Scientific and Practical Cyber Security Journal (SPCSJ) 1(2):14-20
Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

MERKLE WITH QUANTUM TRNG

A.Gagnidze, M.Iavich, G. Iashvili
Scientific Cyber Security Association

ABSTRACT:

Scientists are actively working on the development of quantum computers. Traditional cryptosystem systems that are used in practice are vulnerable to attacks by quantum computers. The security of these systems is based on the problem of factoring large numbers and calculating discrete logarithms. Active work is being conducted to create RSA alternatives, which are protected from attacks by a quantum computer. One of the proposed alternatives are hash based digital signature systems. The security of these crypto systems is based on the collision resistance of hash functions, which they use. In the article is proposed the novel version of Merkle crypto system. The system uses TRNG based on the state of qubits. The system is secure, because we do not change the principle of the crypto system, but only integrate TRNG, to reduce the size of the signature key. TRNG is completely safe; It is based on the state of qubits, which are real random number.

KEYWORDS: Merkle, quantum, TRNG, crypto, security.

РЕЗЮМЕ:

Ученые активно работают над разработкой и усовершенствованием квантовых компьютеров. Традиционные криптосистемы, которые используются в практике уязвимы к атакам квантовых компьютеров. Безопасность данных систем основана на проблеме факторизации больших чисел и вычислении дискретных логарифмов. Ведется активная над созданием альтернатив RSA, которые защищены от атак квантового компьютера. Одной из предложенных альтернативой являются системы электронной подписи, основанные на хешировании. Безопасность данных крипто систем основывается на стойкости к коллизиям хеш функций, которые они используют.

В статье предложена новый вариант крипто системы Merkle. Система использует TRNG основанный на состояниях кубитов. Система является безопасной, т.к. мы не меняем принцип работы крипто системы, а только вставляем TRNG, для уменьшения размера ключа подписи.

TRNG является полностью безопасным, т.к. он основан на состоянии кубитов, которое является реальным случайным числом.

Новая криптосистема, основанная на квантовом генераторе случайных чисел. Ученые активно работают над разработкой и усовершенствованием квантовых компьютеров. Традиционные системы криптосистемы, которые используются в практике уязвимы к атакам квантовых компьютеров. Безопасность данных систем основана на проблеме факторизации больших чисел и вычислении дискретных логарифмов.

Ведется активная над созданием альтернатив RSA, которые защищены от атак квантового компьютера. Одной из предложенных альтернативой являются системы электронной подписи основанные на хешировании. Безопасность данных крипто систем основывается на стойкости к коллизиям хеш функций, которые они используют[1].

Схемы одноразовой подписи

Были предложены одноразовые схемы электронной подписи. Была предложена схема одноразовой подписи Лэмпорта (Lamport–Diffie one-time signature scheme), данная схема является электронной подписью основанной на хешировании и представляет альтернативу для пост квантовой эпохи[2]. В данной схеме генерация ключа и генерация подписи довольно эффективна, но размер подписи является довольно большим. Для уменьшения подписи 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.

Схемы одноразовой подписи очень неудобны в использовании, т.к. для подписи каждого сообщения нужно использовать разную пару ключей. Была предложена крипто система Меркле, для решения этой проблемы. В данной системе используется бинарное дерево, чтобы заменить большое количество ключей верификации одним открытым ключом, корнем бинарного дерева. Данная криптосистема использует схему одноразовой подписи Лэмфпорта или Винтерница и криптографическую хеш функцию:

$h:\{0,1\}^* \rightarrow \{0,1\}^n$

Генерация ключа: Выберается длина дерева H>=2, одним открытым ключом можно подписать 2^H документов. Генерируются 2^H пар ключей подписи и верификации X_i, Y_i, $0<=i<=2^H$. X_i- ключ подписи**,** Y_i- ключ верификации. Вычисляются $h(Y_i)$ и используются как листья дерева. Каждый узел дерева является хешированием объединения его детей.

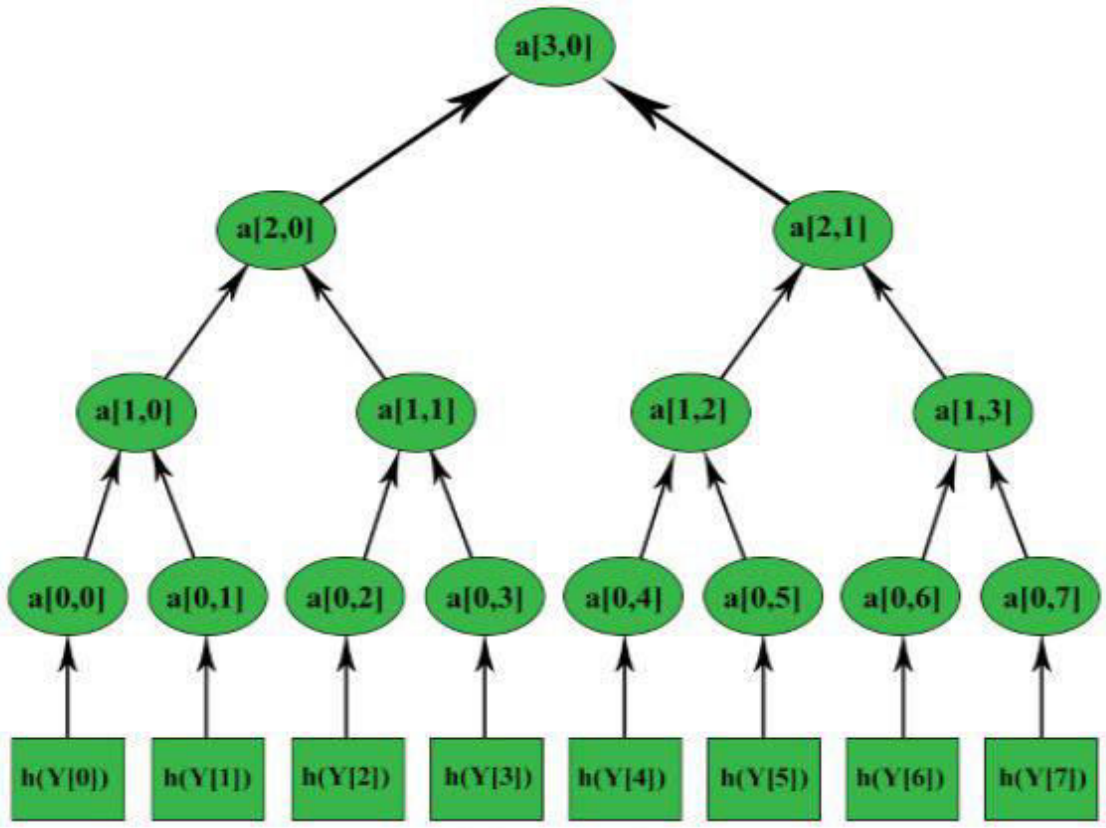

Рис. 1

На рисунке Рис. 1 показано дерево с H=3; a[i,j] узлы дерева; a[1,0]=h(a[0,0] || a[0,1]). Корень дерева является открытым ключом крипто системы - pub. Для генерации открытого ключа нужно высчитать $\mathbf{2^H}$ пар одноразовых ключей и использовать функцию h $\mathbf{2^{H+1}-1}$ раз.

Генерация подписи:

Для подписи сообщения m произвольного размера мы переводим его в размер n с помощью функции хеширования h(m) = hash, и генерируем одноразовую подпись [2], используя любой одноразовый ключ X_{any}, подпись документа будет объединением: одноразовой подписи, одноразового ключа верификации Y_{any} , индекса any и всех братских узлы $auth_i$ по отношению к Y_{any}.

Signature= (sig||any|| Y_{any}||$auth_0$,…,$auth_{H-1}$)

Верификация подписи:

Для верификации подписи мы проверяем одноразовую подпись sig с помощью Y_{any}, если она верна высчитываем все узлы a[i,j], используя $auth_i$, any и Y_{any}. Сравниваем последний узел-корень дерева с открытым ключем, если они равны то подпись верна.

Интеграция PRNG:

Для генерации открытого ключа нужно высчитать и хранить $\mathbf{2^H}$ пар одноразовых ключей. Хранить такое количество информации не эффективно в практике. Для того чтобы сохранить место было предложено использовать псевдо генератор случайных чисел PRNG [3]. При использовании PRNG достаточно хранить только семя генератора и использовать его для генерации одноразовых ключей. Нужно высчитывать одноразовые ключи дважды: один раз в стадии генерации ключей и второй раз в стадии подписи сообщения. PRNG получает семя длины n и выдает новое семя и случайное число длины n.

$PRNG : \{0, 1\}^n \rightarrow : \{0, 1\}^n \times \{0, 1\}^n$

Генерация ключа используя PRNG:

Выбирается семя s_0 длины n случайным образом, с помощью s_i мы вырабатываем sot_i, следующим образом:

$PRNG(s_i) = (sot_i , s_{i+1}) \quad 0 \leq i < 2^H$

sot_i каждый раз меняется при запуске PRNG. Для вычисления ключа X_i, достаточно знать только s_i. Работа PRNG показана на рисунке Рис. 2.

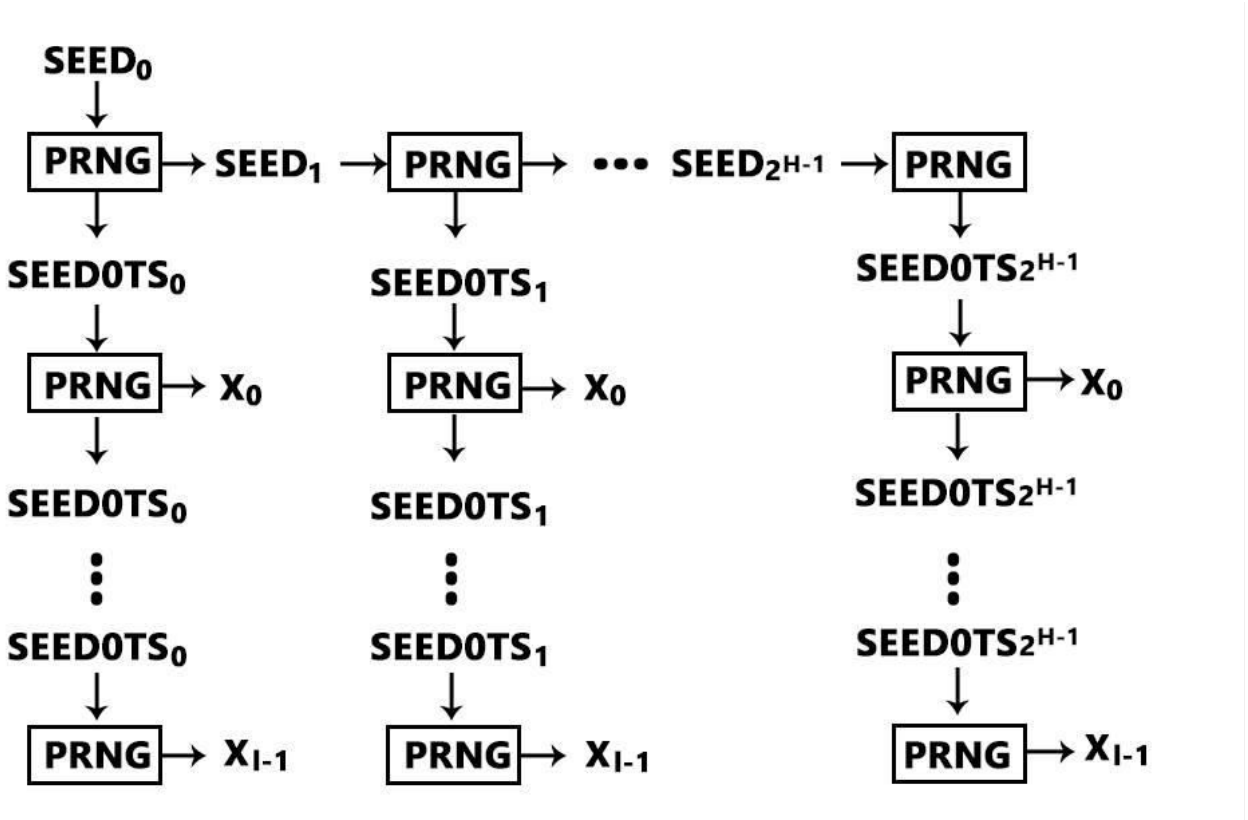

Рис. 2.

Подпись и верификация происходит аналогично как в стандартном варианте крипто системы Меркле.

Квантовые компьютеры способны взломать PRNG, которые считались безопасными против атак классических компьютеров[4]. Показана полиномиальная квантовая атака времени на PRNG Blum-Micali, который считается безопасным от угроз со стороны стандартных компьютеров. Эта атака использует алгоритм Гровера вместе с квантовым дискретным логарифмом, и способна восстанавливать значения на выходе генератора при данной атаке. Такие атаки представляют угрозу взлома PRNG, используемых во многих криптосистемах реального мира. Как мы видим крипто система Меркле с встроенным PRNG может быть уязвима к атакам квантовых компьютеров. Мы предлагаем использовать истинный генератор случайных чисел основанный на кубитах, TRNG.

Для построения данного TRNG рассмотрим квантовые состояния и кубиты.

Квантовый TRNG:

Рассмотрим систему с одним кубитом. Квантовое состояние кубита обозначается как:

$\alpha|0>+\beta|1>$, где α и β комплексные числа; $|\alpha|^2+|\beta|^2=1$

$|0>$ - земное состояние кубита, $|1>$- возбужденное состояние кубита

Данный кубит находится в состоянии $|0>$ с вероятностью α^2 и аналогично в состоянии $|1>$ с вероятностью β^2.

При измерении кубита он оказывается в одном из двух состояний с вероятностью 1.

Рассмотрим систему с двумя кубитами. Квантовое состояние двух кубитов обозначается как:

$\alpha_{00}|00>+\alpha_{01}|01>+\alpha_{10}|10>+\alpha_{11}|11>$

где α_i комплексные числа; $\sum|\alpha_i|^2=1$.

Свяжем эти кубиты с помощью парадокса Белла (Bell state), тогда квантовое состояние этих кубитов обозначается как:

$1/2^{1/2}|00>+1/2^{1/2}|11>$, т.е. при измерении данного кубита он окажется в состоянии $|0>$ с вероятностью ½ и аналогично в состоянии $|1>$ с вероятностью ½. При измерении второго кубита он окажется в том же состоянии, в котором был первый кубит при измерении с вероятностью 1.

Измеряя n кубитов можно получить истинное число размера n.

Генерация ключа с помощью квантового TRNG:

Выбирается длина дерева H>=2, одним открытым ключом можно подписать 2^H документов. Между двумя кубитами устанавливается связь с помощью парадокса Белла. Берутся 2^H пар таких кубитов q_i и b_i ;каждый q_i и b_i состоит из n кубитов. $0<=i<=2^H$; Измеряем 2^H*n кубитов q_i получаем 2^H ключей подписи X_i и вычисляем ключи верификации Y_i,. Вычисляются $h(Y_i)$ и используются как листья дерева.

Подпись и верификация сообщения:

Для подписи сообщения m произвольного размера мы переводим его в размер n с помощью функции хеширования h(m) = hash, измеряем множество состоящее из n кубитов , b_{any} = qany=X_{any} с вероятностью равной 1. Используя одноразовый ключ подписи X_{any} генерируем одноразовую подпись, подпись документа будет объединением: одноразовой подписи, одноразового ключа верификации Y_{any} , индекса any и всех братских узлы $auth_i$ по отношению к Y_{any}.

Signature= $(sig\|any\|Y_{any}\|auth_0,\ldots,auth_{H-1})$

Верификации сообщения происходит аналогично как в стандартной системе Меркле.

Безопастность системы с встроенным квантовым PRNG.

Система является безопасной, т.к. мы не меняем принцип работы крипто системы, а только вставляем TRNG, для уменьшения размера ключа подписи. TRNG является полностью безопасным, т.к. он основан на состоянии кубитов, которое является реальным случайным числом.

1. Гагнидзе А.Г., Явич М.П., Иашвили Г.Ю. Пост-квантовые криптосистемы // Современные научные исследования и инновации. 2016. № 5 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2016/05/67264

2. Gagnidze. A. G. , Iavich. M. P. , Inasaridze. N. K. , Iashvili. G. I. , Analysis of one-time signature schemes// Scientific & practical cyber security journal (SPCSJ) № 1.Electronic journal]. URL: http://journal.scsa.ge/issues/2017/09/455

3. Buchmann, J., Coronado, C., Dahmen, E., Döring, M., Klintsevich, E.: CMSS – an improved Merkle signature scheme. In Progress in Cryptology - INDOCRYPT 2006, LNCS 4329, pages 349–363. Springer-Verlag, 2006.

4. Change GUEDES, E., DE ASSIS, F., & LULA, B. (2013). Quantum attacks on pseudorandom generators. Mathematical Structures in Computer Science, 23(3), 608-634. doi:10.1017/S0960129512000825