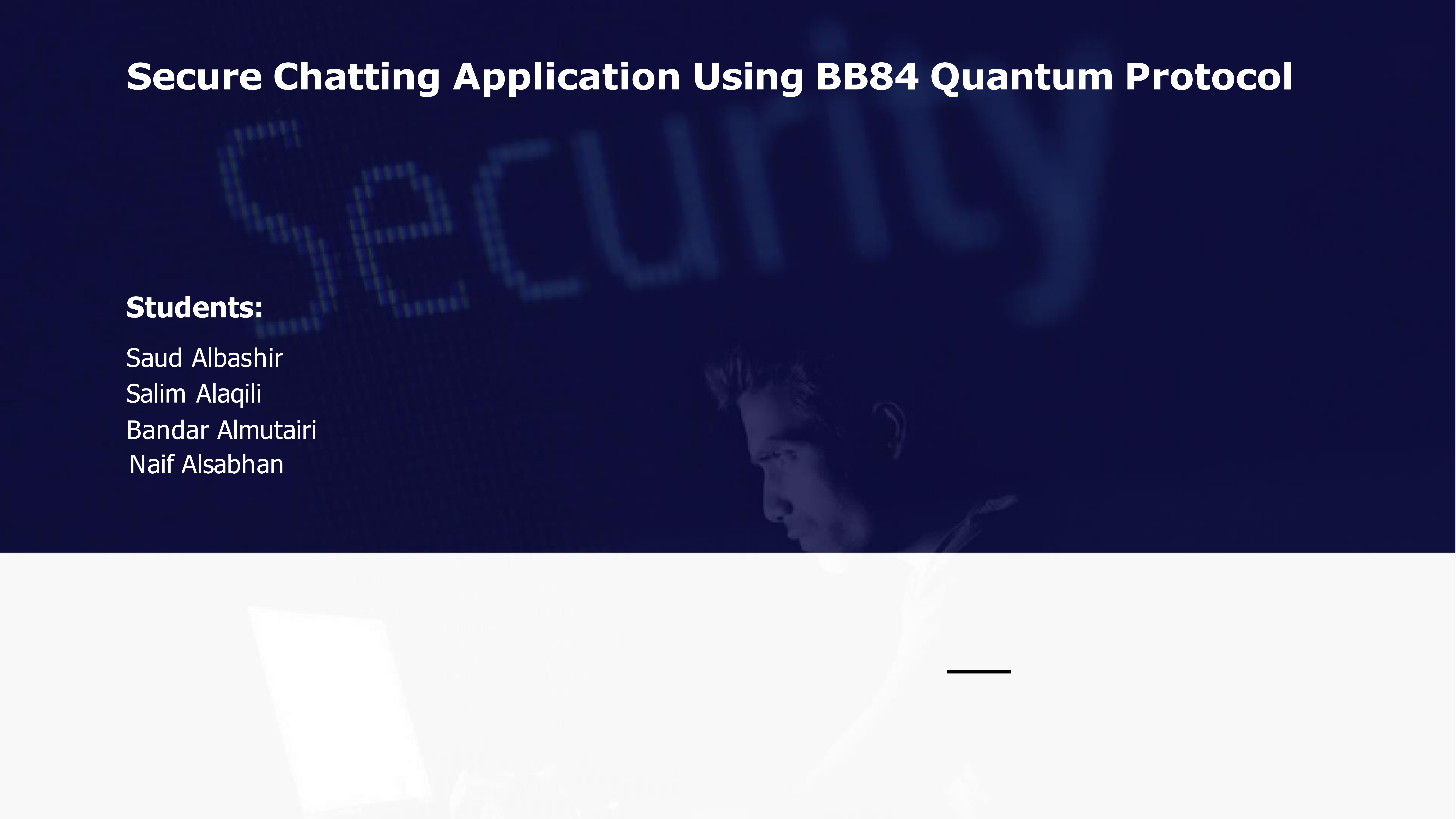
Secure Chatting Application Using BB84 Quantum Protocol

Students:

Saud Albashir
Salim Alaqili
Bandar Almutairi
Naif Alsabhan



alice

eve

bob

Introduction:

- **Traditional forms of communication are not secure and can be easily intercepted by third parties.**

- Quantum cryptography offers unbreakable security.
- The BB84 protocol is a quantum cryptographic protocol that can be used to create a secure key between two parties.

Project Description

- The project is a secure chatting application that uses the BB84 quantum protocol to create a secure key between two users.

- The application works by first creating a secure key using the BB84 protocol.

- Once the key has been created, the application can be used to send encrypted messages between the two users.

- The messages are encrypted using the secure key, so they cannot be read by an eavesdropper.

Tools used

- Python using Spyder IDE.

- IBM Qiskit library.

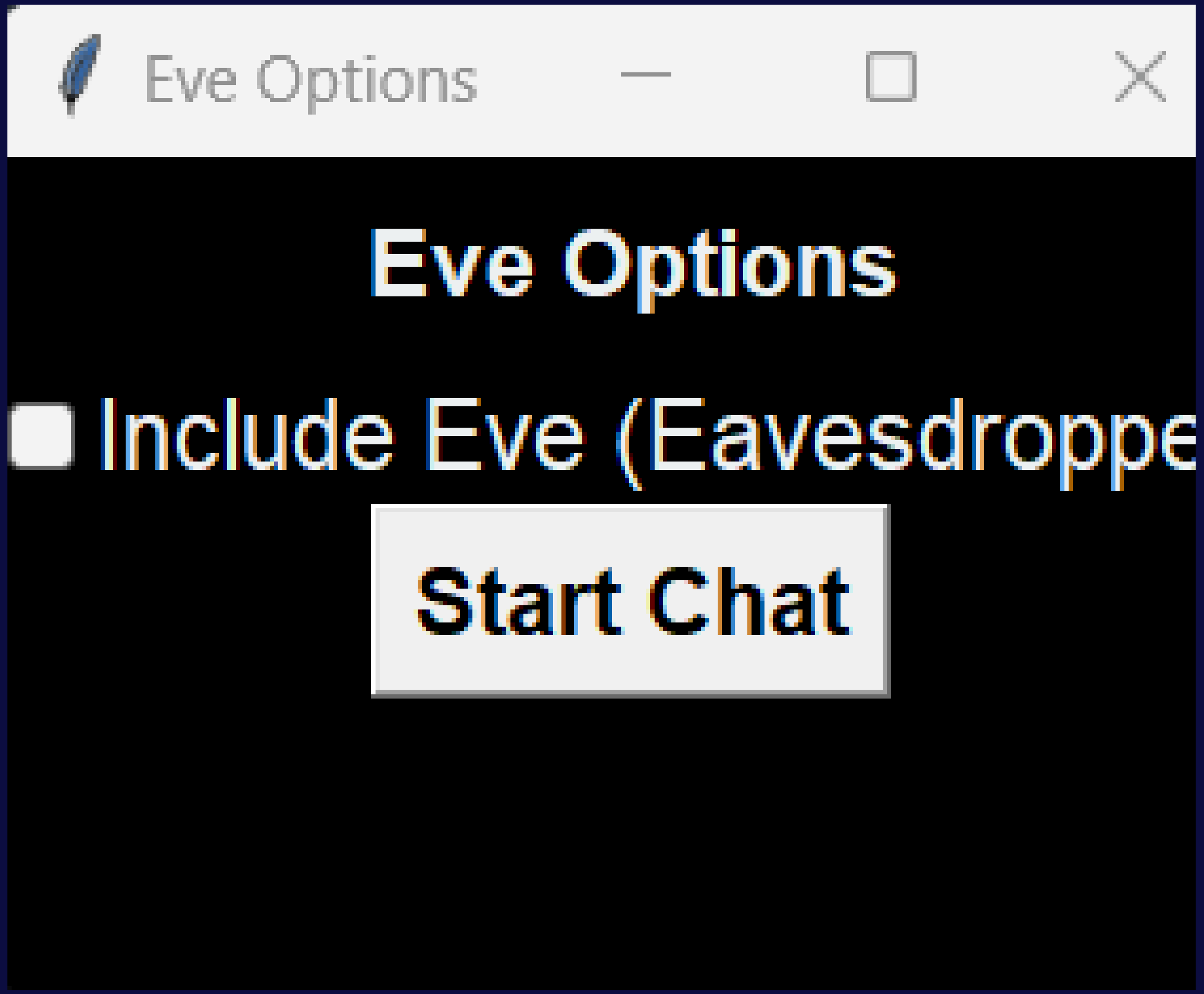
- Numpy library.

- Tkinter library for implementing the GUI.

- Canvas website for designing the presentation.

Sample run

- the user gets to choose whether they want Eve or not.
  - In this example the user choose to no include Eve.

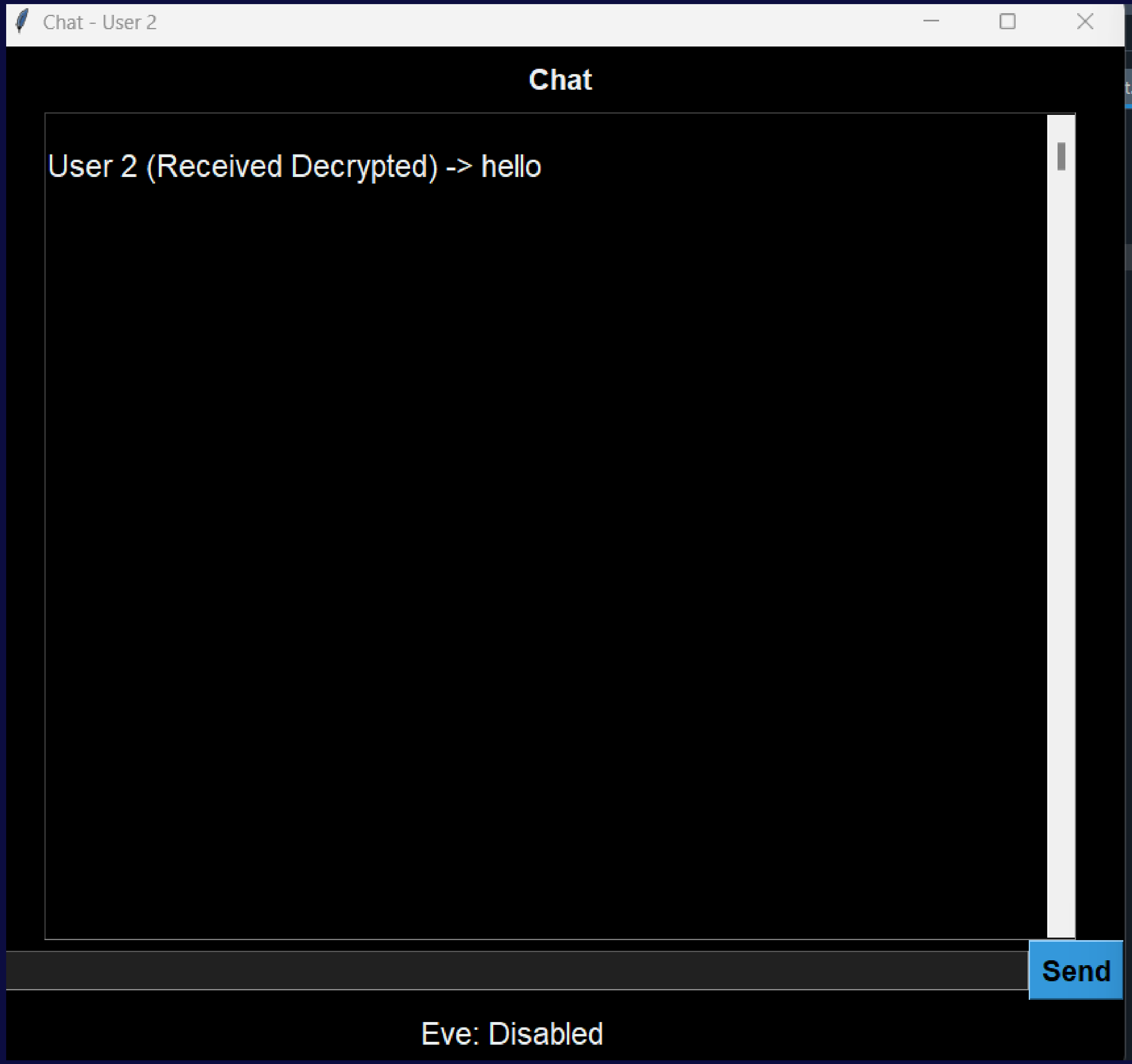


Eve Options

□ Include Eve (Eavesdroppe

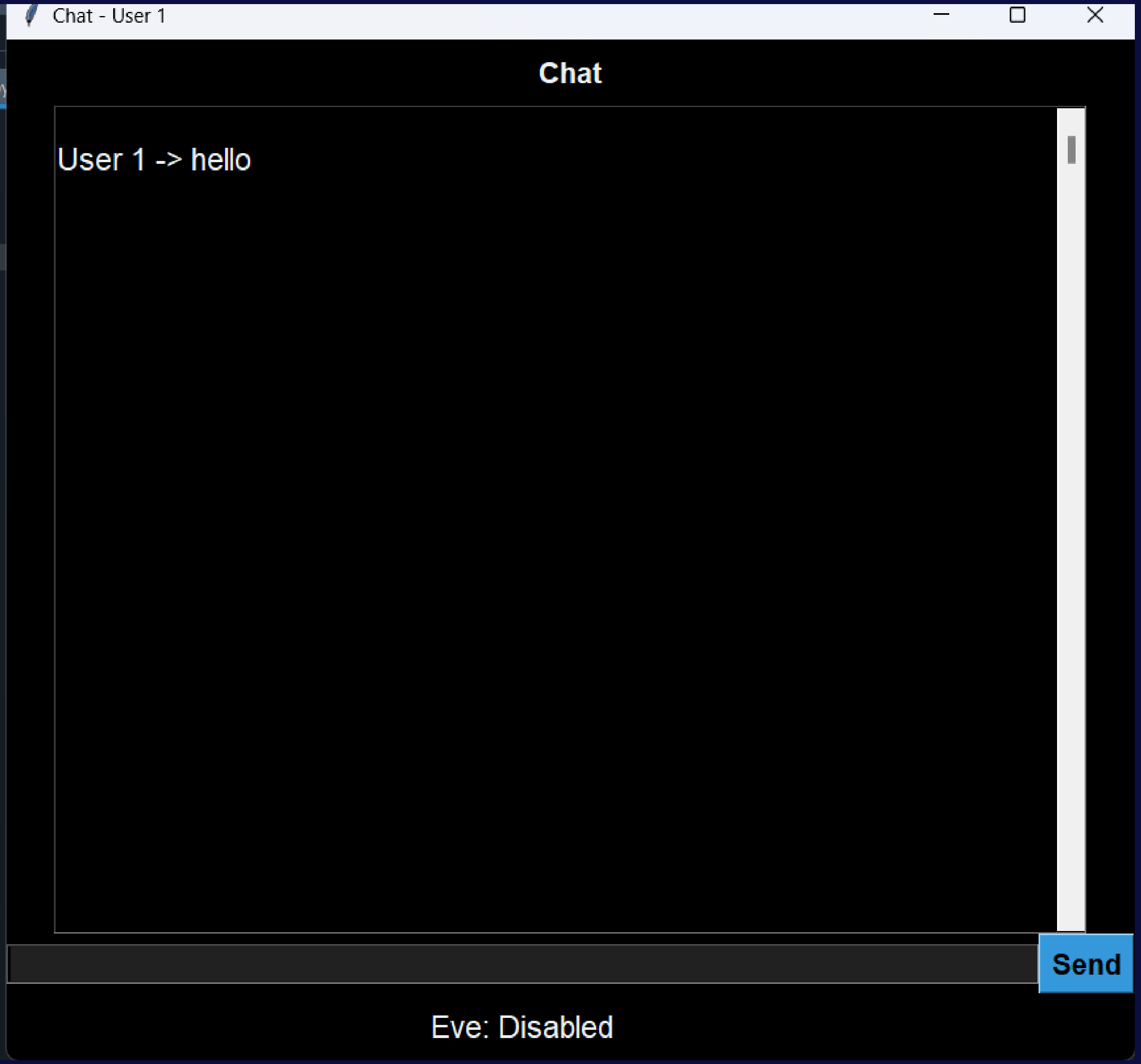
Sample run

- After the user's choice two windows will appear on the screen, one for user 1 (Alice), and one more for user 2 (Bob).
  - In the example below, user 1 wants to send a hello to user 2, and we can see that user (1) sent the message and user 2 received the message in a secured way.



User 2 (Received Decrypted) -> hello

Eve: Disabled

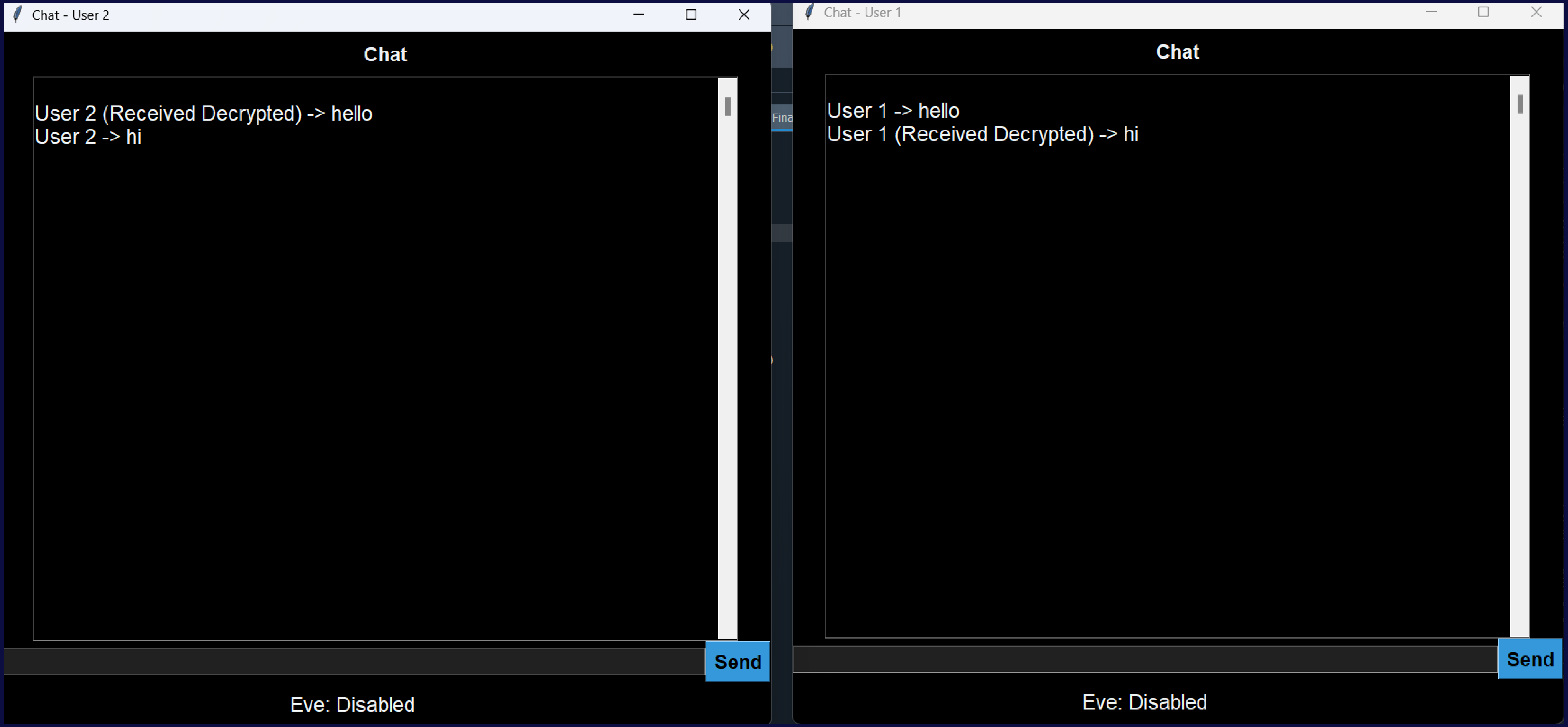


User 1 -> hello

Eve: Disabled

Sample run

- After user (1) sent a hello and user (2) received it, now user (2) wants to say hi back to user (1).



```
User 2 (Received Decrypted) -> hello
User 2 -> hi
```

Eve: Disabled

```
User 1 -> hello
User 1 (Received Decrypted) -> hi
```

Eve: Disabled

Benefits

- Unbreakable security: The BB84 protocol is unbreakable, so users can be confident that their messages are private.

- Easy to use: The application is easy to use, so anyone can use it.

- Secure: The application is secure, so users can be confident that their messages are not being intercepted.

difficulty

- The implementation of the N-queens problem has proven challenging due to its intricate structure. Regrettably, we have encountered difficulties in establishing a direct correlation between the arrangement of queens on the board and the tangible measurement of results in terms of counts. This has hindered our ability to accurately quantify the solutions we generated.

- Concerning the BBM92 protocol, our progress has been hindered by the lack of sufficient materials available for reference. This shortage of comprehensive resources has made it challenging to fully grasp the protocol's details and implications, impacting our ability to understand its intricacies.

- Furthermore, when implementing the E91 protocol using three or more qubits, the resulting circuit size significantly expands. This enlargement places a strain on our computer's processing capabilities, to the extent that it may lead to crashes or performance issues.

Conclusion

- A secure chatting application using the BB84 quantum protocol is a valuable tool for anyone who needs to communicate securely.

- The application is unbreakable, easy to use, and secure.

- We believe that this application has the potential to revolutionize the way we communicate.

Thanks for you time

If you have any further questions feel free to ask