Cryptol: ZUC stream cipher versions 1.4 and 1.5

Description ZUC is a stream cipher for confidentiality and integrity proposed as an ETSI standard. The human readable specification is clear and expressed mathematically. This is translated almost directly to Cryptol. A stream cipher should be resistant to a collision attack but it is shown that v1.4 is not and v1.5 is.

Purpose An example of a protocol specified in Cryptol. Cryptol constructs are well suited for this kind of specification.

Audience This module is intended for:

1 The general public
2 K-12 and college classes on cyber defense
3 preparation for proficiency in the use of tools and a computing environment suitable for the study of cyber defense

Objectives After completing the module:

1 know the ZUC protocol
2 know how to translate a human readable protocol specification to Cryptol
3 know how to look for properties than ensure expected operation

Keywords ZUC, stream cipher, hardware, linear feedback shift register, collision

Category cybersecurity > education

Delivery java applets and written documentation in pdf format

Team John Franco and Ethan Link

Assessment The applets provide the means for experimentation. Questions are asked in the documentation that help with the set up of experiments. The ideas that learners come up with is evidence that the module was successful.

Workflow No particular schedule was established

Environment All materials are contained in a single jar file. The jar file can be run on any computer where java version 11 or higher and some pdf reader such as acroread or evince are available. The jar file may be executed in the cyber range or learners may download the jar file (which is considered to be an executable file) and run it on their personal computers.