УДК 004.056.5

В. А. Лужецький
Д. Б. Рогачевський
В. А. Козира

МЕТОД ЗАХИЩЕНОГО ПЕРЕДАВАННЯ ІНФОРМАЦІЇ

Вінницький національний технічний університет

Анотація

Представлено метод захищеного передавання інформації, який передбачає використання автентифікованого шифрування. Запропонований підхід поєднує переваги блокового перетворення та шифрування гамуванням, а формування секретного ключа здійснюється через багаторівневе ущільнення результатів протоколу Діффі-Геллмана. Особливістю рішення є застосування ортогональної поворотної матриці, сформованої з нормованого кватерніона, що забезпечує сильну дифузію для початкового блоку даних. Частина з гамуванням алгоритму реалізує генерування гами з високим лавинним ефектом та інтегроване формування MAC-коду для підтвердження автентичності повідомлень. Розроблений метод забезпечує уніфікацію процесів узгодження ключа, шифрування та перевірки автентичності, що дозволяє формувати захищений канал передавання інформації між двома сторонами.

Ключові слова: криптографія, автентифікація, шифрування, кватерніон, поворотна матриця, шифрування гамуванням, MAC-код, протокол Діффі-Геллмана.

Abstract

A method of secure information transmission is presented, which involves the use of authenticated encryption. The proposed approach combines the advantages of block transformation and encryption with hashing, and the secret key is generated through multi-level compression of the Diffie-Hellman protocol results. A distinctive feature of the solution is the use of an orthogonal rotation matrix formed from a normalised quaternion, which provides strong diffusion for the initial data block. The gammification part of the algorithm implements the generation of a gamma with a high avalanche effect and integrated MAC code formation to confirm the authenticity of messages. The developed method unifies the processes of key agreement, encryption, and authentication, allowing the formation of a secure channel for information transfer between two parties.

Keywords: cryptography, authentication, encryption, quaternion, rotation matrix, hamming encryption, MAC code, Diffie-Hellman protocol.

Вступ

Захищений обмін інформацією є основним завданням сучасних криптографічних систем, що функціонують у середовищі з недовіреним каналом зв’язку. Відомі підходи передбачають окреме використання протоколів узгодження ключів, алгоритмів шифрування та механізмів автентифікації повідомлень, що ускладнює загальну архітектуру та знижує ефективність реалізації. Відповіддю на ці проблеми є інтегровані методи, що об’єднують ці функціональні складові в єдину схему.

У розробленому методі для формування сеансового секрету використовується протокол Діффі-Геллмана, а наступні етапи побудовані на математичній обробці отриманого числа шляхом ущільнення його до 64 біт. Подальше перетворення секрету у нормований кватерніон дозволяє сформувати ортогональну поворотну матрицю, що використовується для блокового перетворення першої частини повідомлення. Решта даних шифрується потоково, із формуванням гами та MAC у єдиному процесі. Таким чином забезпечується повний цикл захищеної передачі – від узгодження ключа до підтвердження автентичності.

Результати дослідження

Розроблений метод захищеного передавання інформації базується на комплексному поєднанні механізмів узгодження ключа, блокового ортогонального перетворення та шифрування гамуванням з інтегрованим контролем автентичності [1]. В основі системи лежить протокол встановлення спільного секретного параметра між двома сторонами шляхом обчислення однакового значення без його передачі

каналом зв'язку. Для цього використовується алгоритм Діффі-Геллмана, який доповнено процедурою автентифікації користувачів, що забезпечує незалежне автентифіковане формування секрету у кожного учасника. Якщо сторони мають відкриті параметри p та g, то спільний секрет обчислюється як: $K = g^{A,B} \; mod \; p$ [2].

Отримане значення є надмірним для безпосереднього застосування у вигляді робочого сеансового ключа, оскільки має довжину 1024 біти та не оптимізоване для подальшого шифрування. Тому з метою формування компактного, але водночас стійкого представлення секрет перетворюється у 64-бітне значення шляхом багатоступеневої ущільнювальної процедури, що базується на кватерніонних множеннях. Такий підхід забезпечує повне змішування вхідних бітів та задає істотно нелінійний характер перетворення, який унеможливлює лінійну декомпозицію або аналітичне відновлення початкових компонент з кінцевого значення.

З отриманого 64-бітного значення формується кватерніон, який нормується для забезпечення одиничного значення його норми. Далі, на основі цього нормованого кватерніона формується ортогональна поворотна матриця $\mathbf{\Gamma}(\hat{q})$, яка є секретним ключем, що використовується для шифрування першого блоку повідомлення. Застосування матричного обертання дозволяє реалізувати сильну початкову дифузію першого блоку повідомлення, забезпечуючи рівномірний розподіл впливу кожного біта ключа на результат шифрування. Перше перетворення описується співвідношенням: $\mathbf{C}_0 = (\mathbf{\Gamma}(\hat{q}) \cdot \mathbf{M}_0) \; mod \; 65537$ [1, 3]. Схему, що відображає дії, виконувані під час зашифрування, наведено на рис. 1.

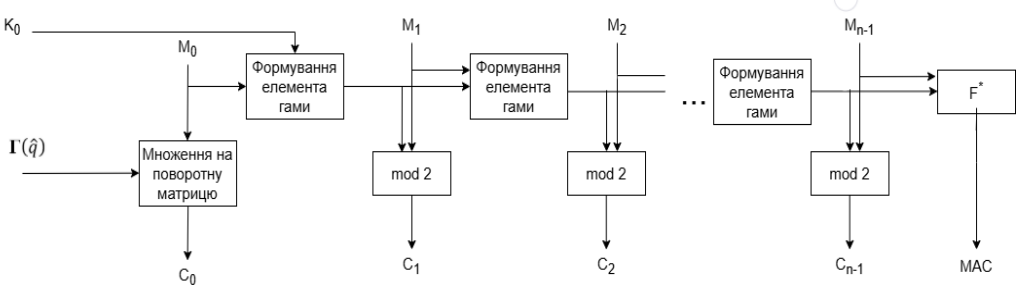

Рисунок 1 – Схема процесу зашифрування

Оскільки матриця $\mathbf{\Gamma}(\hat{q})$ є ортогональною, вона задовольняє умову: $\mathbf{\Gamma}(\hat{q})^{\mathrm{T}}\mathbf{\Gamma}(\hat{q}) \equiv I \; (mod \; p)$, а це означає, що для розшифрування достатньо використати транспоновану матрицю, яка повертає первинний блок повідомлення без накопичення похибок та без необхідності виконання окремих процедур інверсії. Таким чином, відновлення першого блоку здійснюється як: $\mathbf{M}_0 = (\; \mathbf{\Gamma}^{\mathrm{T}}(\hat{q}) \cdot \mathbf{C}_0) \; mod \; 65537$ [1].

Наступні блоки повідомлення шифруються шляхом гамування. У цьому режимі кожен наступний елемент гами залежить від попереднього та від попереднього блоку повідомлення, що дозволяє встановити ланцюгову залежність та забезпечити каскадне поширення змін по всій довжині шифротексту. Формування гами описується співвідношенням: $g_i = f_{64}(M_{i-1}, g_{i-1}) = ((M_{i-1} \cdot g_{i-1})_L + (M_{i-1} \cdot g_{i-1})_R) \; mod \; 2^{64}$.

Для зашифрованого повідомлення на кожен поточний відкритий блок накладається гама операцією XOR, що задає просту і симетричну модель обчислень, яка водночас забезпечує високий рівень стійкості завдяки властивостям функції генерування. Формування шифротексту виконується за формулою: $C_i = M_i \oplus g_{i-1}$. Процес зашифрування завершується формуванням коду автентифікації повідомлення (MAC) [1].

При отриманні повідомлення приймаюча сторона, маючи спільний ключ K_0, відтворює ту саму послідовність гами та виконує обчислення MAC-коду. Якщо отримане значення збігається з переданим, повідомлення вважається автентичним.

Таким чином, процес накладання гами поєднує у собі функції шифрування гамуванням та формування коду автентифікації повідомлення.

Процес розшифрування є оберненим до процесу зашифрування і виконується за аналогічними етапами, але в зворотному порядку. Метою розшифрування є відновлення вихідного повідомлення з шифротексту та перевірка його автентичності за допомогою MAC-коду.

На рис. 2 наведено схему процесу розшифрування, що відображає порядок виконання дій.

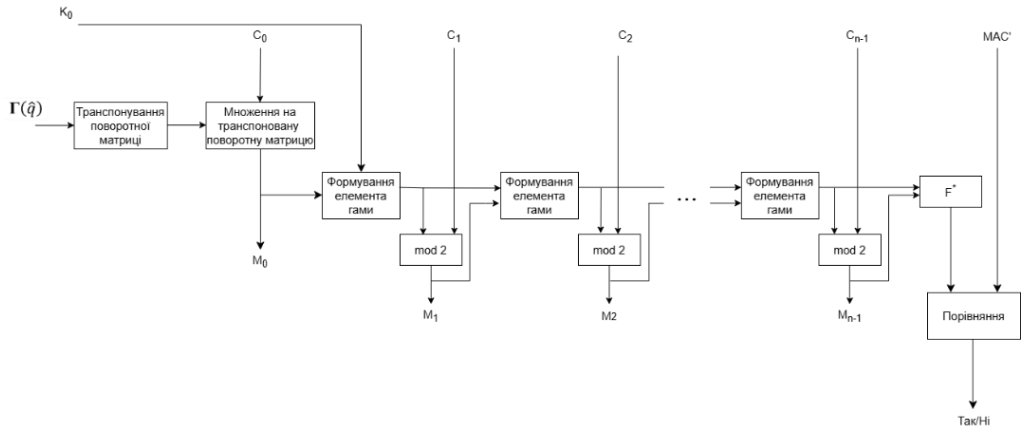

Рисунок 2 – Схема процесу зашифрування

Отримане значення MAC' порівнюється з переданим MAC-кодом. Якщо значення збігаються, повідомлення вважається автентичним (Так). У випадку якщо MAC-коди не збігаються, робиться висновок про наявність змін в зашифрованому повідомленні (Ні).

Поєднання множення на ортогональну поворотну матрицю та шифрування гамуванням під час розшифрування забезпечує не лише відновлення даних, але й перевірку їхньої автентичності.

Висновки

Розроблений метод забезпечує інтегрований підхід до захищеного передавання інформації, у якому вся криптографічна логіка – від формування сеансового ключа до перевірки автентичності – реалізована як єдиний математично узгоджений процес. Поєднання матричного шифрування та шифрування гамуванням, нормованих кватерніонів та принципу лавинного ефекту дозволило досягти високої стійкості при збереженні ефективності. Запропоноване рішення може бути інтегроване у реальні комунікаційні програмні системи та використане як основа для побудови сучасного криптографічного протоколу захищеного обміну повідомленнями.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Dzwonkowski M., Rykaczewski R. Quaternion Encryption Method for Image and Video Transmission // *Article*. – Gdańsk: Gdańsk University of Technology, Department of Teleinformation Networks; Medical University of Gdańsk, Department of Informatics and Statistics, 2013. – Режим доступу до ресурсу: https://www.researchgate.net/publication/261366448.

2. Diffie-Hellman Key Exchange Algorithm [Електронний ресурс]. – Режим доступу до ресурсу: https://www.1kosmos.com/security-glossary/diffie-hellman-key-exchange-algorithm/.

3. Rotation Matrix [Електронний ресурс]. – Режим доступу до ресурсу: https://www.geeksforgeeks.org/maths/rotation-matrix/

Лужецький Володимир Андрійович – зав. кафедри ЗІ, д. т. н., проф., факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: lva.kzi2002@gmail.com

Рогачевський Дмитро Богданович – студент групи 1БС-24м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: dimonrogach@gmail.com

Козира Володимир Андрійович – студент групи 1БС-24м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vovakozira@gmail.com

Luzhetsky Volodymyr A. – Head of the Department of Information Systems, Doctor of Technical Sciences, Professor, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: lva.kzi2002@gmail.com

Rohachevskyi Dmytro B. – student of group 1BS-24m, Faculty of Information Technologies and Computer Engineering,Vinnytsia National Technical University, Vinnytsia, e-mail: dimonrogach@gmail.com

KozyraVolodymyr A. – student of group 1BS-24m, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vovakozira@gmail.com