Documentation

Satyam Sachan

June 2022

1 Introduction

The `test_crypto` library implements the common cryptographic functions found in the Secure Hardware Extension (SHE). This document covers the construction and usage of these functions.

2 Implemented Primitives

The following primitives are available as a module:

- Encryption/Decryption: `AES-ECB` (Electronic Code Book) and `AES-CBC` (Cipher Block Chaining).
- Hash Function: `Miyaguchi-Preneel Compression`.
- `MAC`: `Cipher-based MAC` with `AES` as the pseudorandom function.

2.1 `Miyaguchi-Preneel Compression`

The M-P Compression function uses `AES-ECB` as a pseudoerandom function in order to generate a hash value.

2.2 `CMAC`