

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

1	Введение	3
2	Одноразовые подписи(OTS)	4
2.1	Одноразовая подпись Винтерница(WOTS)	4
2.2	Дополненная подпись Винтерница(WOTS+)	4
2.2.1	Обоснование стойкости(WOTS+)	4
3	Деревя Меркля(MSS)	5
4	Многоразовые подписи(MTS)	6
4.1	HORS	6
4.2	PORS	6
5	Подписи без состояния	7
5.1	SPHINCS	7
5.2	Gravity-SPHINCS	7
5.3	SPHINCS+	7
6	Stateful vs Stateless	7
7	Заключение	8
8	Литература	9

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