УДК 681.32

**В. П. Семеренко**
**Б. О. Бабейко**

# ХЕШ-ФУНКЦІЇ НА ОСНОВІ ЛІНІЙНИХ АВТОМАТІВ

Вінницький національний технічний університет

***Анотація***

*Розглянуто математичні властивості хеш-функцій. Показано, що хешування, скремблювання і потокове шифрування є дуже близькими криптографічними задачами і для них можна використати єдиний математичний апарат – теорію лінійних автоматів. Запропоновано способи підвищення криптостійкості регістрів зсуву з лінійними оберненими зв'язками.*

**Ключові слова:** криптографія, хеш-функція, лінійний автомат, регістр зсуву.

***Abstract***

*Mathematical properties of hash functions are considered. It is shown that hashing, scrambling and streaming encryption are very close cryptographic problems and for them you can use a single mathematical apparatus − the theory of linear automaton. The methods to increase the cryptographic stability of shift registers with linear feedback are proposed.*

**Keywords**: cryptography, hash function, linear automaton, shift register

В сучасній криптографії важливу роль відіграють хеш-функції. Хеш-перетворення використовуються при зберіганні паролів, генерації ключів, засвідчення документів. Хеш-функція $h(X)$ отримує на вході послідовність $X$ довільної довжини і формує на виході хеш-образ $h(X)$ фіксованої довжини. Жодної секретної інформації для обчислення $h(X)$ не потрібно [1].

Нагадаємо, що $h(X)$ є однонаправленою функцією, тобто для неї повинні виконуватись такі умови [2]:

– для кожного текстового повідомлення $X$ легко обчислити значення $h(X)$,

– для заданого $Y$ дуже важко знайти таке $X$, щоб $Y = h(X)$.

Всі сучасні криптоалгоритми базуються на принципі Кірхгофа [3], згідно якого секретність шифру забезпечується секретністю ключа, а не секретністю алгоритму шифрування, тобто супротивнику може бути відома вся програмно-апаратна реалізація, за винятком паролів і ключів.

Це означає, що потрібно глибоко вивчати математичні основи криптографії, аналізувати та усувати можливі слабкі місця нових методів захисту інформації.

На жаль, до цього часу повністю не склалась термінологія в цій сфері, що затрудняє спілкування між собою спеціалістів, в першу чергу інженерів та практиків. Наприклад, давно триває дискусія в Інтернеті про підвищення криптостійкості паролів за допомогою "статичної солі" та "динамічної солі" [4].

В різних сферах науки часто зустрічаються ситуації, коли для опису схожих математичних перетворень можна використати однаковий математичний апарат. Це дає можливість використати однакові терміни та єдине математичне обґрунтування для різноманітних задач. Саме такими близькими задачами є хешування, скремблювання і потокове шифрування [5]. Для цих задач найзручнішою математичною основою є теорія лінійних автоматів, або, точніше, лінійних послідовнісних схем (ЛПС). Ця математична модель над полем Галуа базується на функції переходів

$$S(t+1) = A \times S(t) + B \times U(t),$$

і функції виходів

$$Y(t) = C \times S(t) + D \times U(t),$$

де $t$ – дискретний час,

$A, B, C, D$ – характеристичні матриці ЛПС, $S(t); U(t), Y(t)$ – слова стану, вхідне і вихідне.

Тепер можна звернутись, наприклад, до лінійної алгебри для аналізу криптостійкості хеш-функції. Виявляється, що для всіх згаданих криптозадач необхідно вибирати примітивні поліноми. Саме такі поліноми дають можливість синтезувати на базі ЛПС генератори псевдовипадкових чисел максимальної довжини [6].

Апаратною реалізацією ЛПС є загальновідомий регістр зсуву з лінійними оберненими зв'язками (РЗЛОЗ). Перевагою РЗЛОЗ є велика швидкість обробки інформаційних повідомлень. З іншого боку, потоковий шифр тільки на основі РЗЛОЗ вважається криптографічно слабким і тому до нього додається схема, яка реалізує нелінійну функцію [7].

На практиці не завжди можливо або доцільно утримувати в секреті апаратну структуру РЗЛОЗ. Можна значно підвищити криптозахист зашифрованого тексту навіть при відомій апаратній структурі РЗЛОЗ, якщо використовувати початковий стан ЛПС $S(0)$ як секретний ключ. Саме знаходження $S(0)$ і є головною метою числених криптоатак.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Асосков А. В., Иванов М. А., Мирский А. А., Рузин А. В., Сланин А. В., Тютвин А. Н. Поточные шифры. – М.: КУДИЦ-ОБРАЗ, 2003. – 336 с.
2. Ємець В., Мельник А., Попович Р. Сучасна криптографія. – Львів: БаК, 2003. – 144 с.
3. Гийо Ф.Криптология: искусство секретных кодов, EDP Sciences, 196 с.
4. habr.com/ru/post/145648.
5. Семеренко В. П. Реконструкция линейных скремблеров на основе автоматных моделей: – Системи обробки інформації, 2016, вип. 4(141) – С. 72–76.
6. Гилл А. Линейные последовательностные машины: Пер. с англ. – М.: Наука, 1974. – 288 с.
7. Семеренко В. П. Теорія циклічних кодів на основі автоматних моделей : монографія. Вінниця : ВНТУ, 2015. – 444 с.



***Василь Петрович Семеренко*** – канд. техн. наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця,e-mail: vasilsemerenko@gmail.com

***Богдан Олександрович Бабейко*** – студент групи 2КІ-18б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: bogdan.babeyko@gmail.com

***Vasyl P. Semerenko*** – PhD, Associate Professor, Department of computer technique, Vinnytsia National Technical University, Vinnytsia, e-mail: vasilsemerenko@gmail.com

***Bogdan Babeyko*** – student, Department of computer technique, Vinnytsia National Technical University Vinnytsia, e-mail: bogdan.babeyko@gmail.com