Programmierpraktikum Kryptographie

- Teilnehmerzahl: 3
- Inhaltsbeschreibung:

  Seitenkanalangriffe nutzen Informationen, die während der Ausführung kryptografischer Algorithmen entstehen, statt Schwächen im mathematischen Design. Zu Seitenkanalinformationen gehören Messungen wie Zeitdauer, Energieverbrauch, elektromagnetische Strahlung oder Speicherzugriffe. Selbst wenn der Algorithmus theoretisch und mathematisch sicher ist, können solche indirekten Informationen Rückschlüsse auf geheime Schlüssel ermöglichen. Neben den eher passiven Seitenkanalangriffen gibt es noch die Fehlerangriffe, die aktiv Fehler im Code erzeugen und diese ausnutzen. Beispielsweise können Werte auf Null gesetzt werden oder sogar ganze Instruktionen übersprungen werden. Das Gebiet der physikalischen Sicherheit von kryptographischen Verfahren umfasst die Sicherheit der Verfahren gegenüber Seitenkanal- und Fehlerangriffen.

  Der Lehrstuhl für Datensicherheit und Kryptographie verfügt bereits über ein digitales, umfassendes Literaturverzeichnis bzgl. der physikalischen Sicherheit von Post-Quantum-Kryptographie (PQC) und will diese Informationen als Datenbank auf einer externen Webseite der Allgemeinheit zur Verfügung stellen.

  Zusätzlich soll der Einstieg für Interessierte in Seitenkanalangriffe erleichtert werden, indem ein Containerimage mit einer Arbeitsumgebung für physikalische Angriffe erstellt und dokumentiert wird. Diese soll auf der Online-Webseite bereitgestellt werden.

- **Aufgabe:**
  Der erste Teil des Praktikums besteht darin, eine Online-Webseite für die Literatur-Übersicht zu Seitenkanal- und Fehlerangriffen auf PQC zu erstellen. Derzeit liegen die Daten in einer BiBTeX-Dabei (.bib) vor, d.h. sie müssen zunächst in eine Datenbank überführt werden. Folgende Funktionen sollen in der Webseite u.a. erhalten sein:
  - Übersicht als Tabelle
  - Suchfunktionen für einzelnen Spalten
  - Sortierbar (z.B. Jahr, Verfahren, Angriff/Gegenmaßnahme, Autoren, …)
  - Formularfeld, über das fehlende Arbeiten per E-Mail gesendet werden können
  - Verschiedene Visualisierungsmöglichkeiten
  - Export der Darstellung/Liste
  - Unterschiedliche Zitierstile (APA, MLA, BiBTeX)

Der zweite Teil des Praktikums beinhaltet die Erstellung eines Container-/VM-Images für Linux mit einer Arbeitsumgebung, die SageMath für die mathematischen Berechnungen, das ChipWhisperer Repository für die Aufnahme von Stromverbrauchsmessungen und Jupyter Notebook zur Koordinierung beider Programme enthält. Besonderen Wert soll hier auf die Dokumentation gelegt werden, die neuen Nutzern Schritt für Schritt die Einrichtung erklärt.

- **Anforderungen:**
  - Erfahrung mit Webentwicklung und Webdesign
  - Interesse an Kryptographie
  - Englischkenntnisse

- Termin Kickoff-Meeting: 17.04.2026
- Projektzeitraum: 13.04.2026 bis 17.07.2026 (flexibel)
- Abgabedeadline: 17.07.2026 (flexibel)