|G\rangle|C\rangle$ $|T\rangle|A\rangle|G\rangle|G\rangle$.

Here, $|C\rangle$ is the least frequent DNA basis that appears in the strand and therefore will be sent to Bob over Quantum Channel 1. Bob will create the carrier Bell State, $|\beta_C\rangle$, required for Alice to encrypt the DNA basis states, over Quantum Channel 1 as shown in Figure 2.

1) Superdense DNA coding (S-DNA-C) for Quantum Channel - From Encryption to Decryption Phase: In SDC, Alice chooses any one of the four *maximally entangled* Bell states, from eqn. 4 to 7, to encode the classical bits she wants to transmit. The circuit in Figure 1 shows the Superdense Coding Circuit. Here, the left side is considered as Alice's end and the right side is considered as Bob's end. Both the ends has a Hadamard gate, ***H*** as well as a controlled-NOT gate, ***CNOT***. These two gates are used to create or break entangled states. The circuit separates the composite qubits from $|00\rangle$ to $|0\rangle \otimes |0\rangle$. This is because, the first half of the pair is considered as Alice's half, using which she will encrypt her message and the second half of the pair is considered as Bob's half, using which he will decrypt the message. The two classical bits are used to determine which unitary gate operations, ***Y***, ***Z***, ***X***, ***XZ***, ***YZ*** or ***I*** is used to encrypt the message. In the above circuit, we can see that 00 is the classical input, for which only ***I*** will be used to encrypt the message. Here, ***I*** gate is known as an identity matrix gate and can be translated as *"no gate operation is required to encrypt the classical bits"*, which is why the ***I*** gate is usually not shown in the circuit. The separation of qubits and sending Bob his share of the pairs is one of the key components of Superdense Coding Circuit.

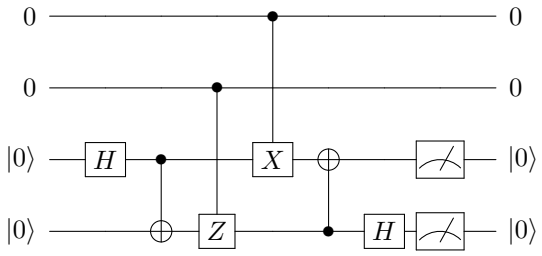


Fig. 1: Superdense Coding circuit

Contrary to SDC, in S-DNA-C, the two classical bits and qubits are encoded by a single DNA letter. This changes the SDC circuit in a significant way by dividing the circuit over two quantum channels. Figure 2 shows Quantum Channel 1. This channel will be used as an authentication channel, since Alice will send the least frequent DNA basis that appears in the strand to Bob, for him to create the corresponding carrier bell state. Here, the channel has both a forward (top line) and backward (bottom line) path, connecting at Bob's end, allowing Bob to send the corresponding carrier bell state to Alice using the backward path. The creation of the DNA encoded carrier bell state is shown in Appendix B. Using this channel, both Alice and Bob will be aware of the least frequent DNA basis that appears in the strand and based on Table IV, Alice will be aware of the corresponding bell state that will

Initial Bell States	$\|C\rangle$	$\|T\rangle$	$\|A\rangle$	$\|G\rangle$
$\|\beta_C\rangle$	$\boldsymbol{I}$ ($\|\beta_C\rangle$)	$\boldsymbol{X}$ ($\|\beta_T\rangle$)	$\boldsymbol{Y}$ ($\|\beta_A\rangle$)	$\boldsymbol{Z}$ ($\|\beta_G\rangle$)
$\|\beta_T\rangle$	$\boldsymbol{X}$ ($\|\beta_C\rangle$)	$\boldsymbol{I}$ ($\|\beta_T\rangle$)	$\boldsymbol{Z}$ ($\|\beta_A\rangle$)	$\boldsymbol{Y}$ ($\|\beta_G\rangle$)
$\|\beta_A\rangle$	$\boldsymbol{XZ}$ ($\|\beta_C\rangle$)	$\boldsymbol{Z}$ ($\|\beta_T\rangle$)	$\boldsymbol{I}$ ($\|\beta_A\rangle$)	$\boldsymbol{YZ}$ ($\|\beta_G\rangle$)
$\|\beta_G\rangle$	$\boldsymbol{Z}$ ($\|\beta_C\rangle$)	$\boldsymbol{XZ}$ ($\|\beta_T\rangle$)	$\boldsymbol{YZ}$ ($\|\beta_A\rangle$)	$\boldsymbol{I}$ ($\|\beta_G\rangle$)

TABLE V: The Bell States before and after the unitary gate operations are applied based on the DNA basis that activates these gate operations in S-DNA-C technique.

be created by Bob. If Alice receives the carrier bell state that she is expecting from Bob, only then will she authenticate to move on to Quantum Channel 2 or else she will break the communication to restart it again. Therefore, it is assumed that Quantum Channel 1 is not affected by noise, cannot be eavesdropped or tampered due to ***no-cloning theorem*** and also acts as an authentic channel for two parties involved. Any changes to the DNA basis or the bell state will notify either party of an untrusted party involved in the communication, thus maintaining ***integrity***.

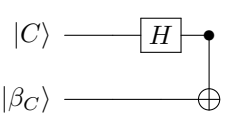


Fig. 2: S-DNA-C circuit for Quantum Channel 1

In SDC, it is said that in order to transmit two classical bits, only one qubit is required, i.e. Bob's share of the Bell pairs, to decrypt. That is, the SDC circuit requires another path to send his share of the pairs, from Alice, as well as two extra paths for the two classical bits to be encrypted. In order to compress the circuit in Fig. 1 and use only two paths for transmission instead of four (four horizontal lines in Fig. 1), the circuit is divided into two different channels, thus reducing the operational or encryption load of Alice. This means that Alice do not need to create the carrier bell state and, at the same time, send Bob the qubit halves to decrypt. Rather, Quantum Channel 1 will allow Bob to create the bell state and send to Alice, for encrypting the equivalent DNA basis of the classical DNA letter, that encodes two classical bits as part of the strand. This compresses the SDC circuit by eliminating the transmission of Bob's share of the pairs. SDC technique is often simply defined as, *"One qubit is used to transmit two classical bits"*. Here, the computational basis, $|00\rangle$, equivalent of two classical bits, 00, is encoded by a single DNA basis, $|C\rangle$. Thus, we can say, that indeed only one qubit was needed to transmit two classical bits.

After authentication, Alice will use the carrier bell state sent by Bob, which can be any one of the four *maximally entangled* DNA encoded Bell states, from eqn. 9 to 12, to encode the DNA basis states that will be transmitted to Bob through Quantum Channel 2, as shown in Figure 3. The circuit in Figure 3. has two paths. The top path works as a control switch for the unitary gate operations, which means, depending on the DNA basis passed, the unitary gates will be activated to encrypt, using the DNA encoded Bell State passed in the bottom path. Also, the DNA basis used will act as the control qubit of the CNOT gate required to break the bell state at Bob's end. The bottom path is used to carry the unitary operations, switched on from the top path, as well as breaking the DNA encoded bell state at Bob's end using the control qubit from the top path. As mentioned earlier, Alice has received the bell state from Bob using Channel 1 and will use this bell state along with the DNA basis from the strand to carry out the unitary operations.

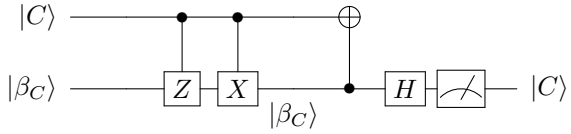


Fig. 3: S-DNA-C circuit for Quantum Channel 2

Table V shows the gates that will be activated, based on the DNA basis, that will be encrypted, using the bell state received, i.e. initial bell states. Here, $\boldsymbol{Y} = \boldsymbol{ZX}$, to show the combined effect of using both the $\boldsymbol{X}$ and $\boldsymbol{Z}$ gates. The mathematical steps of SDC used in [11] to encrypt and decrypt, using these unitary gates, is also used in the S-DNA-C technique as shown in Appendix C. The only difference is the order of the sequence of the unitary gate operations to maintain the complementary rule of the DNA bases. Therefore, the gates activated by the DNA basis states and the changes in the bell states (shown inside the brackets in Table V) to encrypt them using the bell state, $|B_C\rangle$, is shown in the second row of Table V.

As mentioned earlier, the *I* gate operation does not perform any operation, which is why the DNA basis, $|C\rangle$, is encrypted to the bell state, $|B_C\rangle$, i.e. the bell state remains the same. The advantage of using the least frequent DNA base to create the carrier bell state in Channel 1, is to make the coded message more complex and random, since it increases the complexity of the unitary operations required to encrypt the plaintext and decrypt the coded message. Contrary to this, if the most frequent DNA base was selected, then the complexity of the operations will reduce since the carrier bell state will use an *I* gate to encrypt the most frequent base, i.e. there is no unitary operation required to encrypt the most frequent DNA basis state.

To distinguish between the DNA basis states, the circuit in Figure 4 is shown for the DNA basis, $|A\rangle$. Using the *X* gate operation, the carrier bell state, $|B_C\rangle$, is changed to $|B_A\rangle$, to encrypt, $|A\rangle$. Therefore, the coded message will be DNA

encoded Bell States being sent over Quantum Channel 2 to Bob, as shown below.

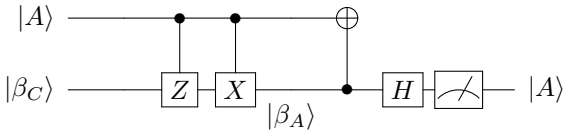


Fig. 4: S-DNA-C circuit for Quantum Channel 2

MQSense = $|T\rangle|A\rangle|A\rangle|C\rangle$ $|T\rangle|A\rangle|T\rangle|T\rangle$ $|T\rangle|A\rangle|G\rangle|C\rangle$ $|T\rangle|A\rangle|G\rangle|C\rangle$ $|T\rangle|A\rangle|G\rangle|G\rangle$.

CodedMSG = $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_A\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_T\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_G\rangle$

C. Noise is not always bad! - Quantum Noise and it's effect on the Bell States

In order to understand the practical effects of noise in quantum systems, it is important to analyze the types of noise that occurs on the bell states in the channels. These noises are known as bit flip, phase flip and both bit and phase flips at the same time. There are other noises that can occur as well, however, these noises are the most common ones to occur in any quantum channel. Since, the proposed cryptosystem consist of a noisy quantum channel, Quantum Channel 2, the models of noise mentioned in Table VI and VII will be applied to only this channel to show tampering of the DNA encoded Bell States message.

It should be noted that the (-) sign before the bell states has been dropped, since it has no observable effect and can only be introduced in case of global phase shifts. Also, some columns or flips have been omitted because, in those cases, it was seen that there is no *maximally* entangled bell states after such noises, in which case the only solution is to halt the communication and restart it again.

	Bell States after being affected by noise flips		
	X Error	Z Error	
Initial Bell States	Bit Flip	Either Phase Flips	Both Phase Flips
$\|\beta_C\rangle$	$\|\beta_T\rangle$	$\|\beta_G\rangle$	$\|\beta_C\rangle$
$\|\beta_T\rangle$	$\|\beta_C\rangle$	$\|\beta_A\rangle$	$\|\beta_T\rangle$
$\|\beta_A\rangle$	$\|\beta_G\rangle$	$\|\beta_T\rangle$	$\|\beta_A\rangle$
$\|\beta_G\rangle$	$\|\beta_A\rangle$	$\|\beta_C\rangle$	$\|\beta_G\rangle$

TABLE VI: Effects of a single noise flip on bell states in a noisy quantum channel

In Table VI, it shows the noise flips that occurs one at a time, that is, either the bits will flip, *X* error, or the phases will flip, *Z* error, but not both of them together. So we can say that the quantum channel is a bit-flip channel or a phase-flip channel. For bit-flip channel, it can be seen that the bell states after the noise effect has no relation with the initial bell states and can be said to have the highest level of noise. However, for phase-flip channel, when either the 1st or the 2nd phase of the bell pairs are flipped, it can be seen that the initial bell states are flipped to it's complementary bell states. Lastly, in case of flipping both the phases, there is no change in the initial bell states and can be used further for rest of decryption steps.

Initial Bell States	Bell States after being affected by XZ error			
$\|\beta_C\rangle$	$\|\beta_A\rangle$	$\|\beta_G\rangle$	$\|\beta_T\rangle$	$\|\beta_C\rangle$
$\|\beta_T\rangle$	$\|\beta_G\rangle$	$\|\beta_A\rangle$	$\|\beta_C\rangle$	$\|\beta_T\rangle$
$\|\beta_A\rangle$	$\|\beta_C\rangle$	$\|\beta_T\rangle$	$\|\beta_G\rangle$	$\|\beta_A\rangle$
$\|\beta_G\rangle$	$\|\beta_T\rangle$	$\|\beta_C\rangle$	$\|\beta_A\rangle$	$\|\beta_G\rangle$

TABLE VII: Effects of multiple noise flips on bell states in a noisy quantum channel

In Table VII, moving towards a more practical effect of noises, it shows the noise flips working concurrently, that is, both bit and phase flips working together. These channels are known as Bit-Phase flip quantum channels. Here, we can see that the effects are similar, with different combinations of bit and phase flips, to what we have seen in Table VI. The only exception is an added column of high noise effect that occurs only in this channel. Therefore, from the above analysis of Table VI and VII, the noise effects can be categorized as: *No Change in the Bell States*, *Complementary Bell States* and *High Level of Noise*. The changes in the Bell States before and after noises is shown in details in Appendix D.

No Change in the Bell states:

Coded message before noise: $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_A\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_T\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_G\rangle$

Coded message after noise: $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_A\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_T\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_G\rangle$

As we can see, that both the messages are same and can be used without any changes required.

Complementary Bell States:

Coded message before noise: $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_A\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_T\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_G\rangle$

Coded message after noise: $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_T\rangle$ $|\beta_G\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_A\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_C\rangle$ $|\beta_G\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_C\rangle$ $|\beta_G\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_C\rangle$ $|\beta_C\rangle$

As we can see, that the messages are complementary to each other. Here, Bob will decrypt the message received after the noise and get the strand given below,

MAntiSense = ATTG ATAA ATCG ATCG ATCC

Here, Bob will notice that, G, is the least frequent DNA letter that occurs in the strand, whereas, the least frequent DNA basis he received from Alice was, $|C\rangle$, equivalent to C from Channel 1. Since, in classical DNA letters, C and G are complementary to each other, Bob will know that he has received the antisense strand, due to noise, instead of the sense strand. Therefore, he will convert the antisense strand to sense strand given below and will carry on the rest of the decryption phase.

MSense = TAAC TATT TAGC TAGC TAGG

Highest Level of Noise:

Coded message before noise: $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_A\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_T\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_G\rangle$

Coded message after noise: $|\beta_C\rangle$ $|\beta_G\rangle$ $|\beta_G\rangle$ $|\beta_T\rangle$ $|\beta_C\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_C\rangle$ $|\beta_C\rangle$ $|\beta_G\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_C\rangle$ $|\beta_G\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_C\rangle$ $|\beta_G\rangle$ $|\beta_A\rangle$ $|\beta_A\rangle$

As we can see, that the messages have no relation to each other and can be said to be completely tampered by noise. Bob will decrypt the message received after the noise and get the strand given below:

M = CGGT CGCC CGAT CGAT CGAA

Here, Bob will notice that, T, is the least frequent DNA letter that occurs in the strand, whereas the least frequent DNA basis he received from Alice was, $|C\rangle$, equivalent to C from Channel 1. Therefore, he will interchange T with C and vice versa, also he will interchange G with A and vice versa to get the sense strand below.

MSense = TAAC TATT TAGC TAGC TAGG

For another type of high noise effect, the example given below shows the coded message before and after it's affected by the noise.

Coded message before noise: $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_A\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_T\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_G\rangle$

Coded message after noise: $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_C\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_G\rangle$ $|\beta_G\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_T\rangle$

Again, the messages have no relation to each other and can be said to be completely tampered by noise. Here, Bob will decrypt the message received after the noise and get the strand given below:

M = GCCA GCGG GCTA GCTA GCTT

Here, Bob will notice that, A, is the least frequent DNA basis that occurs in the strand, whereas the least frequent DNA basis he received from Alice was, $|C\rangle$, equivalent of C from Channel 1. Therefore, he will interchange A with C and vice versa, also he will interchange T with G and vice versa to get the sense strand below and can proceed further with the decryption phase.

MSense = TAAC TATT TAGC TAGC TAGG

Here, we have shown that not all noises are bad and the coded message is still retrievable, due to the biological functionality of the cryptosystem. This analysis is important to understand the effects of a noisy quantum channel. There are many classical or quantum error correcting codes proposed for mitigating such noises but all these codes relies on the use of extra qubits known as ancilla qubits or 9-Qubits in Shor's algorithm to detect and fix such noises. This increases the data redundancy that was initially mitigated, in our cryptosystem, and further complicates the encoding rules of DNA letters for classical bits or qubits. Therefore, it was seen that, despite such noises occurring on the coded message, without using any error correction code, the receiver can still retrieve the original message by using the biological functionality of the DNA system.

D. Decryption Phase - Continuing from Encryption to Decryption

Algorithm 2: Decryption Procedure

Step 1: Convert the DNA Bell state coded message into DNA basis sequence using Controlled-NOT gate followed by Hadamard gate.
Step 2: Convert the DNA basis sequence to it's equivalent classical DNA strand.
Step 3: Check whether the least frequent DNA letter previously shared matches with the least frequent DNA letter of the current DNA strand. If it does, then go to Step 6 or else continue with Step 4.
Step 4: Label the DNA strand as noisy or hacked DNA strand.
Step 5: Interchange the current least frequent DNA letter with previous least frequent DNA letter as well as interchange the other two remaining DNA letters to retrieve the DNA sense strand.
Step 6: Label the DNA strand as DNA Sense strand to convert it to ASCII Binary.
Step 7: Convert the ASCII Binary (PBIN) into Plain text message, P.

IV. Hacking S-DNA-C using Bijection Attacks

While eavesdropping on quantum communications is an important goal for hackers, other types of cyberattacks on quantum computers and communications are possible for which a hacker's intention is not to eavesdrop, but rather to disrupt quantum networked computation and quantum communications. We assume S-DNA-C in an automated setting, where the users do not directly access the quantum gates but, instead, operate on a high-level classical user interface, such that the whole translation of the classical message to the quantum framework is done automatically. In this setting, a hacker can attack different nodes in S-DNA-C, in order to change the sent message without eavesdropping on the circuit, leading to a bijective recoding of the message to be sent. This type of attack to the S-DNA-C protocol that we address here, is known as a *bijection attack* [18]. We assume that the attack is done on a noiseless communication network.

Bijection attack changes the automated gate sequence definition software. Let us assume, Eve has managed to get malware installed on Alice's part in S-DNA-C, so that the automated S-DNA-C protocol is modified. We will consider here the effect of elementary gates in disrupting S-DNA-C, so that we will

be working, for now, with a single gate operation malware. Since the hack takes the form of a single unitary gate, Eve is not eavesdropping on Alice or Bob. The automated quantum operation introduced by the malware is the same whatever the sequence of gates implemented on Alice's side, the protocol is, in this way, disrupted without Eve having to eavesdrop on Alice and Bob. The possible unitary gate insertion or *injection* versions are discussed below.

For our first two versions, let's say Eve injects an X or a Z gate at the end of Alice's operations as shown in Figure 5 and 6. Table VIII and IX shows the changes made to the bell states after adding either X or Z gate at the end of Alice's operations.

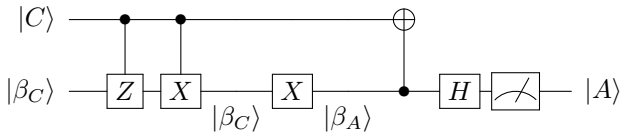


Fig. 5: X gate at the end

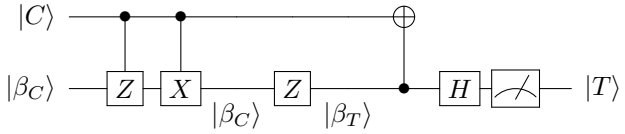


Fig. 6: Z gate at the end

Initial DNA	Initial Bell State	Changed Bell State	Final DNA
$\|C\rangle$	$\|\beta_C\rangle$	$\|\beta_A\rangle$	$\|A\rangle$
$\|T\rangle$	$\|\beta_T\rangle$	$\|\beta_G\rangle$	$\|G\rangle$
$\|A\rangle$	$\|\beta_A\rangle$	$\|\beta_C\rangle$	$\|C\rangle$
$\|G\rangle$	$\|\beta_G\rangle$	$\|\beta_T\rangle$	$\|T\rangle$

TABLE VIII: Effects of a Bijection attack where an X gate was placed at the end of Alice's operations.

Initial DNA	Initial Bell State	Changed Bell State	Final DNA
$\|C\rangle$	$\|\beta_C\rangle$	$\|\beta_T\rangle$	$\|T\rangle$
$\|T\rangle$	$\|\beta_T\rangle$	$\|\beta_C\rangle$	$\|C\rangle$
$\|A\rangle$	$\|\beta_A\rangle$	$\|\beta_G\rangle$	$\|G\rangle$
$\|G\rangle$	$\|\beta_G\rangle$	$\|\beta_A\rangle$	$\|A\rangle$

TABLE IX: Effects of a Bijection attack where a Z gate was placed at the end of Alice's operations.

Here, the changes in the Bell states is similar to the noise effects we have discussed in the previous section, as seen in Table VI and Table VII. In order to retrieve the original strand sent by Alice, Bob needs to use the same approach of interchanging DNA letters, based on the least frequent DNA letter in the strand.

Therefore, for X gate malware attack, based on Table VIII, Bob will receive the coded message, which he will decrypt to get the strand shown below.

Hacked Message: $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_C\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_G\rangle$ $|\beta_G\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_A\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_T\rangle$

Hacked Strand = GCCA GCGG GCTA GCTA GCTT

He will interchange A, the least frequent DNA basis that occurs in the strand, with C, the least frequent DNA basis in the original message, and vice versa. Also, he will interchange T with G and vice versa to get the sense strand below to proceed further.

MSense = TAAC TATT TAGC TAGC TAGG

Similarly, for Z gate malware attack, based on Table IX, Bob will receive the coded message, which he will decrypt to get the strand shown below.

Hacked Message: $|\beta_C\rangle$ $|\beta_G\rangle$ $|\beta_G\rangle$ $|\beta_T\rangle$ $|\beta_C\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_C\rangle$ $|\beta_C\rangle$ $|\beta_G\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_C\rangle$ $|\beta_G\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_C\rangle$ $|\beta_G\rangle$ $|\beta_A\rangle$ $|\beta_A\rangle$

Hacked Strand = CGGT CGCC CGAT CGAT CGAA

He will interchange T, the least frequent DNA basis that occurs in the strand, with C, the least frequent DNA basis in the original message, and vice versa. Also, he will interchange G with A and vice versa to get the sense strand below to proceed further.

MSense = TAAC TATT TAGC TAGC TAGG

This is one way to retrieve the original message from a hacked message without the hacker knowing that the original message was retrieved. This also provides a method to detect a malware attack in the automated gates operations of S-DNA-C and retrieving the message automatically without the receiver, even knowing that they were attacked. However, there are malware attacks, where the approach to retrieve the original message is not as straightforward as it was for the examples discussed above. Below we shall see two more examples of malware attacks, where the X or Z gates are added at the beginning of Alice's operations. This changes the DNA basis states, which further complicates the gates operations as shown below.

For our second two versions, let's say Eve injects an X or a Z gate at the beginning of Alice's operations as shown in Figure 7 and 8. Table X and XI shows the changes made to the bell states after adding either X or Z gate at the beginning of Alice's operations.

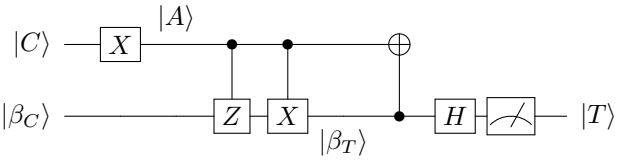


Fig. 7: X gate at the beginning

The changes in the DNA basis states as well as the Bell State, when an X gate is placed at the beginning of Alice's operations, is shown in Table X. In order to retrieve the

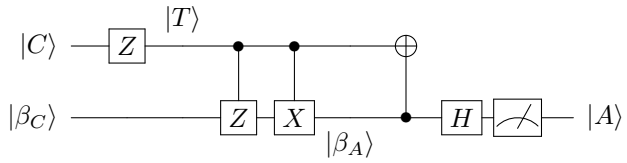


Fig. 8: Z gate at the beginning

Initial DNA	Changed DNA	Bell State	Final DNA
$\|C\rangle$	$\|A\rangle$	$\|\beta_T\rangle$	$\|T\rangle$
$\|T\rangle$	$\|G\rangle$	$\|\beta_G\rangle$	$\|G\rangle$
$\|A\rangle$	$\|C\rangle$	$\|\beta_C\rangle$	$\|C\rangle$
$\|G\rangle$	$\|T\rangle$	$\|\beta_A\rangle$	$\|A\rangle$

TABLE X: Effects of a Bijection attack where an X gate was placed at the beginning of Alice's operations.

Initial DNA	Changed DNA	Bell State	Final DNA
$\|C\rangle$	$\|T\rangle$	$\|\beta_A\rangle$	$\|A\rangle$
$\|T\rangle$	$\|C\rangle$	$\|\beta_C\rangle$	$\|C\rangle$
$\|A\rangle$	$\|G\rangle$	$\|\beta_G\rangle$	$\|G\rangle$
$\|G\rangle$	$\|A\rangle$	$\|\beta_T\rangle$	$\|T\rangle$

TABLE XI: Effects of a Bijection attack where a Z gate was placed at the beginning of Alice's operations.

original message, first, we will use the same approach of interchanging the DNA letters, based on the least frequent DNA letter, as shown below.

Hacked Message: $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_C\rangle$ $|\beta_T\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_G\rangle$ $|\beta_G\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_A\rangle$ $|\beta_T\rangle$ $|\beta_G\rangle$ $|\beta_C\rangle$ $|\beta_A\rangle$ $|\beta_A\rangle$

Hacked Strand = GCCT GCGG GCAT GCAT GCAA

Here, Bob will interchange T, the least frequent DNA basis that occurs in the hacked strand with C, the least frequent DNA basis in the original message, and vice versa as well as A with G, to get the strand below.

M = ATTC ATAA ATGC ATGC ATGG

Unlike in previous examples, we are still not being able to retrieve the original message with a straightforward approach of interchanging the DNA letters. Therefore, in this case, in order to fully retrieve the message, we will only complement the DNA letters, A and T, while keeping C and G as they are, as shown below.

MSense = TAAC TATT TAGC TAGC TAGG

As we can see, we were able to retrieve the original message by first interchanging the DNA letters and then complementing only the *anti-correlated pairs*, in this case A and T. A similar approach can be taken for Table XI, i.e. Z gate attack at the beginning of Alice's operations, as shown below.

Hacked Strand = CGGA CGCC CGTA CGTA CGTT

Interchanging A with C and T with G gives us the strand below.

M = ATTC ATAA ATGC ATGC ATGG

As we can see, this strand is similar to the one discussed above and the same approach of complementing just the *anti-correlated pairs*, A and T, will retrieve the original message.

MSense = TAAC TATT TAGC TAGC TAGG

V. Experimental Result

In this section, we have shown the performance of the proposed cryptosystem based on the encryption and decryption times that are used to evaluate the performance of this cryptosystem. The proposed system was tested on Intel(R) Core (TM) i5-1135G7 CPU @ 2.40 GHz personal computer with 8 GB RAM. The implementation was carried out with Python IDLE 3.12.0. We have experimented on a message kept in a file of different size of kilobytes. The message contains letters, symbols and numbers.

A. Used Dataset

The Plaintext UTF-8 version of ten e-books, shown in Table XII and XIII, were stored in a file and used as they are publicly available from Project Gutenburg [19]. In Table XII, the left-most column shows the name of the books and the middle column shows the size of the plaintext UTF-8 files. Here, we have chosen e-books of size less than 100KB. The right-most column shows the exact number of characters in the e-books.

E-Book name	Size of Plaintext(KB)	Tot. no. of Chars.
Feeding the Mind	37	36,879
Songs of Innocence	51	50,678
The Nursery Alice	68	67,992
Peter Pan	78	77,783
Tom Sawyer	89	88,675

TABLE XII: Specification of five e-book texts $<$ 100KB used in our experiment.

B. Summary of Findings

Fig. 9, 10 and 11 displays the experimental results in terms of encryption and decryption times to evaluate the system's performance. Keep in mind, these results were evaluated on a classical computer, as quantum computers have not adapted such a Qubit system, i.e. *DNA Basis*, mentioned earlier. The classical representation of quantum unitary gate operations as well as Hadamard and Controlled-NOT gates were done using 4 x 4 matrix. Computing such matrices requires a high time complexity in classical computers compared to a quantum computer, which is why it can be assumed that these results will be much more efficient on a quantum computer, which can easily compute such matrices. Our result shows that the encryption time of S-DNA-C is less than or almost half of the decryption time it takes to break the DNA bell states, in a noiseless quantum channel. However, the decryption time is more in case of noisy quantum channels, since the cryptosystem further uses noisy DNA strand to interchange DNA bases, as discussed in Section III.C, based on the least frequent DNA letter, to retrieve the DNA sense strand. For high noise type 1 and 2, the decryption time is higher than the

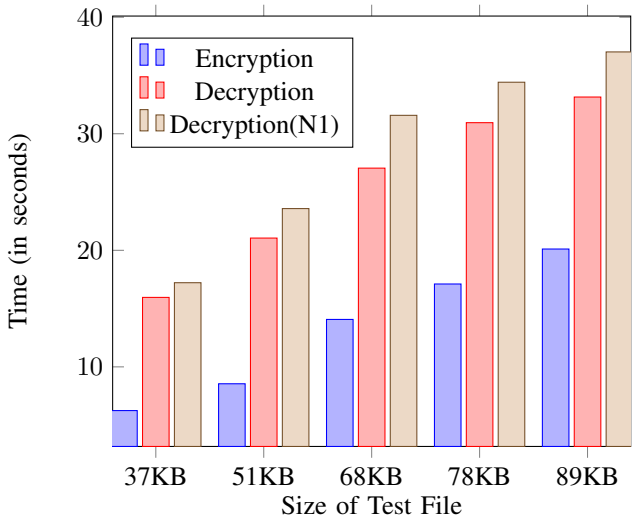


Fig. 9: Encryption and Decryption times of S-DNA-C in a noiseless quantum channel, high noise type 1 (N1) channel for different file sizes $<$ 100KB

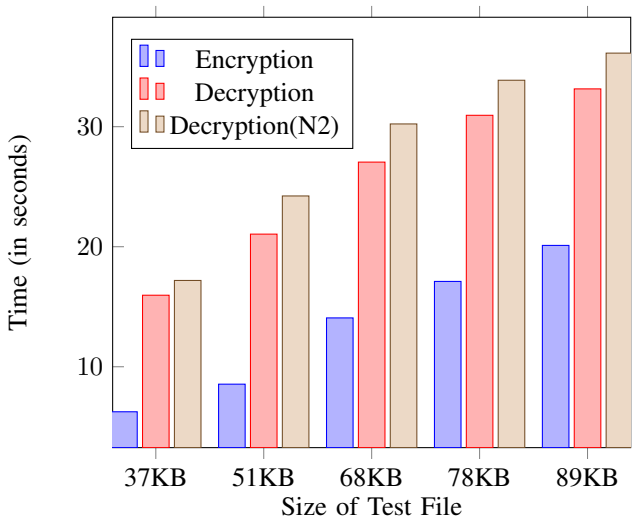


Fig. 10: Encryption and Decryption times of S-DNA-C in a noiseless quantum channel, high noise type 2 (N2) channel for different file sizes $<$ 100KB

decryption time in case of complementary type of noise effect. We have chosen files of size $<$ 100KB data, since the total time of encrypting the plaintext as well as decrypting the coded message takes around 30 seconds, on average, to complete. As the file size increases, the DNA sequence length increases

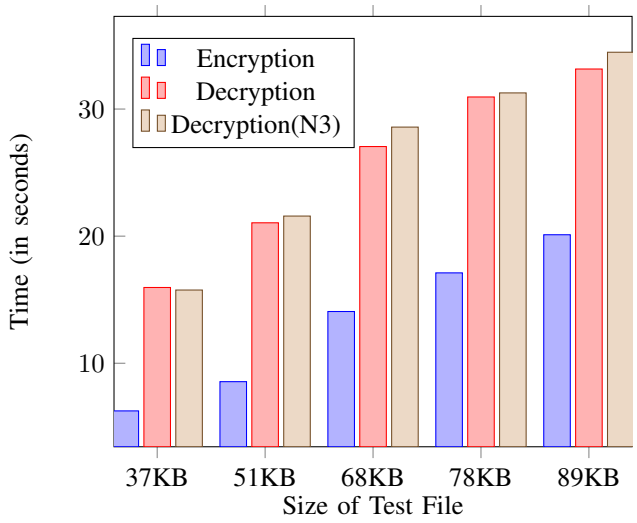


Fig. 11: Encryption and Decryption times of S-DNA-C in a noiseless quantum channel, complementary noise type (N3) channel for different file sizes $<$ 100KB

as well as the encryption and decryption time of S-DNA-C are affected. Therefore, we can say that the DNA sequence's length is directly proportional to the execution time.

Table XIII shows the experimental results in terms of encryption and decryption times for other five e-books of sizes $>$ 100KB to 1MB. Here, as discussed above, the decryption times are almost double that of the encryption times with the total execution time reaching almost 9 minutes. These simulations are assumed to perform more efficiently when conducted on a quantum computer, instead of a classical computer, as it will utilize the high storage capacity as well as the high transmission rate of quantum computers. As the file size increases in Table XIII, the DNA sequence that encodes also increases and in turn, the decryption of DNA Bell States, one at a time, also increases. Thus, increasing the overall execution time to show us the trade-off between security and efficiency for this cryptosystem.

VI. Conclusion

In this paper, a novel symmetric cryptosystem is proposed based on the Superdense Coding technique. S-DNA-C shows the potential of incorporating two major cryptography fields: DNA and Quantum Cryptography while maintaining a decent level of security. *Confidentiality* is maintained throughout the system with a triple layer security and an authentic channel maintains *integrity* between the parties involved during

E-Book name	Size of Plaintext(KB)	Encryption Time(Sec)	Decryption Time(Sec)
Little Women	1100	192.35	529.90
Wuthering Heights	854	147.57	447.30
Pride and Prejudice	681	116.50	302.31
The Adventures of Sherlock Holmes	424	98.35	219.90
The Hound of Baskervilles	379	50.29	107.14

TABLE XIII: Specification and Experimental Results of five e-book texts $>$ 100KB to 1.1MB used in our experiment.

communication. An automated setting of S-DNA-C shows how a noisy or hacked message can be used to retrieve the original message by interchanging DNA letters, thus providing *availability* of the system. The proposed method is blind since the system is inspired from *Quantum Secure Direct Communication* with no keys exchange involved. It is quite impossible to break the system without having full knowledge of the pre-information shared and the steps involved for a particular encryption rule. The proposed cryptosystem can be modified in our future work to increase its DNA steganography capabilities and security, in order to transmit large data while utilizing the high storage capacity of quantum computers and efficient data transmission rate of DNA cryptography and steganography.

REFERENCES

[1] S. Hassan, M. A. Muztaba, M. S. Hossain, and H. S. Narman, "A hybrid encryption technique based on dna cryptography and steganography," in *2022 IEEE 13th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 0501–0508, IEEE, 2022.

[2] H. R. Shakir, S. A. A. Mehdi, and A. A. Hattab, "Chaotic-dna system for efficient image encryption," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 5, pp. 2645–2656, 2022.

[3] N. A. N. Abdullah, N. H. Zakaria, A. H. Ab Halim, F. H. M. Ridzuan, A. Ahmad, K. Seman, and S. Ariffin, "a theoretical comparative analysis of dna techniques used in dna based cryptography," *Journal of Sustainability Science and Management*, 2022.

[4] B. T. Hammad, A. M. Sagheer, I. T. Ahmed, and N. Jamil, "A comparative review on symmetric and asymmetric dna-based cryptography," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 6, pp. 2484–2491, 2020.

[5] M. Mondal and K. S. Ray, "Review on dna cryptography," *arXiv preprint arXiv:1904.05528*, 2019.

[6] A. Hazra, S. Ghosh, and S. Jash, "A review on dna based cryptographic techniques.," *Int. J. Netw. Secur.*, vol. 20, no. 6, pp. 1093–1104, 2018.

[7] R. Renner and R. Wolf, "Quantum advantage in cryptography," *AIAA Journal*, vol. 61, no. 5, pp. 1895–1910, 2023.

[8] M. Mastriani, "Quantum key secure communication protocol via enhanced superdense coding," *Optical and Quantum Electronics*, vol. 55, no. 1, p. 10, 2023.

[9] Z. Hu and S. Kais, "A quantum encryption design featuring confusion, diffusion, and mode of operation," *Scientific Reports*, vol. 11, no. 1, p. 23774, 2021.

[10] J. Li, H. Li, N. Wang, C. Li, Y. Hou, X. Chen, and Y. Yang, "A quantum key distribution protocol based on the epr pairs and its simulation," *Mobile Networks and Applications*, vol. 26, pp. 620–628, 2021.

[11] O. M. Hegazy, A. M. Bahaa-Eldin, and Y. H. Dakroury, "Quantum secure direct communication using entanglement and super dense coding," *arXiv preprint arXiv:1402.6219*, 2014.

[12] X. Li and D. Zhang, "Quantum public-key cryptosystem based on super dense coding technology.," *J. Comput.*, vol. 8, no. 12, pp. 3168–3175, 2013.

[13] R. B. Griffiths, "Dense coding, teleportation, no cloning,"

[14] S. J. Lomonaco Jr, "A talk on quantum cryptography or how alice outwits eve," in *Coding Theory and Cryptography: From Enigma and Geheimschreiber to Quantum Theory*, pp. 144–174, Springer, 2002.

[15] N. Innan and M. Al-Zafar Khan, "Classical-to-quantum sequence encoding in genomics," *arXiv e-prints*, pp. arXiv–2304, 2023.

[16] B. Kösoglu-Kind, R. Loredo, M. Grossi, C. Bernecker, J. M. Burks, and R. Buchkremer, "A biological sequence comparison algorithm using quantum computers," *arXiv e-prints*, pp. arXiv–2303, 2023.

[17] A. Sarkar, Z. Al-Ars, and K. Bertels, "Estimating algorithmic information using quantum computing for genomics applications," *Applied Sciences*, vol. 11, no. 6, p. 2696, 2021.

[18] C. P. Gonçalves, "Cyberattacks on quantum networked computation and communications–hacking the superdense coding protocol on ibm's quantum computers," *arXiv preprint arXiv:2105.07187*, 2021.

[19] Michael Hart, "Project gutenberg." https://gutenberg.org/ebooks/, 1971. Online, accessed 30th January 2024.

APPENDIX

A. How DNA Basis is an Orthonormal Basis

$$|C\rangle = \frac{1}{\sqrt{2}}(\Phi^+ + \Phi^-) = |C\rangle \tag{13}$$

$$|T\rangle = \frac{1}{\sqrt{2}}(\Psi^+ + \Psi^-) = |T\rangle \tag{14}$$

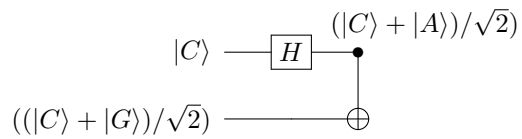
$$|A\rangle = \frac{1}{\sqrt{2}}(\Psi^+ - \Psi^-) = |A\rangle \tag{15}$$

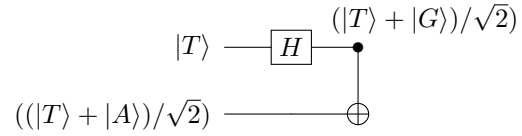
$$|G\rangle = \frac{1}{\sqrt{2}}(\Phi^+ - \Phi^-) = |G\rangle \tag{16}$$

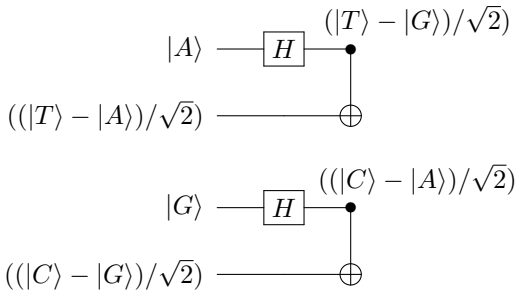
$$\text{State Vector: } \begin{bmatrix} |C\rangle \\ |T\rangle \\ |A\rangle \\ |G\rangle \end{bmatrix}$$

B. How DNA encoded Bell States are created from DNA Basis

We know that a *Hadamard gate* acts on a single qubit and a *CNOT gate* acts on two qubits or more. Below, we have shown that a single qubit, $|C\rangle$, is passed through a Hadamard gate to create an entangled system of two qubits, $|C\rangle$ and $|A\rangle$. Here, $|C\rangle$, one part of correlated pairs, and $|T\rangle$, one part of anti-correlated pairs, acts as the *control qubit* for the CNOT gate, which is why they remain the same for all four basis and depending on this qubit, the second qubit, $|A\rangle$ is changed to $|G\rangle$, for correlated pairs and $|G\rangle$ is changed to $|A\rangle$ for anti-correlated pairs, by performing the *NOT* operation of the CNOT gate. In the figures given below, we can see the changes that occurs according to the control qubit.







C. How a DNA basis is encrypted by a DNA encoded Bell State in S-DNA-C protocol

$$\boldsymbol{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \boldsymbol{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \boldsymbol{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \boldsymbol{Y} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

State Vector: $\begin{bmatrix} |C\rangle \\ |T\rangle \\ |A\rangle \\ |G\rangle \end{bmatrix}$

$|C\rangle$:

$$(\boldsymbol{I} \otimes \boldsymbol{I})|\beta_C\rangle = (1/\sqrt{2}) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} |C\rangle \\ 0 \\ 0 \\ |G\rangle \end{bmatrix}$$

$$= (1/\sqrt{2}) \begin{bmatrix} |C\rangle \\ 0 \\ 0 \\ |G\rangle \end{bmatrix} = |\beta_C\rangle$$

$|T\rangle$:

$$(\boldsymbol{X} \otimes \boldsymbol{I})|\beta_C\rangle = (1/\sqrt{2}) \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} |C\rangle \\ 0 \\ 0 \\ |G\rangle \end{bmatrix}$$

$$= (1/\sqrt{2}) \begin{bmatrix} 0 \\ |T\rangle \\ |A\rangle \\ 0 \end{bmatrix} = |\beta_T\rangle$$

$|A\rangle$:

$$(\boldsymbol{Y} \otimes \boldsymbol{I})|\beta_C\rangle = (1/\sqrt{2}) \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix} \begin{bmatrix} |C\rangle \\ 0 \\ 0 \\ |G\rangle \end{bmatrix}$$

$$= (1/\sqrt{2}) \begin{bmatrix} 0 \\ |T\rangle \\ -|A\rangle \\ 0 \end{bmatrix} = |\beta_A\rangle$$

$|G\rangle$:

$$(\boldsymbol{Z} \otimes \boldsymbol{I})|\beta_C\rangle = (1/\sqrt{2}) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} |C\rangle \\ 0 \\ 0 \\ |G\rangle \end{bmatrix}$$

$$= (1/\sqrt{2}) \begin{bmatrix} |C\rangle \\ 0 \\ 0 \\ -|G\rangle \end{bmatrix} = |\beta_G\rangle$$

Decrypting the DNA encoded Bell State, $|\beta_C\rangle$, using *Hadamard* and *CNOT* gate.

$|\beta_C\rangle$:

$$(\boldsymbol{H} \otimes \boldsymbol{CNOT})|\beta_C\rangle$$

$$= (1/\sqrt{2}) \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix} (1/\sqrt{2}) \begin{bmatrix} |C\rangle \\ 0 \\ 0 \\ |G\rangle \end{bmatrix}$$

$$= (1/2) \begin{bmatrix} |C\rangle + |G\rangle \\ 0 \\ 0 \\ |C\rangle - |G\rangle \end{bmatrix}$$

$$= (1/2)|C\rangle + (1/2)|G\rangle + (1/2)|C\rangle - (1/2)|G\rangle = |C\rangle$$

D. Bit and Phase Flip effects on DNA encoded Bell States

1. Bit-Flip and Phase-Flip Channel changes:

For Bell State: $|\beta_C\rangle$

$|\beta_C\rangle$: $|C\rangle + |G\rangle \xrightarrow[\text{flip}]{\text{1st Bit}} |A\rangle + |T\rangle : |T\rangle + |A\rangle : |\beta_T\rangle$

$|\beta_C\rangle$: $|C\rangle + |G\rangle \xrightarrow[\text{flip}]{\text{2nd Bit}} |T\rangle + |A\rangle : |\beta_T\rangle$

$|\beta_C\rangle$: $|C\rangle + |G\rangle \xrightarrow[\text{flip}]{\text{1st Phase}} - |C\rangle + |G\rangle : - (|C\rangle - |G\rangle) : -|\beta_G\rangle$

$|\beta_C\rangle$: $|C\rangle + |G\rangle \xrightarrow[\text{flip}]{\text{2nd Phase}} |C\rangle - |G\rangle : |\beta_G\rangle$

$|\beta_C\rangle$: $|C\rangle + |G\rangle \xrightarrow[\text{flip}]{\text{Both Bits}} |G\rangle + |C\rangle : |C\rangle + |G\rangle : |\beta_C\rangle$

$|\beta_C\rangle$: $|C\rangle + |G\rangle \xrightarrow[\text{flip}]{\text{Both Phases}} : - (|C\rangle + |G\rangle) : -|\beta_C\rangle$

For Bell State: $|\beta_T\rangle$

$|\beta_T\rangle$: $|T\rangle + |A\rangle \xrightarrow[\text{flip}]{\text{1st Bit}} |G\rangle + |C\rangle : |C\rangle + |G\rangle : |\beta_C\rangle$

$|\beta_T\rangle$: $|T\rangle + |A\rangle \xrightarrow[\text{flip}]{\text{2nd Bit}} |C\rangle + |G\rangle : |\beta_C\rangle$

$|\beta_T\rangle$: $|T\rangle + |A\rangle \xrightarrow[\text{flip}]{\text{1st Phase}} - |T\rangle + |A\rangle : - (|T\rangle - |A\rangle) : -|\beta_A\rangle$

$|\beta_T\rangle$: $|T\rangle$ + $|A\rangle \xRightarrow[\text{flip}]{\text{2nd Phase}} |T\rangle$ - $|A\rangle$: $|\beta_A\rangle$

$|\beta_T\rangle$: $|T\rangle$ + $|A\rangle \xRightarrow[\text{flip}]{\text{Both Bits}} |A\rangle$ + $|T\rangle$: $|T\rangle$ + $|A\rangle$: $|\beta_T\rangle$

$|\beta_T\rangle$: $|T\rangle$ + $|A\rangle \xRightarrow[\text{flip}]{\text{Both Phases}}$: - ($|T\rangle$ + $|A\rangle$) : -$|\beta_T\rangle$

For Bell State: $|\beta_A\rangle$

$|\beta_A\rangle$: $|T\rangle$ - $|A\rangle \xRightarrow[\text{flip}]{\text{1st Bit}} |G\rangle$ - $|C\rangle$: *no maximally entangled Bell State*

$|\beta_A\rangle$: $|T\rangle$ - $|A\rangle \xRightarrow[\text{flip}]{\text{2nd Bit}} |C\rangle$ - $|G\rangle$: $|\beta_G\rangle$

$|\beta_A\rangle$: $|T\rangle$ - $|A\rangle \xRightarrow[\text{flip}]{\text{1st Phase}}$ - $|T\rangle$ - $|A\rangle$: - ($|T\rangle$ + $|A\rangle$) : -$|\beta_T\rangle$

$|\beta_A\rangle$: $|T\rangle$ - $|A\rangle \xRightarrow[\text{flip}]{\text{2nd Phase}} |T\rangle$ + $|A\rangle$: $|\beta_T\rangle$

$|\beta_A\rangle$: $|T\rangle$ - $|A\rangle \xRightarrow[\text{flip}]{\text{Both Bits}} |A\rangle$ - $|T\rangle$: *no maximally entangled Bell State*

$|\beta_A\rangle$: $|T\rangle$ - $|A\rangle \xRightarrow[\text{flip}]{\text{Both Phases}}$: - $|T\rangle$ + $|A\rangle$: - ($|T\rangle$ - $|A\rangle$) : -$|\beta_A\rangle$

For Bell State: $|\beta_G\rangle$

$|\beta_G\rangle$: $|C\rangle$ - $|G\rangle \xRightarrow[\text{flip}]{\text{1st Bit}} |A\rangle$ - $|T\rangle$: *no maximally entangled Bell State*

$|\beta_G\rangle$: $|C\rangle$ - $|G\rangle \xRightarrow[\text{flip}]{\text{2nd Bit}} |T\rangle$ - $|A\rangle$: $|\beta_A\rangle$

$|\beta_G\rangle$: $|C\rangle$ - $|G\rangle \xRightarrow[\text{flip}]{\text{1st Phase}}$ - $|C\rangle$ - $|G\rangle$: - ($|C\rangle$ + $|G\rangle$) : -$|\beta_C\rangle$

$|\beta_G\rangle$: $|C\rangle$ - $|G\rangle \xRightarrow[\text{flip}]{\text{2nd Phase}} |C\rangle$ + $|G\rangle$: $|\beta_C\rangle$

$|\beta_G\rangle$: $|C\rangle$ - $|G\rangle \xRightarrow[\text{flip}]{\text{Both Bits}} |G\rangle$ - $|C\rangle$: *no maximally entangled Bell State*

$|\beta_G\rangle$: $|C\rangle$ - $|G\rangle \xRightarrow[\text{flip}]{\text{Both Phases}}$: - $|C\rangle$ + $|G\rangle$: - ($|C\rangle$ - $|G\rangle$) : -$|\beta_G\rangle$

2. Bit-Phase-Flip Channel changes:

For Bell State: $|\beta_C\rangle$

$|\beta_C\rangle$: $|C\rangle$ + $|G\rangle \xRightarrow[\text{1st Phase flip}]{\text{1st Bit}}$ - $|A\rangle$ + $|T\rangle$: $|T\rangle$ - $|A\rangle$: $|\beta_A\rangle$

$|\beta_C\rangle$: $|C\rangle$ + $|G\rangle \xRightarrow[\text{1st Phase flip}]{\text{2nd Bit}}$ - $|T\rangle$ + $|A\rangle$: $|A\rangle$ - $|T\rangle$: *no maximally entangled Bell State*

$|\beta_C\rangle$: $|C\rangle$ + $|G\rangle \xRightarrow[\text{2nd Phase flip}]{\text{1st Bit}} |A\rangle$ - $|T\rangle$: *no maximally entangled Bell State*

$|\beta_C\rangle$: $|C\rangle$ + $|G\rangle \xRightarrow[\text{2nd Phase flip}]{\text{2nd Bit}} |T\rangle$ - $|A\rangle$: $|\beta_A\rangle$

$|\beta_C\rangle$: $|C\rangle$ + $|G\rangle \xRightarrow[\text{1st Phase flip}]{\text{Both Bits}}$ - $|G\rangle$ + $|C\rangle$: $|C\rangle$ - $|G\rangle$: $|\beta_G\rangle$

$|\beta_C\rangle$: $|C\rangle$ + $|G\rangle \xRightarrow[\text{2nd Phase flip}]{\text{Both Bits}} |G\rangle$ - $|C\rangle$: *no maximally entangled Bell State*

$|\beta_C\rangle$: $|C\rangle$ + $|G\rangle \xRightarrow[\text{1st Bit flip}]{\text{Both Phase}}$ - $|A\rangle$ - $|T\rangle$: - ($|T\rangle$ + $|A\rangle$) : -$|\beta_T\rangle$

$|\beta_C\rangle$: $|C\rangle$ + $|G\rangle \xRightarrow[\text{2nd Bit flip}]{\text{Both Phase}}$ - $|T\rangle$ - $|A\rangle$: - ($|T\rangle$ + $|A\rangle$) : -$|\beta_T\rangle$

$|\beta_C\rangle$: $|C\rangle$ + $|G\rangle \xRightarrow[\text{Both Bits flip}]{\text{Both Phase}}$ - $|G\rangle$ - $|C\rangle$: - ($|C\rangle$ + $|G\rangle$) : -$|\beta_C\rangle$

For Bell State: $|\beta_T\rangle$

$|\beta_T\rangle$: $|T\rangle$ + $|A\rangle \xRightarrow[\text{1st Phase flip}]{\text{1st Bit}}$ - $|G\rangle$ + $|C\rangle$: $|C\rangle$ - $|G\rangle$: $|\beta_G\rangle$

$|\beta_T\rangle$: $|T\rangle$ + $|A\rangle \xRightarrow[\text{1st Phase flip}]{\text{2nd Bit}}$ - $|C\rangle$ + $|G\rangle$: $|G\rangle$ - $|C\rangle$: *no maximally entangled Bell State*

$|\beta_T\rangle$: $|T\rangle$ + $|A\rangle \xRightarrow[\text{2nd Phase flip}]{\text{1st Bit}} |G\rangle$ - $|C\rangle$: *no maximally entangled Bell State*

$|\beta_T\rangle$: $|T\rangle$ + $|A\rangle \xRightarrow[\text{2nd Phase flip}]{\text{2nd Bit}} |C\rangle$ - $|G\rangle$: $|\beta_G\rangle$

$|\beta_T\rangle$: $|T\rangle$ + $|A\rangle \xRightarrow[\text{1st Phase flip}]{\text{Both Bits}}$ - $|A\rangle$ + $|T\rangle$: $|T\rangle$ - $|A\rangle$: $|\beta_A\rangle$

$|\beta_T\rangle$: $|T\rangle$ + $|A\rangle \xRightarrow[\text{2nd Phase flip}]{\text{Both Bits}} |A\rangle$ - $|T\rangle$: *no maximally entangled Bell State*

$|\beta_T\rangle$: $|T\rangle$ + $|A\rangle \xRightarrow[\text{1st Bit flip}]{\text{Both Phase}}$ - $|G\rangle$ - $|C\rangle$: - ($|C\rangle$ + $|G\rangle$) : -$|\beta_C\rangle$

$|\beta_T\rangle$: $|T\rangle$ + $|A\rangle \xRightarrow[\text{2nd Bit flip}]{\text{Both Phase}}$ - $|C\rangle$ - $|G\rangle$: - ($|C\rangle$ + $|G\rangle$) : -$|\beta_C\rangle$

$|\beta_T\rangle$: $|T\rangle$ + $|A\rangle \xRightarrow[\text{Both Bits flip}]{\text{Both Phase}}$ - $|A\rangle$ - $|T\rangle$: - ($|T\rangle$ + $|A\rangle$) : -$|\beta_T\rangle$

For Bell State: $|\beta_A\rangle$

$|\beta_A\rangle$: $|T\rangle$ - $|A\rangle \xRightarrow[\text{1st Phase flip}]{\text{1st Bit}}$ - $|G\rangle$ - $|C\rangle$: - ($|C\rangle$ + $|G\rangle$) : -$|\beta_C\rangle$

$|\beta_A\rangle$: $|T\rangle$ - $|A\rangle \xRightarrow[\text{1st Phase flip}]{\text{2nd Bit}}$ - $|C\rangle$ + $|G\rangle$: $|G\rangle$ - $|C\rangle$: *no maximally entangled Bell State*

$|\beta_A\rangle$: $|T\rangle$ - $|A\rangle \xRightarrow[\text{2nd Phase flip}]{\text{1st Bit}} |G\rangle$ + $|C\rangle$: $|C\rangle$ + $|G\rangle$: $|\beta_C\rangle$

$|\beta_A\rangle$: $|T\rangle$ - $|A\rangle \xRightarrow[\text{2nd Phase flip}]{\text{2nd Bit}} |C\rangle$ + $|G\rangle$: $|\beta_C\rangle$

$|\beta_A\rangle$: $|T\rangle$ - $|A\rangle \xRightarrow[\text{1st Phase flip}]{\text{Both Bits}}$ - $|A\rangle$ - $|T\rangle$: - ($|T\rangle$ + $|A\rangle$) : -$|\beta_T\rangle$

$|\beta_A\rangle$: $|T\rangle$ - $|A\rangle \xRightarrow[\text{2nd Phase flip}]{\text{Both Bits}} |A\rangle$ + $|T\rangle$: $|T\rangle$ + $|A\rangle$: $|\beta_T\rangle$

$|\beta_A\rangle$: $|T\rangle$ - $|A\rangle \xRightarrow[\text{1st Bit flip}]{\text{Both Phase}}$ - $|G\rangle$ + $|C\rangle$: $|C\rangle$ - $|G\rangle$: $|\beta_G\rangle$

$|\beta_A\rangle$: $|T\rangle$ - $|A\rangle \xRightarrow[\text{2nd Bit flip}]{\text{Both Phase}}$ - $|C\rangle$ + $|G\rangle$: $|G\rangle$ - $|C\rangle$: *no maximally entangled Bell State*

$|\beta_A\rangle$: $|T\rangle$ - $|A\rangle \xRightarrow[\text{Both Bits flip}]{\text{Both Phase}}$ - $|A\rangle$ + $|T\rangle$: $|T\rangle$ - $|A\rangle$) : $|\beta_A\rangle$

For Bell State: $|\beta_G\rangle$

$|\beta_G\rangle$: $|C\rangle$ - $|G\rangle$ $\xRightarrow[\text{1st Phase flip}]{\text{1st Bit}}$ - $|A\rangle$ - $|T\rangle$: - ($|T\rangle$ + $|A\rangle$) : -$|\beta_T\rangle$

$|\beta_G\rangle$: $|C\rangle$ - $|G\rangle$ $\xRightarrow[\text{1st Phase flip}]{\text{2nd Bit}}$ - $|T\rangle$ - $|A\rangle$: - ($|T\rangle$ + $|A\rangle$) : -$|\beta_T\rangle$

$|\beta_G\rangle$: $|C\rangle$ - $|G\rangle$ $\xRightarrow[\text{2nd Phase flip}]{\text{1st Bit}}$ $|A\rangle$ + $|T\rangle$: $|T\rangle$ + $|A\rangle$: $|\beta_T\rangle$

$|\beta_G\rangle$: $|C\rangle$ - $|G\rangle$ $\xRightarrow[\text{2nd Phase flip}]{\text{2nd Bit}}$ $|T\rangle$ + $|A\rangle$: $|\beta_T\rangle$

$|\beta_G\rangle$: $|C\rangle$ - $|G\rangle$ $\xRightarrow[\text{1st Phase flip}]{\text{Both Bits}}$ - $|G\rangle$ - $|C\rangle$: -($|C\rangle$ + $|G\rangle$) : -$|\beta_C\rangle$

$|\beta_G\rangle$: $|C\rangle$ - $|G\rangle$ $\xRightarrow[\text{2nd Phase flip}]{\text{Both Bits}}$ $|G\rangle$ + $|C\rangle$: $|C\rangle$ + $|G\rangle$: $|\beta_C\rangle$

$|\beta_G\rangle$: $|C\rangle$ - $|G\rangle$ $\xRightarrow[\text{1st Bit flip}]{\text{Both Phase}}$ - $|A\rangle$ + $|T\rangle$: $|T\rangle$ - $|A\rangle$: $|\beta_A\rangle$

$|\beta_G\rangle$: $|C\rangle$ - $|G\rangle$ $\xRightarrow[\text{2nd Bit flip}]{\text{Both Phase}}$ - $|T\rangle$ + $|A\rangle$: $|A\rangle$ - $|T\rangle$: *no maximally entangled Bell State*

$|\beta_G\rangle$: $|C\rangle$ - $|G\rangle$ $\xRightarrow[\text{Both Bits flip}]{\text{Both Phase}}$ - $|G\rangle$ + $|C\rangle$: $|C\rangle$ - $|G\rangle$: $|\beta_G\rangle$