Выбор оптимальных параметров криптосистемы SPHINCS+

Александр Марухненко[1], Геннадий Халимов[1], Антон Янко[2]

1. Кафедра безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, УКРАИНА, г. Харьков, пр. Науки, 14,

2. Кафедра автоматизации и проектирования вычислительной техники, Харьковский национальный университет радиоэлектроники, УКРАИНА, г. Харьков, пр. Науки, 14,
E-mail: oleksandr.marukhnenko@nure.ua

Краткая аннотация – The article describes a structure and parameters of the SPHINCS+ cryptosystem. The right choice of parameters allows you to optimize system performance relative to the time and memory costs. We propose few sets of parameters for 384 and 512-bit security.

Ключевые слова – ЭЦП на основе хеш-функций, SPHINCS, постквантовая криптография, дерево Меркли.

I. Введение

Криптосистемы на основе хеш-функций является перспективным направлением постквантовой криптографии. Особенностью криптосистем этого класса является ограниченное количество подписей, которые могут быть созданы с использованием одного ключа. Первые разработанные алгоритмы позволяли подписывать только одно сообщение, что стало причиной их низкой популярности. Для устранения этого недостатка сначала были предложены хеш-дерева, построенные на основе одноразовых подписей, а затем гипер-деревья, состоящие из хеш-деревьев. В основе алгоритма SPHINCS + лежит именно конструкция гипер-дерева. Использование такой многоуровневой структуры требует установки и обоснование ряда параметров.

Целью работы является проанализировать структуру алгоритма SPHINCS + и предложить определенные параметры для заданных показателей стойкости.

II. Подписи W-OTS и FORS

Общая идея подписи Винтерница (W-OTS – Winternitz One-Time Signature) [1] заключается в следующем: секретным ключом является массив случайных битовых последовательностей, открытым ключом является массив прохешированных *w* (параметр Винтерница) раз элементов приватного ключа, при создании подписи сообщения разбивается на блоки по *w* битов, в конец добавляется контрольная сумма, подпись состоит из элементов приватного ключа, прохешированных определенное количество раз, в зависимости от значения соответствующего блока. Во время проверки элементы подписи «дохешируются» до *w* раз и сравниваются с открытым ключом.

Подпись FORS относится к классу многоразовых подписей с постепенным снижением стойкости. Основная идея этой группы алгоритмов заключается в том, что частный ключ имеет достаточно большой размер, например, 1 мегабайт, при создании подписи раскрывается некая «случайная» часть ключа, таким образом каждая новая подпись увеличивает вероятность подделки. Безопасная количество использований одной ключевой пары определяется требованиями к стойкости системы.

Алгоритм FORS (Forest Of Random Subset) является модификацией алгоритма HORST и используется в схеме SPHINCS + [3]. Суть алгоритма заключается в том, что сообщению однозначно соответствует некоторое подмножество элементов заданного множества (секретного ключа), которое становится подписью, для проверки элементы подписи хешируются и сравниваются с соответствующими элементами из множества хеш-значений (открытого ключа). Особенность FORS заключается в том, что для каждого блока, который подписывается, используют отдельный массив случайных чисел.

III. Дерево и гипер-дерево Меркли

Метод многократного использования пары ключей подпис на основе хеш-функции, предложенный Меркли, базируется на применении так называемых хеш-деревьев или деревьев Меркли [2]. Хеш-деревом называют полное бинарное дерево, в листовые вершины которого помещены хеши от блоков данных, а внутренние вершины содержат хеши от конкатенации значений в дочерних вершинах. Корневой узел дерева содержит хеш от всего набора данных, то есть хеш-дерево является однонаправленной хеш-функцией.

Листьями дерева выступают хеш-значения открытых ключей одноразовых подписей, например ЦП Винтерница. Открытым ключом является корень дерева. Для подтверждения того, что использован в подписи открытый ключ OTS принадлежит данному дереву, к подписи добавляется путь аутентификации - элементы дерева, необходимые для прохождения заданного листа к корню дерева, номер использованного одноразового ключа и сам открытый ключ OTS.

Таким образом проверка подписи состоит из двух этапов - проверка подписи по открытому ключу, аутентификация ключа. В алгоритмах, в которых открытый ключ полностью исчисляется с подписи (WOTS), нет необходимости передавать используемый ключ, позволяющий уменьшить размер подписи.

Описанные ранее механизмы не решают проблемы ограниченного количества использований одной пары ключей. Для FORS стойкость пропорциональна количеству элементов ключа, соответственно большее количество подписей требует увеличения размеров приватного (может быть заменен инициализатор для ГПСЧ) и открытого ключей. Для подписей, основанные на деревьях Меркли, количество

использований также ограничивается при генерации пары ключей, а также для построения дерева на n подписей необходимо сгенерировать n пар ключей одноразовых подписей и провести $2n$ хешированиий внутри дерева, это требует значительных вычислений уже для деревьев с тысячами листьев.

Альтернативным решением является использование структуры гипердерева, представляющая собой дерево из хеш-деревьев, листья деревьев верхнего уровня используются для подписи корней деревьев, лежащих уровнем ниже [4]. Открытым ключом пользователя есть корень верхнего дерева. Такая схема позволяет генерировать дерева низших уровней, не меняя при этом общего ключа. Подпись сообщения включает в себя непосредственно подпись, пути аутентификации на каждом уровне и подписи для промежуточных узлов.

IV. Алгоритм SPHINCS+

Наиболее перспективным ЭЦП на базе хеш-функций в настоящее время является семейство алгоритмов SPHINCS, а именно две независимые модификации первичного подписи SPHINCS - SPHINCS+ [3] и Gravity-SPHINCS, которые были участниками первого тура конкурса постквантовых алгоритмов NIST. Анализ алгоритма SPHINCS+ продолжается в рамках второго тура.

Данный алгоритм использует гипердерево следующего вида: листьями деревьев на всех уровнях являются хеш-значения открытых ключей подписи WOTS+, которые используются для подписи корня соответствующего дерева уровнем ниже, на нижнем уровне ключи используются для подписания открытых ключей алгоритма FORS. Индекс используемой ключевой пары подписи FORS выбирается на основе дайджеста сообщения. Подпись сообщения представляет собой подпись FORS, соответствующая ему подпись WOTS+ из листа гипер-дерева, подписи корней промежуточных деревьев, пути аутентификации и случайная последовательность, которая использовалась во время генерации подписи.

Общесистемные параметры:

- n – параметр безопасности, определяет байтовую длину всех элементов гипер-дерева;
- h – высота гипер-дерева;
- d – количество слоёв гипер-дерева, каждый содержит хеш-деревья высоты $h' = h / d$;
- w – параметр Винтерница;
- k – количество деревьев в FORS;
- t – количество листов одного дерева FORS.

При выборе конкретных параметров алгоритма должен достигаться пространственно-временной компромисс, с одной стороны подпись может быть меньше, но время создания и проверки больше, с другой создания и проверка будут быстрее, но подпись занимает больше памяти. Авторы SPHINCS+ предлагают два набора параметров: «быстрый» и «маленький» для уровней стойкости 128, 192 и 256 бит. Мы предлагаем следующие значения параметров для обеспечения уровней стойкости 384 и 512 бит (Табл.1). Оценка оптимальности предложенных параметров требует дальнейших исследований.

ТАБЛИЦА 1

РЕКОМЕНДУЕМЫЕ ПАРАМЕТРЫ ДЛЯ РАЗНЫХ УРОВНЕЙ СТОЙКОСТИ

	n	h	d	τ	k	w	sec	size
128s	16	64	8	15	10	16	133	8080
128f	16	60	20	9	30	16	128	16976
192s	24	64	8	16	14	16	196	17064
192f	24	66	22	8	33	16	194	35664
256s	32	64	8	14	22	16	255	29792
256f	32	68	17	10	30	16	254	49216
384s	48	64	8	16	23	16	391	59904
384f	48	60	15	10	39	16	390	94800
512s	64	66	6	19	26	16	519	87872
512f	64	65	13	12	42	16	512	148160

Выводы

Цифровые подписи на основе хеш-функций является перспективным направлением пост-квантовой криптографии. Разработчикам криптосистемы SPHINCS+ удалось устранить недостатки, которые имелись в предыдущих алгоритмах. Сложная структура гипер-дерева требует выбора ряда системных параметров, влияющих на стойкость системы, скорость ее работы и размеры подписи, поэтому сложно однозначно выбрать лучший набор составляющих, поскольку в зависимости от конкретного применения требования могут меняться. Мы предложили значения параметров, которые могут быть применены в криптосистеме SPHINCS+ с устойчивостью 384 и 512 бит.

Литература

[1] Andreas Hülsing. W-OTS+ – shorter signatures for hash-based signature schemes. In Amr Youssef, Abderrahmane Nitaj, and Aboul-Ella Hassanien, editors, Progress in Cryptology – AFRICACRYPT 2013, volume 7918 of LNCS, pages 173–188. Springer, 2013.

[2] Ralph Merkle. A certified digital signature. In Gilles Brassard, editor, Advances inCryptology – CRYPTO ’89, volume 435 of LNCS, pages 218–238. Springer, 1990.

[3] Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder and others. SPHINCS+ – Submission to the NIST’s post-quantum cryptography standardization process, 2017.

[4] Andreas Hülsing, Lea Rausch, and Johannes Buchmann. Optimal parameters for XMSSMT. In Alfredo Cuzzocrea, Christian Kittl, Dimitris E. Simos, Edgar Weippl, and Lida Xu, editors, Security Engineering and Intelligence Informatics, volume 8128 of Lecture Notes in Computer Science, pages 194–208. Springer Berlin Heidelberg, 2013.