Scientific and Practical Cyber Security Journal (SPCSJ) 1(1):20-23
Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

ANALYSIS OF ONE-TIME SIGNATURE SCHEMES

A. Gagnidze, M. Iavich, N. Inasaridze, G. Iashvili

Scientific Cyber Security Association (SCSA)

ABSTRACT

Active work is being done to create and develop quantum computers. Traditional digital signature systems that are used in practice are vulnerable to quantum computers attacks. The security of these systems is based on the problem of factoring large numbers and calculating discrete logarithms. Scientists are working on the development of alternatives to RSA, which are protected from attacks by quantum computer. One of the alternatives are hash based digital signature schemes. In the article hash based one-time signatures are considered, their analysis and comparison are done. It is shown that, using Winternitz one-time signature scheme, the length of the signature and of the keys is substantially reduced. But this scheme also has disadvantages, in the case of generating keys, creating a signature and verifying a signature, one-way function should be used much more times, than in Lamport signature scheme. So, as we see, must be paid serious attention at the choice of this function, it should be quickly executed and safe

KEYWORDS: Lamport, one-time signature scheme, quantum, Winternitz.

АННОТАЦИЯ

Ведется активная работа над созданием и развитием квантовых компьютеров. Традиционные системы электронной подписи, которые используются в практике уязвимы к атакам квантовых компьютеров. Безопасность данных систем основана на проблеме факторизации больших чисел и вычислении дискретных логарифмов. Ученые работают над разработкой альтернатив RSA, которые защищены от атак квантового компьютера. Одной из альтернативой являются системы электронной подписи основанные на хешировании. В статье рассмотрены одноразовые подписи основанные на хеширование, произведен их анализ и сравнение. Показано, что с помощью схемы одноразовой подписи Винтерница существенно уменьшается длина подписи. Но также данная схема имеет недостатки, в случае генерации ключей, создания подписи и верификации подписи нужно использовать одностороннюю функцию намного больше раз, чем в случае одноразовых схем подписи Лэмпорта. Исходя из этого выбору данной функции должно быть уделено серьезное внимание, она должна быть быстро исполнима и безопасна

Ведется активная работа над созданием и развитием квантовых компьютеров.

Корпорация Google, NASA и Ассоциация космических исследований университетов (Universities Space Research Association — USRA) объединились с компанией DWAFE, которая является производителем квантовых процессоров. D-Wave 2X это квантовый процессор, который содержит 2048 физических кубитов. Из них 1152 кубита используются для выполнения расчетов. Современные, традиционные криптографические схемы являются уязвимыми по отношению к квантовым компьютерам. Квантовый компьютер с легкостью может взломать все системы основанные на задаче факторизации целых чисел, в том числе и RSA. Традиционные системы электронной подписи, которые используются в практике уязвимы к атакам квантовых компьютеров. Безопасность данных систем основана на проблеме факторизации больших чисел и вычислении дискретных логарифмов.

Ученые работают над разработкой альтернатив RSA, которые защищены от атак квантового компьютера. Одной из альтернатив являются системы электронной подписи, основанные на хешировании. Данные системы используют криптографическую хеш функцию. Безопасность данных систем электронной подписи основывается на стойкости к коллизиям хеш функций, которые они используют[1,2].

Схема одноразовой подписи Лэмпорта

Схема одноразовой подписи Лэмпорта (Lamport–Diffie one-time signature scheme) является электронной подписью, основанной на хэшировании, и представляет альтернативу для пост квантовой эпохи. Генерация ключей в данной системе происходит следующим образом: ключ подписи X данной системы состоит из 2n строк длины n, и выбирается случайным образом.

$X= (x_{n-1}[0], x_{n-1}[1], \ldots, x_0[0], x_0[1]) \in \{0,1\}^{n,2n}$

Ключ верификации Y данной системы состоит из 2n строк длины n.

$Y= (y_{n-1}[0], y_{n-1}[1], \ldots, y_0[0], y_0[1]) \in \{0,1\}^{n,2n}$

Данный ключ вычисляется следующим образом:

$y_i[j] = f(x_i[j]), 0<=i<=n-1, j=0,1$

f – это односторонняя функция:

$f: \{0,1\}^n$ à$\{0,1\}^n$;

Для генерации ключа верификации нужно использовать функцию f **2n** раз.

Подпись документа: Для подписи сообщения m произвольного размера мы переводим его в размер n с помощью функции хеширования:

$h(m)=hash = (hash_{n-1}, \ldots , hash_0)$

Функция h- это криптографическая хеш функция:

$h: \{0,1\}^*$à$\{0,1\}^n$

Подпись происходит следующим образом:

$sig= (x_{n-1}[hash_{n-1}], \ldots, x_0[hash_0]) \in \{0,1\}^{n,n}$

i-ая строчка в данной подписи выбирается равной $x_i[0]$, если i-ый бит в sign равен 0. Строчка выбирается равной $x_i[1]$, если i-ый бит в sign равен 1.

Длина подписи получается $\mathbf{n^2}$ и мы **ни разу** не используем функцию f при подписи.

Для верификации подписи $sig = (sig_{n-1}, \ldots, sig_0)$, вычисляется хеш сообщения $hash = (hash_{n-1}, \ldots, hash_0)$ и проверяется следующее равенство:

$(f(sig_{n-1}), \ldots, f(sig_0)) = (y_{n-1}[hash_{n-1}], \ldots, y_0[hash_0])$

Если равенство верно, то подпись верна.

Для верификации нужно использовать функцию f **n** раз.

Схема одноразовой подписи Винтерница

Как мы видим, в схеме одноразовой подписи Лэмпорта генерация ключа и генерация подписи довольно эффективны, размер подписи получается равным n^2 – довольно большим. Поэтому была предложена схема одноразовой подписи Винтерница (Winternitz one-time signature scheme). В данной схеме одной строчкой ключа подписываются одновременно несколько битов хешированного сообщения, этим существенно уменьшается длина подписи[3,4]. Генерация ключей в данной системе происходит следующим образом: ключ подписи X данной системы состоит из p строк длины n, ключ выбирается случайным образом. Выбирается параметр Винтерница w>=2, равный количеству битов для одновременной подписи. Вычисляется $p_1=n/w$ и $p_2=(\log_2 p_1 +1+w)/w$, $p= p_1+ p_2$

Ключ подписи X данной системы состоит из p строк длины n, выбранных случайным образом:

$X= (x_{p-1}[0], \ldots, x_0) \in \{0,1\}^{n,p}$

Ключ верификации следующий:

$Y= (y_{p-1}[0], \ldots, y_0) \in \{0,1\}^{n,p}$, где

$y_i=f^{2\wedge w-1}(x_i)$, 0<=i<=p-1

Длина подписи и ключа верификации равна **np** битам, а для генерации ключа верификации нужно использовать функцию f, $p(2^w-1)$ раз.

Подпись происходит следующим образом: Мы хешируем сообщение hash=h(m) и прибавляем к hash минимальное количество нулей, чтобы длина hash делилась на w. Затем делим его на p_1 частей длины w.

$hash=k_{p-1},\ldots, k_{p—p1}$

вычисляется контрольная сумма:

$c=\sum_{i=p—p1}^{p-1}(2^w-k_i)$

т.к. $c<= p_1 2^w$, длина ее двоичного представления меньше чем $\log_2 p_1 2^w+1$

Прибавляем к данному двоичному представлению минимальное количество нулей, чтобы его длина делилась на w, и делим его на p_2 частей длины w.

$c=k_{p2-1},\ldots, k_0$

вычисляем подпись сообщения m:

$sig=(f\hat{}k_{p-1}(x_{p-1}), \ldots, f\hat{}k_0(x_0))$

В худшем случае для подписи нужно использовать функцию f, $\mathbf{p(2^w-1)}$ раз. Размер подписи получается pn.

Для верификации подписи $sig = (sig_{n-1}, \ldots, sig_0)$ вычисляются битовые строки $k_{p-1},\ldots, k_0$.

Мы проверяем следующее равенство:

$(f\hat{}(2^w-1-k_{p-1}))(sig_{n-1}), \ldots, (f\hat{}(2^w-1-k_0))(sig_0) = y_{n-1}, \ldots y_0$

Если подпись верна, то $sig_i = f\hat{}k_i(x_i)$, т.е.

$(f\hat{}(2^w-1-k_i))(sig_i)= (f\hat{}(2^w-1))(x_i)=y_i$ верно для всех $i=p-1,\ldots, 0$

В худшем случае для верификации подписи нужно использовать функцию f $\mathbf{p(2^w-1)}$ раз.

Исходя из проведенного нами анализа схем одноразовой подписи, мы получили, что с помощью схемы одноразовой подписи Винтерница существенно уменьшается длина подписи, а также длина ключей. Однако, данная схема имеет недостатки в случае генерации ключей, создания подписи и верификации подписи нужно использовать одностороннюю функцию большее количество раз, чем в случае одноразовых схем подписи Лэмпорта. Исходя из этого, выбору данной функции должно быть уделено серьезное внимание, она должна быть быстро исполнима и безопасна.

Библиографический список:

- Гагнидзе А.Г., Явич М.П., Иашвили Г.Ю. Пост-квантовые криптосистемы // Современные научные исследования и инновации. № 5 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2016/05/67264
- Гагнидзе А.Г., Явич М.П., Иашвили Г.Ю. Улучшенный вариант пост квантовой системы Merkle // Современные научные исследования и инновации. 2017. № 5 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2017/05/
- Klintsevich, K. Okeya, C.Vuillaume, J. Buchmann, E.Dahmen. Merkle signatures with virtually unlimited signature capacity. 5th International Conference on Applied Cryptography and Network Security – ACNS07, 2007
- D. Naor, A. Shenhav, and A. Wool. One-Time Signatures Revisited: HaveThey Become Practical? Technical Report 2005/442, Cryptology ePrintArchive, 2005. Available at http://eprint.iacr.org/2005/442/ CMSS — An Improved Merkle Signature Scheme. (PDF Download Available). Available from: https://www.researchgate.net/publication/221540869_CMSS_-_An_Improved_Merkle_Signature_Scheme