МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Кафедра математического моделирования и анализа данных

Курсовая работа

Криптография на основе функций хэширования: подписи без состояния

Болтач Антон Юрьевич
Студент 3 курса 9 группы
Научный руководитель
С. В. Агиевич

Минск, 2019 г.

Содержание

Введение

Одноразовые подписи(OTS)

2.1 Одноразовая подпись Винтерница(WOTS)

2.2 Дополненная подпись Винтерница(WOTS+)

2.2.1 Обоснование стойкости(WOTS+)

Деревля Меркля(MSS)

Многоразовые подписи(MTS)

4.1 HORS

4.2 PORS

Подписи без состояния

5.1 SPHINCS

5.2 Gravity-SPHINCS

5.3 SPHINCS+

Stateful vs Stateless

Заключение

Литература