АНАЛІЗ ШВИДКОСТІ РОЗКРИТТЯ КЛЮЧА ПІДПИСУ HORS

Марухненко О.С.
Науковий керівник – к.т.н., доц. Петренко О.Є.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Безпеки інформаційних технологій),
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 speed of key disclosure. The results show that the choice of system parameters determines the number of messages that can be signed without the threat of signature forgery.

Алгоритми ЕЦП на основі геш-функцій є перспективним класом постквантових криптосистем. Їх важлива особливість – обмежена кількість використань пари ключів, за цією ознакою їх можна класифікувати наступним чином: одноразові, багаторазові з поступовим зниженням стійкості, на основі дерев Мерклі та на основі гіпер-дерев.

Розглянемо один з декілько-разових алгоритмів підпису – HORS [1]. Особливістю є те, що кожний новий підпис знижує стійкість ключової пари, отже, кількість використань ключа повинна визначатися відповідно до необхідної стійкості. Суть алгоритму полягає в тому, що повідомленню однозначно відповідає деяка підмножина елементів заданої множини (секретного ключа), яке стає підписом, для перевірки елементи підпису гешуються і порівнюються з відповідними елементами з множини геш-значень (відкритого ключа).

Загальносистемні параметри.

1) $t = 2^{\tau}$ – розмір множини ключів;

2) k – кількість елементів у підписі, $k\tau = n$, n – бітова довжина геш-значення повідомлення.

Оскільки елементи підпису обираються зі спільної множини відповідно до значень блоків дайджесту повідомлення, при співпадінні значень блоків елементи підпису будуть дублюватися. При використанні криптографічної геш-функції, статистичні властивості якої повинні бути близькі до випадкової послідовності, ймовірність колізії між двома блока повинна дорівнювати $P = 1/t$. Таким чином, один підпис в середньому розкриває k елементів ключа, r підписів, відповідно, rk елементів, ймовірність підробити підпис без урахування можливих колізій складає $P = \left(rk \diagup t \right)^k$.

Проведемо експериментальне дослідження стійкості блоків довжини τ біт геш-значень SHA256 та SHA512 до колізій. Розглянемо

випадки, коли повідомлення представляють собою випадкові значення (табл. 1, 2 та рис.1).

Таблиця 1 – Результати досліджень

Hash	τ	Кількість створених підписів									
		1	2	4	8	16	32	64	128	256	512
SHA256	8	11.7	22.2	39.4	63.3	86.5	98.2	100	100	100	100
	16	0.02	0.05	0.1	0.2	0.39	0.78	1.55	3.08	6.06	11.8
SHA512	8	22.2	39.4	63.3	86.5	98.2	100	100	100	100	100
	16	0.05	0.1	0.2	0.39	0.78	1.55	3.08	6.06	11.8	22.1

Таблиця 2 – Результати досліджень

Hash	τ	Кількість створених підписів					
		1024	2048	4096	8192	16384	32768
SHA256	16	22.1	39.3	63.3	86.5	98.2	100
SHA512	16	39.3	63.2	86.5	98.2	100	100

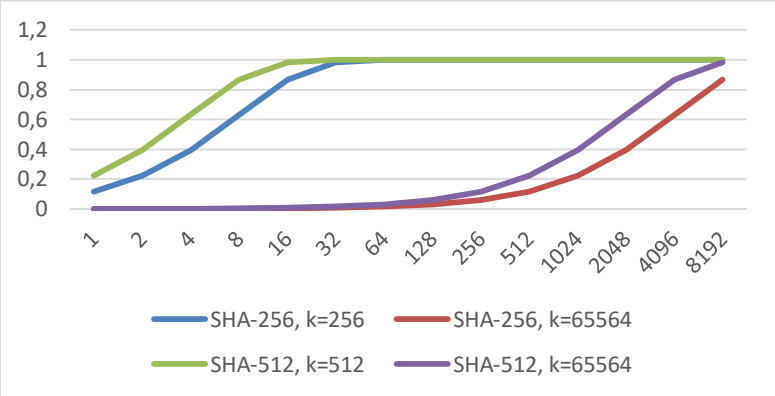

Рисунок 1 – Графік залежності розкриття ключа від кількості підписів

За результатами досліджень видно, що ключі HORS з 256 елементів можуть бути використані для підпису лише одиниць повідомлень, в той час як ключем з 65564 елементів можна безпечно підписати сотні повідомлень. Визначення конкретних значень параметрів є важливою задачею при проектуванні більш складних криптосистем, які використовують декілько-разовий підпис як один з компонентів.

Список використаних джерел:

1. Leonid Reyzin and Natan Reyzin. Better than BiBa: Short one-time signatures with fast signing and verifying. In Lynn Batten and Jennifer Seberry, editors, In-formation Security and Privacy 2002, volume 2384 of LNCS, pages 1–47. Springer, 2002.