Hochschule RheinMain
Andreas Hellenbrand und Fabio Campos

Projekt
XMSS in Rust

XMSS (eXtended Merkle Signature Scheme) ist ein quantensicheres, hashbasiertes Signaturschema, das entwickelt wurde, um widerstandsfähig gegen Angriffe von Quantencomputern zu sein.

Projektaufgaben

- Implementierung einer vereinfachten Version von XMSS in Rust

Projektabgaben

- Erstellen Sie eine 10 minütige Präsentation pro Teilnehmer.
- Quellcode und Dokumentation (in einem offenen Format wie LaTeX, Markdown, .o.ä.) zu Ihrem Projekt. Die Dokumentation sollte alle Aspekte des Quellcodes Ihres Projekts so detailliert abdecken, dass Sie Ihre Ergebnisse verstehen und nachvollziehen können.
- Die Projektabgabe muss bis spätestens zum 26.08. 23:59 CET per Mail erfolgen.
- Die Präsentation der Projekte findet 28.08. um 08:00 Uhr im Raum C405 statt.