

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ
Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе
«Криптография на основе функций хэширования: подписи без
состояния»

Болтач Антон Юрьевич

Научный руководитель - доцент кафедры математического
моделирования и анализа данных канд. физ.-мат. наук С. В. Агиевич

Минск, 2020

РЕФЕРАТ

Дипломная работа, 34 с., 6 рис., 1 табл., 7 источников, 1 прил.

Ключевые слова: ЭЦП, ОДНОРАЗОВЫЕ ПОДПИСИ, ДЕРЕВЬЯ МЕРКЛЯ, МНОГОРАЗОВЫЕ ПОДПИСИ, ПОДПИСИ БЕЗ СОСТОЯНИЯ, БЛОКЧЕЙН BITSHARES.

Объект исследования — ЭЦП на основе функций хэширования: подписи без состояния.

Цель работы — изучить возможность использования на практике систем ЭЦП на основе функций хэширования без состояния.

Результаты работы — проведён сравнительный анализ систем ЭЦП на основе функций хэширования без состояния; разработаны программные реализации систем SPHINCS, SPHINCS⁺, Gravity-SPHINCS; программные реализации интегрированы в блокчейн-систему Bitshares.

ABSTRACT

Diploma work, 34 p., 6 pic., 1 tab., 7 sources, 1 app.

Keywords: DIGITAL SIGNATURE, ONE-TIME SIGNATURE, MERKLE SIGNATURE SCHEME, FEW-TIME SIGNATURES, STATELESS SIGNATURES, BLOCKCHAIN BITSHARES.

Object of research — Hash based digital signatures: stateless.

Purpose of work — research hash-based stateless digital signature algorithms in practice.

Results of work — a comparative analysis of hash-based stateless digital signature algorithms; development SPHINCS, SPHINCS⁺, Gravity-SPHINCS systems; integrated into the Bitshares blockchain system.