Programmierpraktikum Kryptographie

- Teilnehmerzahl: 1
- Inhaltsbeschreibung:

  Traditionell sind Authenticated Encryption (AE) Verfahren erforderlich um Vertraulichkeit und Authentizität zu gewährleisten. In letzter Zeit hat sich herausgestellt, dass sogenannte Committing Sicherheit, ein weiteres relevantes Sicherheitsziel ist. Diese macht es Angreifern unmöglich, Chiffretexte zu finden, die unter mehreren Schlüsseln entschlüsselt werden können. Das Fehlen von Committing Sicherheit kann zu Angriffen führen, wenn AE Verfahren in größeren Protokollen verwendet werden. Dies kann beispielsweise am Angriff gegen das Facebook Message Franking Protokoll [DGRW18] beobachtet werden.

  Von 2018 bis 2023 führte das National Institute of Standards and Technology (NIST) einen Standardisierungsprozess für Lightweight Cryptography (LWC) durch [NIST]. Aus den 57 ursprünglichen Einreichungen wurden 10 AE Verfahren als Finalisten ausgewählt, bevor Ascon 2023 zur Standardisierung ausgewählt wurde. Mehrere Finalisten erwiesen sich als anfällig für verschiedene Committing Angriffe [KSW23].

  Aufgabe:

  Das Ziel des Praktikums ist es, die Committing Angriffe aus [KSW23] zu implementieren. Dafür sind die folgenden Schritte notwendig:

  1. Einlesen in Authenticated Encryption und Committing Sicherheit
  2. Vertraut machen mit den bestehenden Implementierungen der NIST LWC Finalisten
  3. Implementieren der Committing Angriffe

  Anforderungen:

  - Programmierkenntnisse in C
  - Interesse an Kryptographie
  - Englischkenntnisse (Lesen von englischen Papers)

  Referenzen:

[DGRW18] – Dodis, Grubbs, Ristenpart, Woodage. Fast message franking: From invisible salamanders to encryptment. CRYPTO 2018. (https://ia.cr/2019/016)
[KSW23] – Krämer, Struck, Weishäupl. Committing AE from sponges: Security analysis of the NIST LWC finalists. Preprint 2023. (ia.cr/2023/1525)
[NIST] - https://csrc.nist.gov/Projects/lightweight-cryptography/

- Termin Kickoff-Meeting: nach Absprache
- Projektzeitraum: 23.04.2025 bis 25.07.2025 (flexibel)
- Abgabedeadline: 25.07.2025 (flexibel)