Literature Review

# Literature Survey

| **Citation** | **Summary** | **Technology used** | **Limitations** | **Contribution** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

TODO:

1. Break the implementation into multiple sections.
   1. Authentication
   2. Key-exchange
   3. Block encryption
   4. Certificates
2. Add tables to each of those sections with the citation, summary, technology used, limitations, and contributions.

# Authentication

## Existing authentication algorithms

Existing authentication algorithms use a public-key encryption algorithm, such as ECDH or RSA. Typically a CA will generate a certificate which is used to authenticate if the public-key holder is a trusted source. This is done by validating if the certificate issuer is trusted.

(Talk about the TLS/ SSL certificates and its structure).

## Quantum-secure authentication algorithms

Quantum-secure authentication algorithms work much like existing authentication algorithms. A CA’s self-signed certificate is generated using quantum-secure public key cryptographic algorithms and they’re used to produce certificates that are distributed to individual devices.

## Certificateless authentication

Unlike certificate-based authentication, this system does not use certificates to authenticate end nodes in the network.

(Talk about the new research and the uses of these systems. Also, talk about the stolen/ compromised CA issue).

# Key-exchange

## Existing key-exchange algorithms

(Talk about ECDH-RSA-KEM)

## Quantum-secure key-exchange algorithms

(Talk about how this could be achieved using Kyber).

# Block encryption

(Talk about AES-256 and mention that it’s quantum-secure)