АЛГОРИТМЫ МНОГОРАЗОВОЙ ПОДПИСИ НА ОСНОВЕ ХЕШ-ФУНКЦИ Й

Марухненко А.С.
Научный руководитель – д.т.н., проф. Халимов Г.З
Харьковский национальный университет радиоэлектроники (61166, Харьков, пр. Науки,14, каф. Безопасности информационных технологий), тел. (057) 702-14-25 e-mail: oleksandr.marukhnenko@nure.ua

Modern asymmetric cryptography is vulnerable to quantum computing. A possible solution is to use hash-based digital signatures. This class includes various algorithms: one-time and few-time signatures and schemes based on their composition. This paper discusses a reusable signature algorithm with a decrease in the security: HORS and its modifications PORS and FORS. When creating a new signature, these algorithms reveal a part of the secret key, so the key pair can be used to sign a limited number of messages, this number depends on chosen system parameters.

Стойкость большинства используемых асимметричных криптосистем базируется на сложности решения задач факторизации, дискретного логарифма в простом поле или группе точек эллиптической кривой. В случае использования алгоритма Шора на квантовом компьютере, решение будет иметь полиномиальную сложность, следовательно, в обозримом будущем такие криптосистемы будут небезопасны. Целью работы является анализ перспективных постквантовых алгоритмов цифровой подписи на основе хеш-функций.

ЭЦП на основе хеш функций можно классифицировать следующим образом:

- одноразовые (Лампорта, Винтерница);
- многоразовые с использованием деревьев Меркли;
- многоразовые со снижением стойкости (HORS, FORS, PORS);
- многоразовые с использованием гипердеревьев (SPHINCS, SPHINCS+, Gravity-SPHINCS, XMMS-MT).

Рассмотрим алгоритмы многоразовой ЦП со снижением стойкости, основная идея заключается в том, что секретный ключ имеет достаточно большой размер (например, 1 мегабайт) и при создании подписи раскрывается некоторая его часть, таким образом каждая новая подпись снижает стойкость ключа и увеличивает вероятность подделки.

Алгоритм HORS (Hash to Obtain Random Subset – хеш для получения случайного подмножества) [1] помимо используемых хеш-функций имеет два общесистемных параметра $t = 2^{\tau}$ - размер множества ключей, k – количество элементов в подписи, $kt = n$ - длина хеша сообщения. Модификация данного алгоритма – HORST используется в ЭЦП SPHINCS.

Секретный ключ – массив из t случайных чисел, их размерность определяется требуемой стойкостью системы $SK = (sk_0, sk_1, ..., sk_{t-1})$.

Открытый ключ – массив из хешей элементов секретного ключа $PK = (pk_0, pk_1, ..., pk_{t-1}) = (H(sk_0), H(sk_1), ..., H(sk_{t-1}))$, для уменьшения размера открытого ключа может быть использована дерево Меркли, как это реализовано в алгоритме HORST.

Подпись – хеш подписываемого сообщения делится на блоки по τ бит, в подпись включаются элементы секретного ключа, соответствующие значениям блоков $H(M) = (h_0, h_1, ..., h_{k-1})$, $\sigma = (sk_{h_0}, sk_{h_1}, ..., sk_{h_{k-1}})$.

Проверка – элементы подписи хешируются и сравниваются с соответствующими элементами открытого ключа.

Подпись HORS имеет недостаток, заключающийся в том, что при совпадении значений блоков в хеше сообщения в подписи будут использованы одни и те же элементы ключа, что приводит к снижению стойкости. Алгоритм PORS (PRNG to obtain a random subset – генератор псевдослучайных чисел для получения случайного подмножества) используется в криптосистеме Gravity-SPHINCS [2] и устраняет описанный недостаток. Системные параметры и ключи остаются без изменений, в алгоритмы создания и проверки подписи после разбиения хеша сообщения добавляется следующая проверка: если $h_i = h_j$, $i > j$, h_i отбрасывается, генерируется новый блок длины τ и добавляется в конец последовательности, операция повторяется до тех пор, пока все блоки не будут уникальными. Генерация осуществляется при помощи ГПСЧ, инициализируемым сообщением.

Алгоритм FORS (Forest Of Random Subset) также является модификацией HORST, используемой в схеме SPHINCS+ [3]. Его основное отличие заключается в том, что для каждого подписываемого блока используется свой массив случайных чисел, т.е. размер секретного ключа увеличивается в k раз, но благодаря использованию деревьев Меркли размер открытого ключа остаётся неизменным.

Цифровые подписи PORS и FORS являются альтернативными модификациями алгоритма HORST, устраняющими возможность повторения компонентов подписи. Алгоритм FORS сложнее в реализации, однако позволяет создать больше подписей без потери стойкости.

Список источников:

1. Leonid Reyzin and Natan Reyzin. Better than BiBa: Short one-time signatures with fast signing and verifying. 2002.

2. Jean-Phillippe Aumasson and Guillaume Endignoux. Gravity-SPHINCS – Submission to the NIST's post-quantum cryptography standardization process, 2017.

3. Daniel J. Bernstein and others. SPHINCS+ – Submission to the NIST's post-quantum cryptography standardization process, 2017.