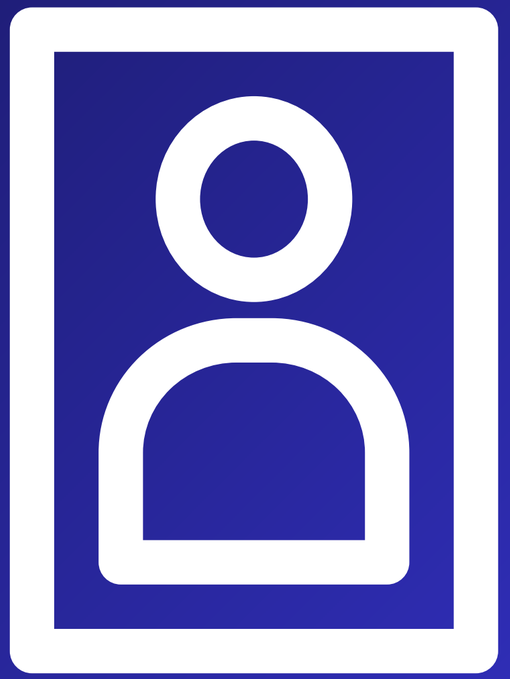
TO BE DETERMINED

BB84 AND PROBLEM

CLASSICAL ENCRYPTION METHODS (RSA,ECC)ARE NOT USEFUL FOR QUANTUM COMPUTERS

BB84 QKD PROTOCOL CAN BE USED

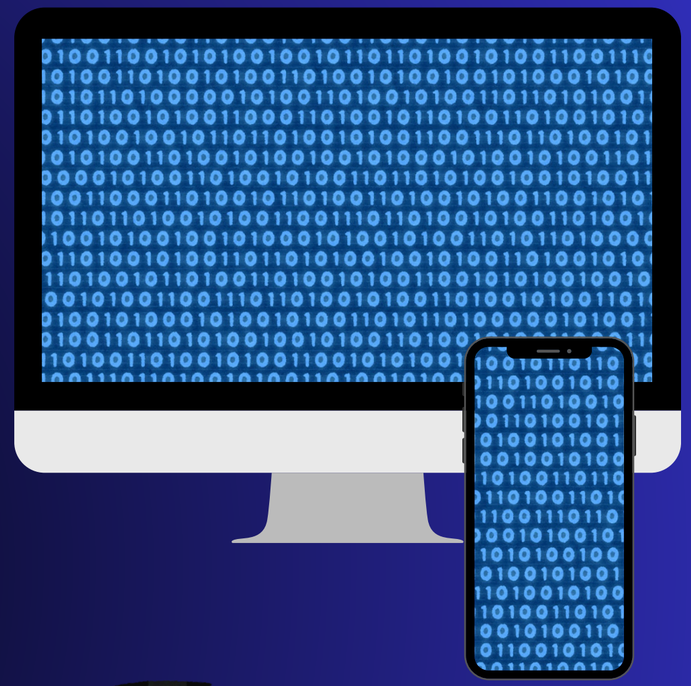


BB84

ALICE

BOB

ALICE AND BOB WANT TO USE QUBITS TO SHARE SECRET KEY BETWEEN EACH OTHER(BB84)



IF EVE TRIES TO EAVESDROP !!!!! ERRORS !!!!!

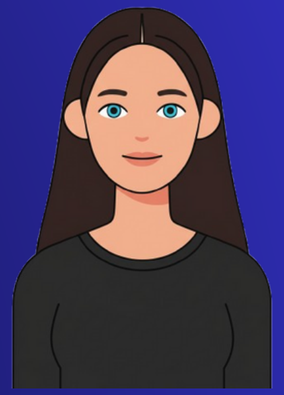
EVE

OUR SOLUTION

NAZ

We create secret keys using BB84

Keys are stored in a hash table for quick and safe lookup



ALEYNA

Messages are sent as emojis so only the right user can read them

Even if someone gets the emojis, they can’t decode them without the key

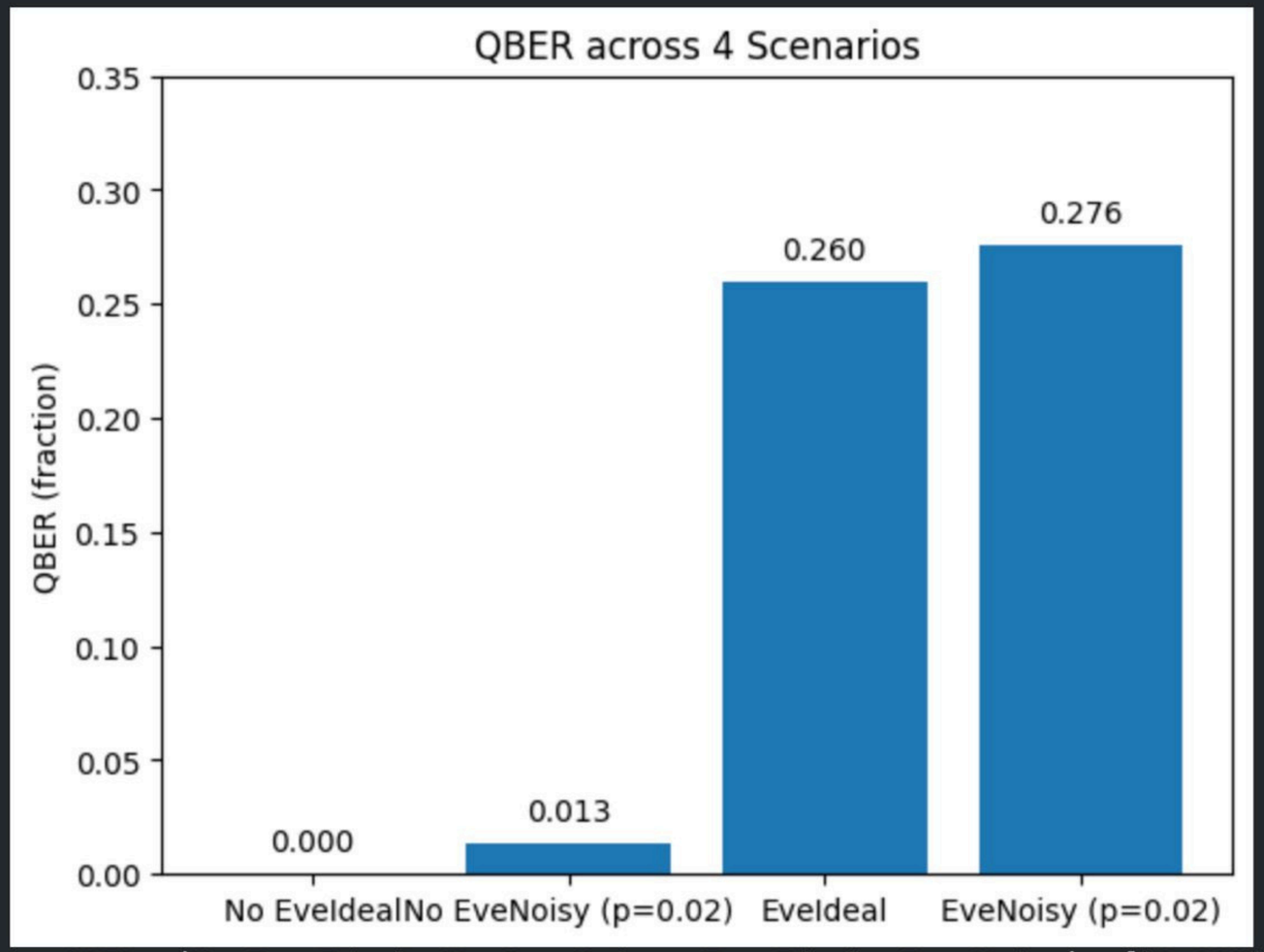
It can spot any eavesdropper instantly through error detection

YASSINE

KAMEEL

GEBRIL

IMPLEMENTATION & RESULTS




```
>> QBERs (No Eve Ideal, No Eve Noisy, Eve Ideal, Eve Noisy): ['0.000', '0.013', '0.260', '0.276']
>> We will now continue the pipeline using **No Eve, Ideal** results for clean outputs.
```

STEPS

1

```
Kept: 1507 | Sample: 100 | QBER_est on sample: 0.000 | Remaining: 1407
```

2

```
Block sizes: 200 & 200   |  leakage = 2 bit(s)
Parities A/B: Block1 0/0 | Block2 1/1
Keys equal after reconcile?  YES
```

3

```
Estimated secure length ≈ 388 bits
Final Session Key (256-bit, hex): 88808d51519f1a9e85935a6696122b9b44918c49ec19aa65e28e3b5178d09637
```

CONCLUSION

```python
msg = b"Meet me at 10:30 near the fountain."
epoch = current_epoch()
sk = derive_session_key(K256, epoch)
nonce, ct = enc_aesgcm(sk, msg, aad=b"meta:demo")
pt = dec_aesgcm(sk, nonce, ct, aad=b"meta:demo")
print(f"Decryption OK (same epoch {epoch})?  {pt == msg}")
try:
    sk_wrong = derive_session_key(K256, epoch+1)
    _ = dec_aesgcm(sk_wrong, nonce, ct, aad=b"meta:demo")
    print("[Unexpected] wrong-epoch decryption succeeded")
except Exception as e:
    print("Wrong epoch decryption fails (expected):", type(e).__name__)
```

```
Decryption OK (same epoch 1957699)?  True
```

```
Left  stream (preview): 🎈🍀🪄🎈🎉🎈🪄🪄🎈🍀🎈🍀🎉🎈🪄🎉🎈🍀🎉🍀🪄🎈🎈🎈🎈🎉🎈🍀🪄🎈🍀🪄🍀🎉🎈🎈🎉🍀🎉🎈🎉🎉🪄🎉🎉🪄🍀🎈🪄🪄 ...
Right stream (preview): 🪄🎈🍀🎉🎉🪄🎈🍀🎈🎉🎉🪄🎈🪄🍀🎈🎈🪄🎈🎈🪄🎈🍀🎈🍀🎉🍀🪄🪄🪄🍀🪄🪄🎈🎈🍀🍀🎉🪄🪄🎉🍀🎉🎈🎉🍀🍀🪄🪄🪄 ...
Recovered == original?  True
```

THANK YOU

TO BE DETERMINED