Benchmarking Post-quantum Public Key Encryption in TLS1.3
# A Case Study on Kyber

Jingzhe Wang

Data Description

- Kyber is a post-quantum public key encryption construction that shows resistance to quantum attacks.

- **Data Source: https://github.com/xvzcf/pq-tls-benchmark/tree/master/emulation-exp/data/kex**

- **Description:**

  - Handshake completion time results under different packet loss rate and round-trip time settings.

  - Raw performance benchmarking results

Visualization 1 - Line Plot

- **Group 1 : Handshake Completion Time v.s. Packet Loss Rate**

Figure 1: TLS Handshake Completion Time v.s. Packet Loss Rate
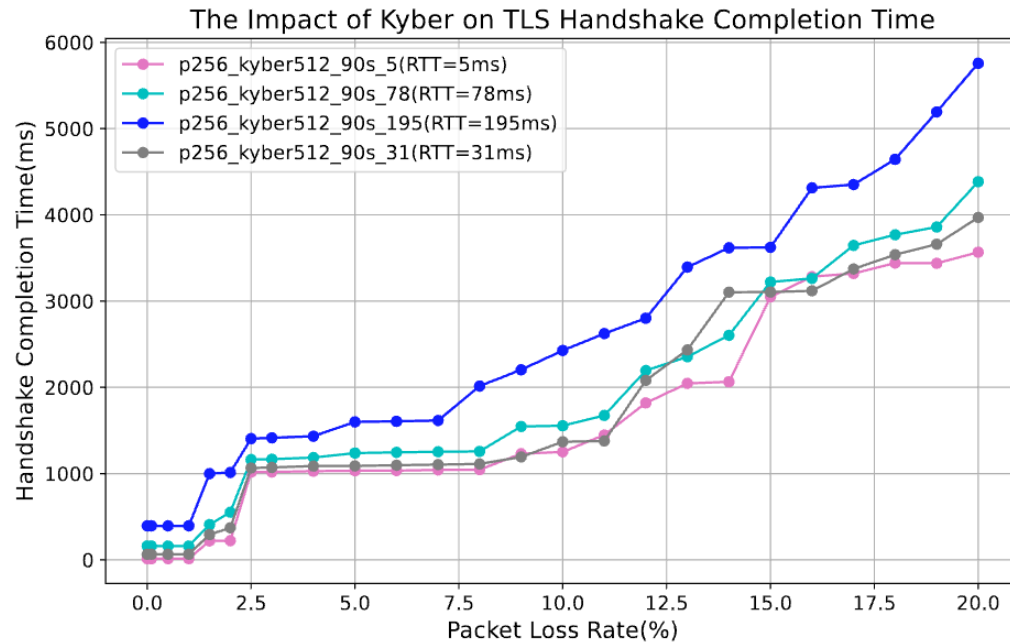
- **Objective:** Visualize the variations of the handshake completion time of Kyber under different packet loss settings

- **Findings:** with the increasing packet loss rate, the handshake completion time becomes longer. This observation works for all four settings.

Visualization 1 - Line Plot

- **Group 2: Percentile Visualization**

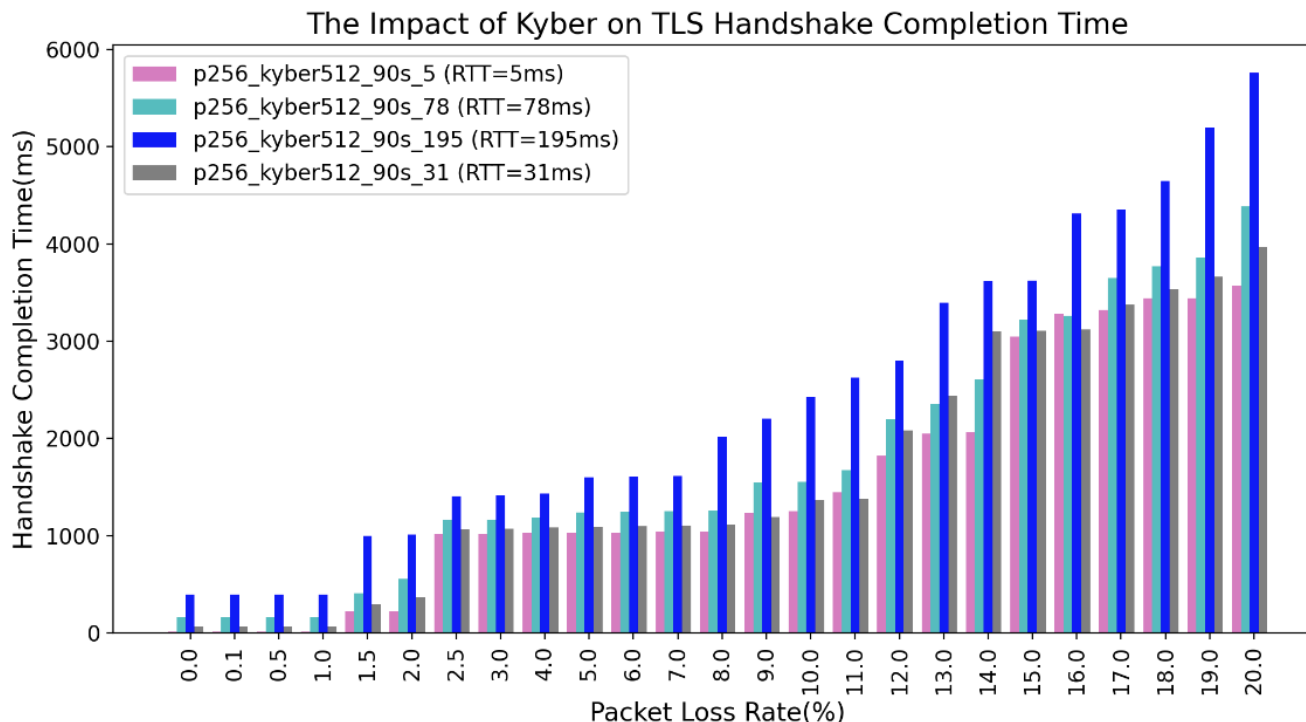The Impact of Kyber on TLS Handshake Completion Time(RTT=5ms)
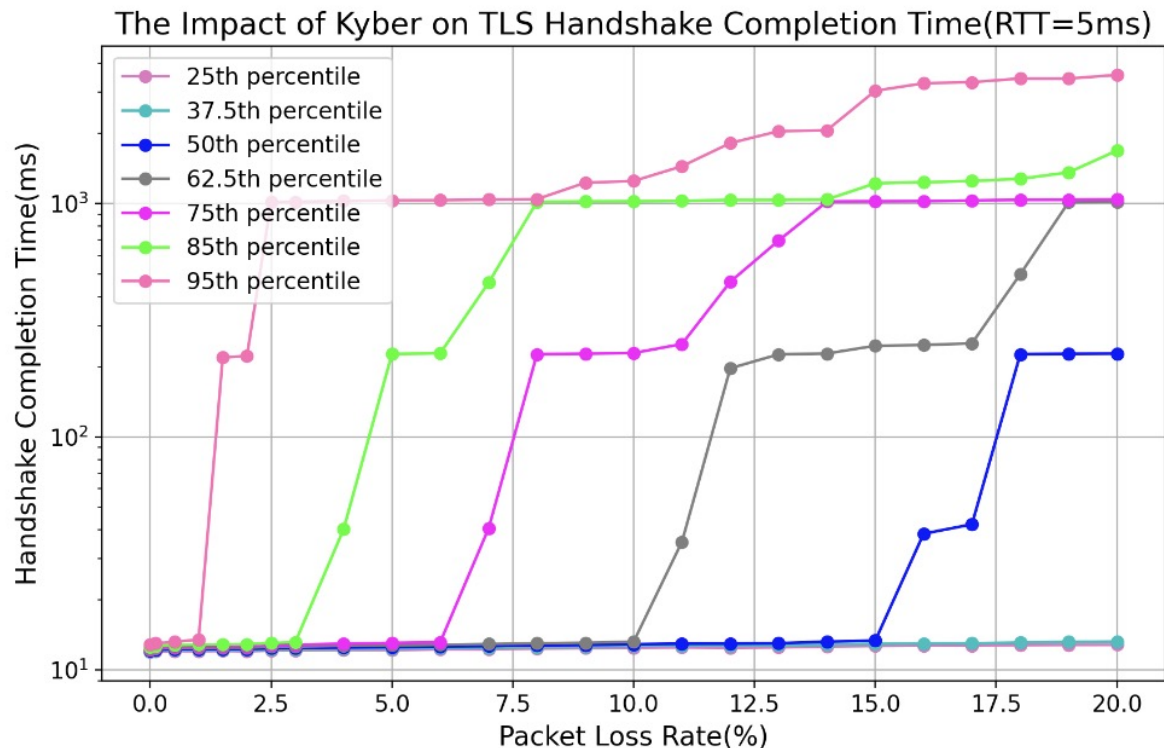
- **Objective**: Visualize data distribution when fixing RTT.

- **Findings:** Observing horizontally, we can see that higher packet loss rate incurs significant variations in terms of handshake completion time

- **Aesthetic Considerations:**
  - Adopt log-scale y-axis to fit all data clearly.
  - Adopt proper colors.

Visualization 2 – Bar Plot

- **Group 1 : Handshake Completion Time v.s. Packet Loss Rate (Alternative Views)**

The Impact of Kyber on TLS Handshake Completion Time

- **Objective:** clearly shows the impact of RTT under each packet loss rate setting.

- **Findings:** in almost each packet loss setting, a higher RTT results in longer handshake completion time.

- **Aesthetic Considerations:**
  - Rotate x-axis ticks horizontally to make it look better.

Visualization 2 – Bar Plot

• **Group 2: Raw Performance Results**

Figure 3: Kyber Raw Performance Result (Bar Chart)
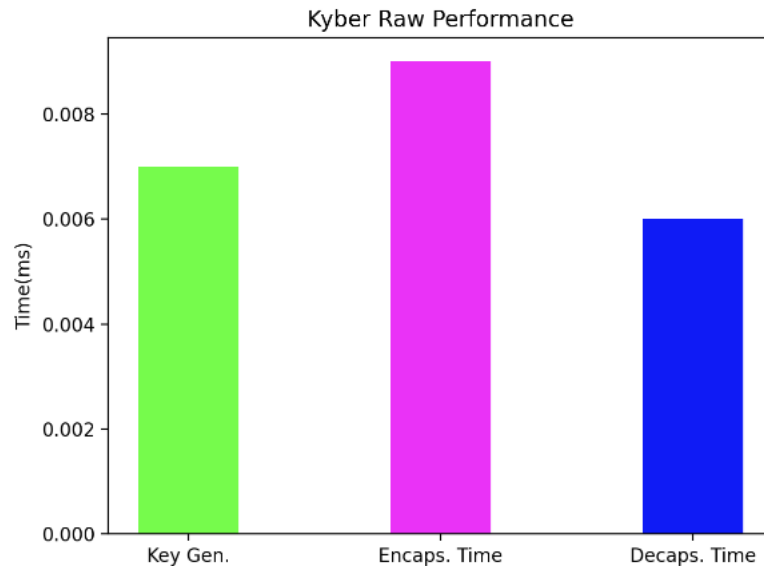
• **Objective:** Visualize raw performance of Kyber.

• **Findings:** It is easy to see that the encapsulation time of Kyber dominates the raw performance metrics.

• **Aesthetic Considerations:**
  • High-contrast Color
  • Label x-tick as categories.

Thanks!