Constant Uncertainty – QKD Challenge

Francesco Vista

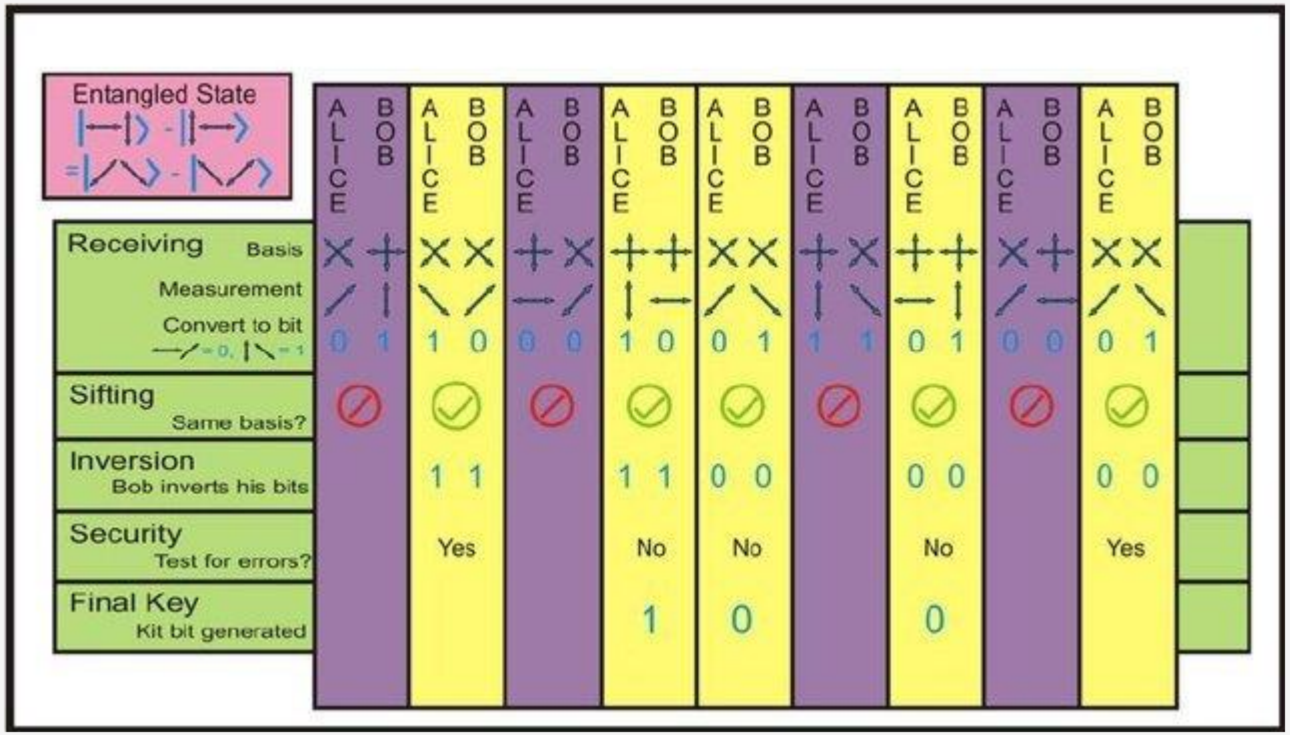
Guy Meyer

Nemanja Miljkovic

Quantum Internet
Hackathon 2022

Implementation of BBM92 protocol in QAN-AKD

BBM92 QKD Protocol overview



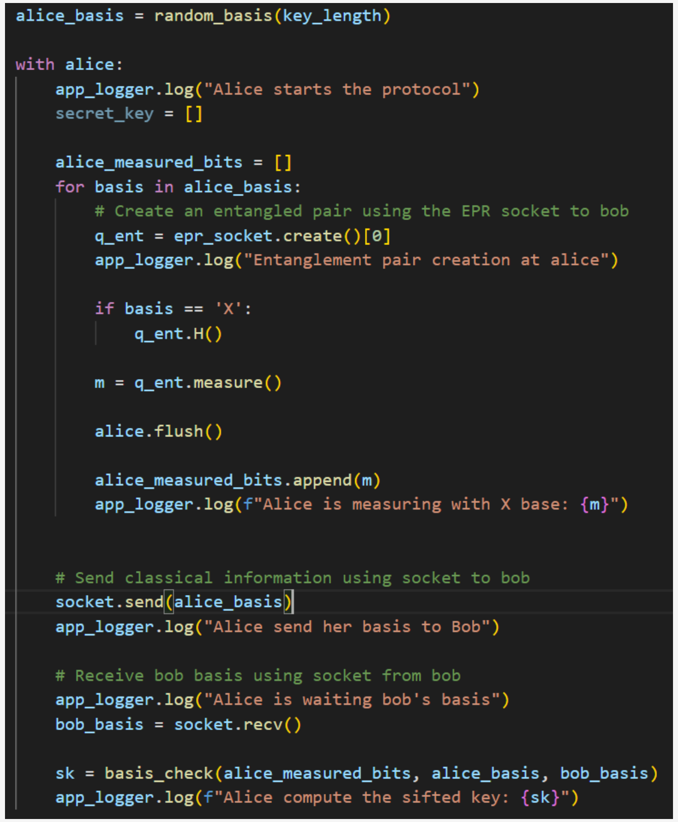
Entangled State
$|{\leftrightarrow}{\updownarrow}\rangle - |{\updownarrow}{\leftrightarrow}\rangle = |{\nearrow}{\searrow}\rangle - |{\searrow}{\nearrow}\rangle$

	ALICE	BOB	ALICE	BOB	ALICE	BOB	ALICE	BOB	ALICE	BOB	ALICE	BOB	ALICE	BOB	ALICE	BOB	ALICE	BOB
Receiving Basis	×	+	×	×	+	×	+	+	×	×	+	×	+	+	×	+	×	×
Measurement	↗	↕	↘	↗	↔	↗	↕	↔	↗	↘	↕	↘	↔	↕	↗	↔	↗	↘
Convert to bit ↔ ↗ = 0, ↕ ↘ = 1	0	1	1	0	0	0	1	0	0	1	1	1	0	1	0	0	0	1
Sifting Same basis?	⊘		✓		⊘		✓		✓		⊘		✓		⊘		✓	
Inversion Bob inverts his bits			1	1			1	1	0	0			0	0			0	0
Security Test for errors?			Yes				No		No				No				Yes	
Final Key Kit bit generated							1		0				0					

Implementation of BBM92 protocol in QAN-AKD

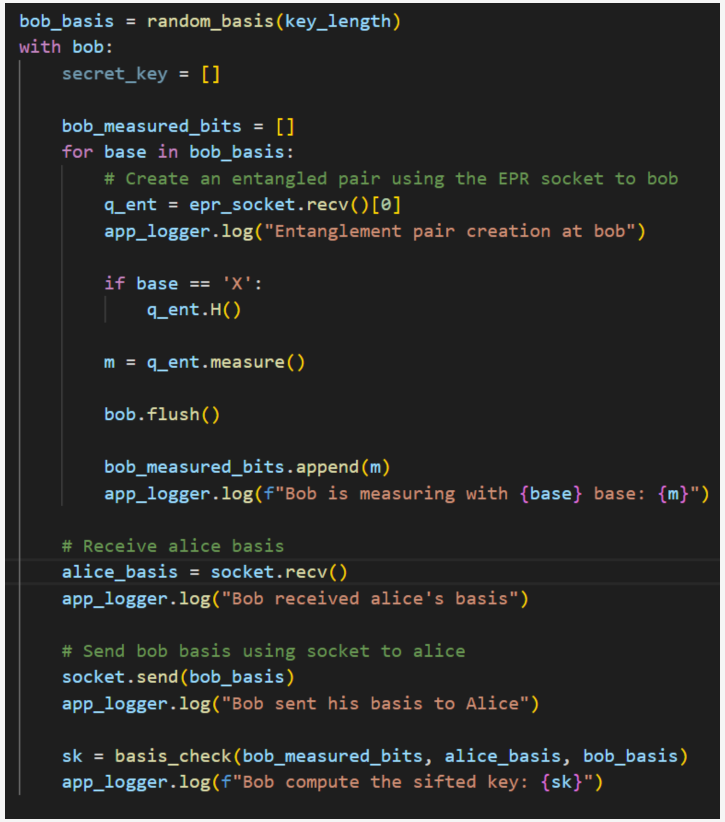
Implementation of protocol in QAN-AKD, main focus on Alice and Bob

Alice



```
alice_basis = random_basis(key_length)

with alice:
    app_logger.log("Alice starts the protocol")
    secret_key = []

    alice_measured_bits = []
    for basis in alice_basis:
        # Create an entangled pair using the EPR socket to bob
        q_ent = epr_socket.create()[0]
        app_logger.log("Entanglement pair creation at alice")

        if basis == 'X':
            q_ent.H()

        m = q_ent.measure()

        alice.flush()

        alice_measured_bits.append(m)
        app_logger.log(f"Alice is measuring with X base: {m}")


    # Send classical information using socket to bob
    socket.send(alice_basis)
    app_logger.log("Alice send her basis to Bob")

    # Receive bob basis using socket from bob
    app_logger.log("Alice is waiting bob's basis")
    bob_basis = socket.recv()

    sk = basis_check(alice_measured_bits, alice_basis, bob_basis)
    app_logger.log(f"Alice compute the sifted key: {sk}")
```

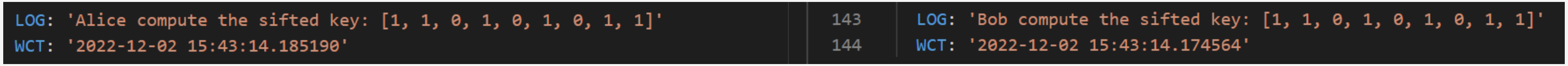
Bob



```
bob_basis = random_basis(key_length)
with bob:
    secret_key = []

    bob_measured_bits = []
    for base in bob_basis:
        # Create an entangled pair using the EPR socket to bob
        q_ent = epr_socket.recv()[0]
        app_logger.log("Entanglement pair creation at bob")

        if base == 'X':
            q_ent.H()

        m = q_ent.measure()

        bob.flush()

        bob_measured_bits.append(m)
        app_logger.log(f"Bob is measuring with {base} base: {m}")

    # Receive alice basis
    alice_basis = socket.recv()
    app_logger.log("Bob received alice's basis")

    # Send bob basis using socket to alice
    socket.send(bob_basis)
    app_logger.log("Bob sent his basis to Alice")

    sk = basis_check(bob_measured_bits, alice_basis, bob_basis)
    app_logger.log(f"Bob compute the sifted key: {sk}")
```

Implementation of BBM92 protocol in QAN-AKD

Results



```
LOG: 'Alice compute the sifted key: [1, 1, 0, 1, 0, 1, 0, 1, 1]'
WCT: '2022-12-02 15:43:14.185190'
```

```
LOG: 'Bob compute the sifted key: [1, 1, 0, 1, 0, 1, 0, 1, 1]'
WCT: '2022-12-02 15:43:14.174564'
```

Implementation of BBM92 protocol in QAN-AKD

Challenges

- Installation and understanding the APK
- Understanding the protocol
- Debugging

Implementation of BBM92 protocol in QAN-AKD

Next steps

- Try to implement option with Eve
- Try to implement other protocols