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

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 квантовостойких 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+)

Деревья Меркля(MSS)

Первый способ создать схему многократной подписи из схемы одноразовой подписи - использовать конструкцию, предложенную Мерклом в 1989 году. Учитывая целые числа n, h и хэш-функцию $H : \{0,1\}^{2n} \to \{0,1\}^n$, так называемое Дерево Меркля представляет собой двоичное дерево высоты h, узлы которого помечены значением $x \in \{0,1\}^n$, таким образом, что значение каждого внутреннего узла вычисляется как $x = H(y||z)$, где y и z - значения левых и правых дочерних элементов.

Корневое значение r может быть сначала отправлено для последующей аутентификации любого из 2^h листового значения $v_1, ..., v_{2^h}$. Действительно, чтобы проверить, что значение v находится в листовом индексе i, нужно просто v, i и путь аутентификации i. Этот путь аутентификации содержит братьев и сестер всех узлов на пути между листом i и корнем (значения h). Это позволяет рекурсивно вычислять значения внутренних узлов вплоть до корня и сравнивать результат с r.

Эта конструкция позволяет превратить схему одноразовой подписи в схему многократной подписи следующим образом. Учитывая 2^h экземпляров OTS, подписывающий создает дерево Меркля, каждое листовое значение которого являются открытым ключом экземпляра OTS. Общий открытый ключ - это корневое значение. i-я подпись содержит подпись, сгенерированную i-м экземпляром OTS, а также путь аутентификации i.

Следовательно, открытый ключ содержит только n битов, по сравнению с подходом 2^h OTS открытых ключей. Однако время генерации ключа экспоненциально в h, потому что на этом этапе необходимо вычислить полное дерево Меркля. Например, $h = 20$ возможно, но может быть недостаточно для всех подписывающих. Кроме того, подписывающий должен отслеживать индексы i, которые уже были использованы, поэтому схема является $stateful$.

Многоразовые подписи(MTS)

В то время как одноразовые подписи обеспечивают удовлетворительную криптографическую безопасность для подписания и проверки транзакций, для них характерен существенный недостаток - их можно использовать безопасно только один раз. Поэтому существуют схемы подписи для включения более чем одной действительной одноразовой подписи, что позволяет сформировать предварительно столько подписей, сколько будет пар ключей одноразовых подписей. Логичным путем достижения этого является построение двоичного хеш-дерева, известного как дерево Меркля.

4.1 HORS

4.2 PORS

Подписи без состояния

5.1 SPHINCS

5.2 Gravity-SPHINCS

5.3 SPHINCS+

Stateful vs Stateless

Схемы с сохранением состояния имеют дерево Меркля с количеством одноразовых подписей внизу. Каждая разовая подпись может быть использована один раз, следовательно, подписывающий должен отслеживать, какие из них он использовал. То есть, когда он использует одноразовую подпись для подписи сообщения, он должен обновить свое состояние.

Схемы без состояния имеют большое дерево, но внизу у них есть несколько подписей времени. Каждая такая небольшая временная подпись может подписать несколько сообщений. Таким образом, когда подписывается сообщение, подписывающий выбирает случайную подпись с небольшим количеством времени, использует ее для подписи сообщения, а затем подтверждает ее подлинность через деревья Меркля вплоть до корня, который является открытым ключом. Поскольку мы используем несколько раз подпись, мы не против, если мы иногда выбираем одну и ту же подпись несколько раз. Схема подписи нескольких раз может справиться с этим. И, поскольку нам не нужно обновлять какое-либо состояние при генерации подписи, это считается «без сохранения состояния».

Заключение

Литература