Weiterentwicklung eines Post-Quantum-Krypto-Prototyps

Projektpräsentation

Gruppe 3
Berk Meric, Valentin Bäuerle, Dennis Bantel, Florian Vasica

November 2024

Inhalt

Einleitung

- Traditionelle Verschlüsselungsmethoden wie RSA und ECC werden anfällig
- Projekt baut auf der Masterarbeit von Niyati Venugopal auf
- Ziel: Zukunftssichere Verschlüsselung durch Post-Quantum-Kryptografie

Hintergrund

- Die Masterarbeit testete post-quanten-kryptografische Algorithmen (z. B. Kyber, SPHINCS+) auf einer Client-Server-Architektur (Raspberry Pi)
- Limitierungen:
  - begrenzt Experimente durchgeführt
  - Code nur auf einem Gerät getestet
- Wichtige Erkenntnisse:
  - Kyber: Effizient, aber etwas mehr Overhead als RSA
  - SPHINCS+: Langsamer beim Signieren, aber starke Quantenresistenz

Projektidee

- Aufgabe: Verbesserung des bestehenden Prototyps für bessere Leistung und breitere Tests
  1. **Code-Optimierung:** Verbesserte Ergebnisgenerierung (z. B. mit Standardabweichung)
  2. **Client-Server-Kommunikation:** Tests auf verschiedenen Geräten
  3. **Automatisierung:** Daten sammeln und Analysen automatisieren
  4. **Ergebnisdarstellung:** Ergebnisse mit Diagrammen visualisieren

Ziele

- Verbesserung der Zuverlässigkeit und Skalierbarkeit des Codes
- Anpassung des Prototyps an IoT-Umgebungen
- Ausweitung der Tests auf verschiedene Geräte
- Bereitstellung bedeutungsvoller Leistungsanalysen durch Visualisierungen

Geplanter Ablauf

1. **Analyse der bestehenden Lösung:**
   - Review des bestehenden Codes und der Dokumentation
   - Identifikation von Schwächen und Optimierungspotentialen
2. **Code-Optimierung und Testing:**
   - Verbesserung der Ergebnisgenerierung
   - Ausführliche Tests auf verschiedenen Geräten
3. **Automatisierung der Experimente:**
   - Entwicklung eines automatisierten Workflows zur Messung und Analyse
4. **Visualisierung der Ergebnisse:**
   - Erstellung von Diagrammen zur Darstellung der Performance
5. **Abschluss und Dokumentation:**
   - Zusammenfassung der Erkenntnisse und Erstellung einer Abschlussdokumentation

Fazit

- Projekt adressiert Schwächen der Masterarbeit
- Ziel: Ein Prototyp für die Evaluation post-quanten-kryptografischer Verfahren
- Bedeutung:
  - Angesichts des Aufstiegs des Quantencomputings essenziell für zukunftssichere IoT-Sicherheit
  - Verbindung von theoretischer Kryptografie und praktischer Anwendung

Noch Fragen?