Sprawozdanie z realizacji zadania

szer. pchor. Agata Greguła

10 września 2020

Spis treści

1 Wstęp

Zadanie wykonane zostało w ramach praktyk w STK NCBC w dniach 07.09.2020 - 11.09.2020. Praktyki prowadzone były w trybie zdalnym.

1.1 Zakres zadania indywidualnego

Zadanie polegało na wykonaniu implementacji szyfru strumieniowego **Grain-128AEAD** w funkcyjnym języku programowania - Cryptol, następnie sprawdzenie jego poprawności oraz zgodności z implementacją referencyjną napisaną w języku C za pomocą formalnej weryfikacji przy użyciu skryptu wykonanego w SAW (Software Analysis Workbench).

1.2 Wykonane oprogramowanie

Kody źródłowe zostały umieszczone w repozytorium: https://github.com/inlonelyday/cryptol_AG.

- **Grain.cry**

2 Grain-128AEAD

2.1 Wstęp teoretyczny

- Szyfr strumieniowy
- 2011r.
- autorzy: Martin Hell, Thomas Johansson, Willi Meier, Jonathan Sönnerup, Hirotaka Yoshida
- 128-bitowy klucz, 96-bitowy nonce

2.2 Oznaczenia

W opisie poszczególnych operacji algorytmu użyto następujących oznaczeń.