**АНОТАЦІЯ**

Кваліфікаційна робота включає пояснювальну записку (51 с., 25 рис. 4 табл., 4 додатки, 20 слайдів).

Об’єкт розробки – криптографічний модуль у стандарті RBG2, в основі якого полягає хешування даних хеш-функцією Keccak. HDL-модель дозволяє хешувати введені дані та виводити результат роботи модуля хешування.

Криптографічний модуль дозволяє: хешування вхідних даних; генерувати криптографічно стійкі випадкові послідовності. В процесі розробки були використані мова опису архітектури VHDL та стандарти FIPS 202, NIST Special Publication 800-90A, NIST Special Publication 800-90B, NIST Special Publication 800-90C. Для моделювання роботи хеш-функції Keccak використовується мова опису архітектури VHDL в середовищі Active-HDL.

В ході розробки:

* Проведено аналіз хеш-функцій з конкурсу SHA-3.
* Проведено аналіз вразливостей хеш-функцій.
* Проведено аналіз генератора псевдовипадкових бітів.
* Сформульовано вимоги до реалізації криптографічного модуля.
* Описано HDL-модель апаратної реалізації хеш-функції Keccak.
* Описано HDL-сутності генератора випадкових бітів на базі хеш-функції Keccak.

Ключові слова: КРИПТОГРАФІЧНИЙ МОДУЛЬ, ХЕШ-ФУНКЦІЯ KECCAK, SHA-3, ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ БІТІВ, VHDL.

ABSTRACT

The qualification work includes an explanatory note (51 pages, 25 figures, 4 tables, 4 appendices, 20 slides).

The object of development is a cryptographic module based on the RBG2 standard, which utilizes data hashing with the Keccak hash function. The HDL model enables the hashing of input data and outputs the results of the hashing module.

The cryptographic module allows for the hashing of input data and the generation of cryptographically secure random sequences. The development process involved the use of the VHDL architecture description language and the standards FIPS 202, NIST Special Publication 800-90A, NIST Special Publication 800-90B, NIST Special Publication 800-90C. The VHDL architecture description language in the Active-HDL environment was used to model the operation of the Keccak hash function.

During the development:

 • An analysis of the SHA-3 competition hash functions was conducted.

• An analysis of the vulnerabilities of hash functions was performed.

• An analysis of the pseudorandom bit generator was conducted.

 • Requirements for the implementation of the cryptographic module were formulated.

• The HDL model of the hardware implementation of the Keccak hash function was described.

• The HDL entities of the pseudorandom bit generator based on the Keccak hash function were described.

Keywords: CRYPTOGRAPHIC MODULE, KECCAK HASH FUNCTION, SHA-3, PSEUDORANDOM BIT GENERATOR, VHDL.