

Hochschule Ostwestfalen-Lippe
University of Applied Sciences
inIT – Institut Industrial IT
Prof. Dr. Stefan Heiss

Liebigstraße 87
32657 Lemgo

Abschlussarbeit

EAX auf einer JavaCard

Im Rahmen dieser Abschlussarbeit soll der EAX-Modus für Blockchiffren auf einer JavaCard implementiert werden. EAX (Authenticated Encryption with Associated Data) ist ein Verfahren zur gleichzeitigen Verschlüsselung und Authentifizierung von Nachrichten auf Basis einer symmetrischen Blockchiffre. Die zu entwickelnde Lösung soll eine auf der JavaCard verfügbare AES-Implementierung nutzen.

Das erste Ziel dieser Abschlussarbeit ist eine detaillierte Untersuchung und Beschreibung des EAX-Modus und die Einarbeitung in die JavaCard-Programmierung. Im zweiten Schritt soll eine Implementierung des EAX-Modus für eine JavaCard erstellt werden, welche schließlich in Bezug auf die Performance zu untersuchen und zu optimieren ist.

Ansprechpartner: Prof. Dr. Stefan Heiss (stefan.heiss@hs-owl.de)
M.Sc. Stefan Hausmann (stefan.hausman@hs-owl.de)