УДК 003.26:004.056+512.548

Г.В. Крайнічук[1]
І. Ю. Пилявець[2]
Є. В. Радченко[3]

ОГЛЯД МЕТОДІВ ШИФРУВАННЯ ЗА ДОПОМОГОЮ КВАЗІГРУПОВИХ ОПЕРАЦІЙ

[1] Вінницький національний технічний університет

Анотація

Розглянуто та проаналізовано відомі методи шифрування, що використовують квазігрупові операції, за характеристиками переваг та недоліків.

Ключові слова: квазігрупа, парастроф, латинський квадрат, шифр, алгоритм, метод.

Abstract

Considered and analyzed known encryption methods using quasi-group operations, according to the characteristics of advantages and disadvantages.

Keywords: quasigroup, parastrophe, latin square, cipher, algorithm, method.

Вступ

Шифрування є однією з найважливіших технологій для збереження конфіденційності та захисту інформації від несанкціонованого доступу. У наш час існує багато різних методів шифрування, включаючи симетричні та асиметричні шифри, блочні та потокові шифри, шифри з відкритим ключем та інші. Однак, з'явилися нові інструменти для створення захисту сучасних технологій. Одним із таких інструментів є квазігрупові операції, що можуть бути використані для шифрування інформації. Метою дослідження є огляд та синтез відомих методів шифрування, що побудовані на основі квазігрупових операцій та їх комбінаторних властивостей.

Результати дослідження

Симетричні та асиметричні шифри – це два основні типи шифрів. У симетричних шифрах використовується той самий ключ для шифрування та дешифрування повідомлень. Асиметричні шифри потребують два ключі: публічний та приватний. Публічний ключ використовується для шифрування повідомлень, а приватний ключ використовується для дешифрування [1].

Симетричні шифри мають поділ на блочні та потокові шифри. У блочних шифрах повідомлення ділиться на блоки, кожен з яких зашифровується окремо. У потокових шифрах повідомлення шифрується по одному біту або байту за один раз.

Шифри з відкритим ключем використовуються для обміну ключами між віддаленими комп'ютерами та забезпечення безпеки в інтернет-переговорах по електронній пошті. Ці шифри використовують два ключі: публічний та секретний. Крім цього, у таких шифрах використовують математичні функції для шифрування повідомлень.

Сучасні методи шифрування, такі як симетричні та асиметричні шифри, блочні та потокові шифри, шифри з відкритим ключем, мають свої переваги та недоліки. Наприклад, симетричні шифри є дуже швидкими та ефективними для шифрування великих повідомлень, але потребують обміну ключами між віддаленими комп'ютерами. Асиметричні шифри можуть бути використані для обміну ключами без безпеки та забезпечують більш високий рівень безпеки, але вони повільніші та менш ефективні для шифрування великих повідомлень [1].

З появою криптограм з відкритим ключем і схем цифрового підпису, зросла увага до шифрування за допомогою хеш-функцій, зокрема на основі квазігрупових операцій.

Квазігрупою називається групоїд $(Q;\cdot)$ (з визначеною операцією $(\cdot)$, яка взагалі кажучи неасоціативна і некомутативна), такий, що для будь-яких елементів a, b з множини Q кожне з рівнянь $x \cdot a = b$ і $a \cdot y = b$ має єдиний розв’язок [2]. Порядком квазігрупи є кількість її елементів. Кожній квазігрупі відповідає латинський квадрат: внутрішня таблиця Келі квазігрупи порядку n є латинським квадратом порядку n і навпаки [3].

Саме ці математичні об’єкти використані для створення нових методів шифрування, що базуються на комбінаторних властивостях квазігруп і латинських квадратів у дисертації [4], де описані квазігрупові шифри на основі простих квазігрупових перетворень. Метод шифрування, який використовує квазігрупи - це квазігруповий шифр, у ньому повідомлення розбивається на блоки,

кожен з яких шифрується окремо за допомогою квазігрупових перетворень, що залежить від ключа шифрування. Перетворення квазігруп дозволяє виконувати шифрування та дешифрування повідомлень за допомогою тих самих операцій або ж оборотних операцій до даних. Такими операціями є парастрофи – обернені квазігрупові операції. Це робить квазігруповий шифр більш ефективним відносно інших методів шифрування.

Криптографічні методи побудовані на квазігрупах, в основі мають алгебричну структуру квазігрупових операцій для шифрування повідомлень. Наприклад, серед сімейства потокових шифрів для апаратного забезпечення відомий квазігруповий шифр Edon80. Це апаратний бінарний адитивний синхронний потоковий шифр, в якого внутрішня структура висококонвеєрна, має розпаралелювання процесів, що робить його масштабованим з точки зору швидкості обробки. З принципами його розробки та повним описом з останніми оновленнями можна ознайомитися в [5].

Квазігрупи можуть бути використані для створення криптографічних протоколів, які мають деякі переваги над табличними методами шифрування. Основна перевага полягає в тому, що квазігрупи можуть забезпечити більшу стійкість до атак, таких як атака методом перебору, оскільки квазігрупи мають більше оборотних операцій, ніж звичайні таблиці замін [2, 4].

Крім того, квазігрупи також можуть бути використані для побудови електронних підписів та інших криптографічних протоколів. Наприклад, квазігрупові електронні підписи можуть бути більш стійкими до атак на основі квазігрупових алгебричних структур, ніж звичайні RSA електронні підписи [6].

Висновки

Отже, використання квазігруп для криптографії може забезпечити більшу стійкість до атак і можливості для розширення криптографічних протоколів. Однак, розробка криптографічних алгоритмів на основі квазігруп великих порядків потребує значних обчислювальних ресурсів, що може збільшити витрати на розробку апаратних засобів для впровадження таких алгоритмів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. T. Vitalii, B. Anna, H. Kateryna and D. Hrebeniuk, "Method of Building Dynamic Multi-Hop VPN Chains for Ensuring Security of Terminal Access Systems," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 613- 618, doi: 10.1109/PICST51311.2020.9467953.

2. Denes J. Latin Squares and their Applications / J. Denes, Keedwell A. – Akademiai Kiado, Budapest; Academic Press, New York, 1974. – 547 p.

3. McKay B. D. and Wanless I. M. On the number of Latin Squares // Ann. Combin. − 2005. − No. 9. − P. 335-344.

4. Mileva A. Cryptographic Primitives with Quasigroup Transformations / Dissertation Phd, − 2009. − P.139.

5. Gligoroski D., Markovski S., Knapskog S. J. The Stream Cipher Edon80. Lecture Notes in Computer Science. Berlin, Heidelberg. P. 152–169.

6. Nager D., Niu J. Xifrat - compact public-key cryptosystems based on quasigroups. // 2010, С. 13.

Шелепало Галина Василівна — к. фіз.-мат. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна.

Shelepalo Halyna V. — PhD (Eng), Associated Professor of Data Protection Department in Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine.

Пилявець Ігор Юрійович — студент групи 1БС-19Б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: igormorozov920@gmail.com.

Pyliavets Ihor Y.— student of group 1BS-19B, faculty of information technologies and computer engineering, Vinnytsia National Technical University, email: igormorozov920@gmail.com.

Радченко Євгеній Валентинович — студент групи 1БС-19Б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: jenya.radchenko@gmail.com.

Radchenko Yevhenii V.— student of group 1BS-19B, faculty of information technologies and computer engineering, Vinnytsia National Technical University, email: jenya.radchenko@gmail.com.