PS Einführung Kryptographie und IT-Sicherheit

Salzburg, T03, 14:45 *17.03.2025*
***Abgabe**: bis SO 16.03. 12:00 an uhl@cs.sbg.ac.at*

6.) Erklären sie, warum bei Hamming ECC die Parity Bits zwischen den Datenbits eingefügt werden und nicht einfach alle geschlossen den Datenbits vorangestellt oder angehängt werden. Illustrieren sie das anhand eines Beispiels unter Verwendung eines (15,11)-Hamming Codes.

7.) Erklären sie, warum es allgemein schwierig ist, aus biometrischen Messungen kryptographisches Schlüsselmaterial zu gewinnen. Illustrieren sie das ganz konkret anhand der Features/Merkmale einer bestimmten biometrischen Modalität (also wie würde man konkret einen Schlüssel generieren und was ist das Problem).

8.) Erklären sie das Fuzzy Commitment Scheme zur Erzeugung von kryptographischen Schlüsseln aus biometrischen Messungen. Welche Rolle spielen dabei fehlerkorrigierende Codes? (siehe auch S.67f meines Biometrie Skriptums https://www.cosy.sbg.ac.at/∼uhl/biometrics_slides.pdf).

9.) Implementieren sie das Fuzzy Commitment Scheme mit Hilfe von Hamming ECC (gerne library verwenden für letzteres). Als binäres biometrisches Template generieren sie ein zufälliges binäres Muster, der Schüssel soll 128 Bits lang sein. Die biometrische Varianz simulieren sie durch Kippen einiger Bits. Dokumentieren sie den korrekten Key-release trotz biometrischer Varianz.

VIEL ERFOLG !!