

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
1.1	Почему Hash-Based Signatures?	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

Цифровые подписи широко используются в Интернете, в частности, для аутентификации, проверки целостности и отказа от авторства. Алгоритмы цифровой подписи, наиболее часто используемые на практике - RSA, DSA и ECDSA, - основаны на допущениях твердости о задачах теории чисел, а именно факторизации составного целого числа и вычислении дискретных логарифмов. В 1994 году Питер Шор показал, что эти теоретические проблемы с числами могут стать решаемыми при наличии квантовых вычислений. Квантовые компьютеры могут решить их за полиномиальное время, ставя под угрозу безопасность схем цифровой подписи, используемых сегодня. Хотя квантовые компьютеры еще не доступны, их развитие происходит быстрыми темпами и поэтому представляет собой реальную угрозу в течение следующих десятилетий. К счастью, постквантовая криптография предоставляет множество квантостойких альтернатив классическим схемам цифровой подписи. Подписи на основе хеша или подписи Меркле, как они также известны, являются одной из наиболее многообещающих из этих альтернатив.

1.1 Почему Hash-Based Signatures?

Есть много причин использовать схемы подписи на основе хеша и предпочитать их другим альтернативам. Хотя в самой ранней схеме подписи отсутствуют практические требования к производительности и пространству, современные схемы на основе хэшей, такие как XMSS, достаточно быстры, при небольшом размере. Также требования безопасности являются убедительными. Использование такой схемы подписи всегда требует хеш-функции. В то время как другие схемы подписи полагаются на дополнительные предположения о неразрешимости для генерации подписи, для решения на основе хеша требуется только безопасная хеш-функция. Некоторые схемы, основанные на хэше, даже уменьшают потребность в хэш-функции, устойчивой к столкновениям, до той, которая должна выдерживать атаки только на второе изображение. В качестве примера известны практические атаки средствами защиты от столкновений функции MD5, но мы до сих пор не знаем о виртуальных атаках на второе изображение.

Одноразовые подписи(OTS)

Одноразовые подписи (OTS) называются одноразовыми, поскольку сопутствующие сокращения безопасности гарантируют безопасность только при атаках с одним сообщением. Однако это не означает, что эффективные атаки возможны при атаках с двумя сообщениями. Особенно в контексте основанных на хэшировании OTS (которые являются основными строительными блоками последних предложений по стандартизации) это приводит к вопросу о том, приводит ли случайное повторное использование одноразовой пары ключей к немедленной потере безопасности. Проанализируем безопасность наиболее известных хэш-основанных OTS: WOTS, WOTS+ при различных видах атак с двумя сообщениями. Интересно, что оказывается, что схемы все еще безопасны при двух атаках сообщений, асимптотически.

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