ОРГАНІЗАЦІЯ ЗЧЕПЛЕННЯ БЛОКІВ ДЛЯ ШИФРІВ НА ОСНОВІ АРИФМЕТИЧНИХ ОПЕРАЦІЙ ЗА МОДУЛЕМ

Володимир Лужецький[1], Олександр Дмитришин[2]

Вінницький національний технічний університет,
вул. Хмельницьке шосе, 95, Вінниця, 21021, Україна,
[1]тел.: +380-432-598-386, [2]тел.: +380–682–091–397, E-mail: oleksander.dmytryshyn@gmail.com

Анотація

В ході проведених досліджень, було проаналізовано структуру роботи блокових симетричних шифрів в режимі зчеплення блоків шифра. Виділено основні етапи роботи симетричних блокових шифрів в режимі зчеплення блоків шифра.

На підставі проведеного аналізу, розроблено керовані процедури формування блоків зчеплення, а саме просту, ускладнену та комбіновані процедури. Для можливих варіантів зчеплення блоків даних спроектовані керовані функції зчеплення блоків даних з реакцією на 1 та 0 з урахуванням отриманих процедур формування блоків зчеплення.

В якості формування керуючих векторів, для керованих елементів, використовуються проста та складна функції парності, які на виході видаються значення 0 або 1 для відповідного вхідного елемента даних.

Отримано три узагальненених математичних моделей блокових шифрів в режимах попереднього, фіксуючого та комбінованого зчеплення. Для кожної із моделей описуються етапи зчеплення та шифрування, а саме: етап ініціалізації шифру, виконання процедур формування та зчеплення блоків.

Вступ

Блокові шифри на основі арифметичних операцій за модулем, такі як блокові шифри, що запропоновані в роботі [1], Nimbus [2] та БСШ [3], які працюють в режимі електронної кодової книги, мають такі нелодіки: однаковим значенням вхідних блоків даних, відповідають однакові значення вихідних блоків шифротексту; видалення або заміна одного із блоків шифротексту не впливає на інші блоки шифротексту, що дозволяє порушувати цілісність зашифрованого повідомлення. В блокових шифрах RC6, MRC6 та Rijndael [4] за рахунок використання режиму зчеплення блоків шифра, який пов'язує кожний наступний блок шифротексту з поперднім блоком шифротекста або блоком вхідних даних, проблеми, які виникають в режимі електронно кодової книги – відсутні.

Мета досліджень

Аналіз структури роботи блокових симетричних шифрів в режимі зчеплення блоків шифра(Ciphertext Block Chaining (CBC) та отримання узагальненених математичних моделей блокових шифрів в режимі CBC.

Постановка задачі

Класична ідея шифрування, в режимі CBC, полягає у виконанні такого правила [5]: інформаційне повідомлення X = {x_1, x_2, …, x_p} розбивається на p блоків фіксованої довжини, кожен наступний n-розрядний блок відкритого повідомлення x_l ($l = \overline{1 \div p}$) попередньо зчіплюється з попереднім зашифрованим блоком c_l-1 на секретному підключі k_l, тобто $c_l = E_{k_l}\left(x_l \oplus c_{l-1}\right)$.

Процес шифрування в режимі CBC ділиться на три етапи: обрання попердніх блоків для зчеплення, зчеплення блоку відритого повідомлення (шифротекста) і на заключному виконується шифрування.

Задачею дослідження є аналіз варіантів процедур формування блоків зчеплення, в залежності від вмісту блоків, розроблення функцій зчеплення для запропонованих процедур формування блоків зчеплення та математичних моделей блокових шифрів в режимі CBC.

Процедури формування блоків зчеплення

Визначення 1. Для вхідного вектора даних S = {s_1, s_2, …, s_t} та керуючого вектора V = {v_1, v_2, …, v_t}, $s_i \in GF(2)^n$, $v_i \in GF(2)$, $i = \overline{1 \div t}$, t ∈ N, функція $f_V(S)$ називається простою процедурою формування блоків зчеплення, яка формує вектор вихідних даних W = {v_1s_1, v_2s_2, …, v_ts_t}, $w_i \in GF(2)^n$.

В якості вхідного вектора даних S, в простій процедурі формування блоків зчеплення, використовується або інформаційні блоки даних X = {x_1, x_2, …, x_p}, або блоки шифротексту C = {c_1, c_2, …, c_p}, режим обрання яких задає керуючий параметр d_1, $d_1 \in GF(2)$. Якщо d_1 = 0, то в якості вхідного вектора S використовується множина інформаційних даних X, в протилежному випадку множина шифротекстів C.

Визначення 2. Для вхідного вектора даних S = {s_1, s_1', s_2, s_2', …, $s_{t/2}$, $s_{t/2}'$} і керуючого вектора V={v_1, v_2, …, v_t}, s_i, $s_i' \in GF(2)^n$, $v_j \in GF(2)$, $i = \overline{1 \div t/2}$, $j = \overline{1 \div t}$, $t = 2^q$, q ∈ N, функція $f_V(S,S')$ називається ускладненою процедурою формування блоків зчеплення, яка формує вектор вихідних даних

W={$v_1\ s_1$, $v_2\ s_1'$, $v_3\ s_2$, $v_4\ s_2'$, …, $v_{t-1}\ s_{t/2}$, $v_t\ s_{t/2}'$}, $w_j \in GF(2)^n$.

Елементами вхідного вектора даних S для значень s_i є інформаційні блоки даних X = {x_1, x_2, …, x_p}, а для значень s'_i – блоки шифротексту C = {c_1, c_2, …, c_p}.

Визначення 3. Для вектора функції P = {$f_V(S)$, $f_V(S, S')$} та керуючого параметра d_2, функція F_{d_2} (P), $d_2 \in GF(2)$ називається комбінованою процедурою формування блоків зчеплення, в якій при $d_2 = 0$ використовується проста процедура формування блоків $f_V(S)$, а при $d_2 = 1$ – складна процедура формування блоків $f_V(S, S')$.

Функція зчеплення блоків

Визначення 4. Для вхідного вектора даних W = {w_1, w_2, …, w_t} та керуючого вектора V={v_1, v_2, …, v_t}, $w_i \in GF(2)n$ ($w_i \neq 0$), $v_i \in GF(2)$, $i = \overline{1 \div t}$, і керуючого параметра d_3, функція Z_{d_3}(W) називається функцією зчеплення блоків даних з реакцією на 1, якщо в процедурах формування блоків зчеплення wi використовуються прямі значення v_i або функцією зчеплення блоків даних з реакцією на 0, якщо в процедурах формування блоків зчеплення wi використовуються інверсні значення $\overline{v_i}$, яка знаходиться таким чином, якщо $d_3 = 0$, то

$$Z_{d_3}(W) = \sum_1^t w_i \bmod 2,$$

якщо $d_3 = 1$, то

$$Z_{d_3}(W) = \sum_1^t w_i \bmod 2^n.$$

Математичні моделі блокових шифрів для режиму CBC

Визначення 5. Функція $\psi(s_l)$, $s_l = \{q_1, q_2, \ldots, q_n\}$, $s_l \in GF(2)^n$, $q_i \in GF(2)$, $i = \overline{1 \div n}$ називається простою функцією парності, якщо вона приймає значення 1 в тому випадку, коли число елементів q_i містить парну кількість 1 та значення 0, в протилежному випадку.

Визначення 6. Функція ψ(H), де вектор H = {q_1, q_2, …, q_n}, $q_i \in GF(2)$, $i = \overline{1 \div n}$, знаходиться за допомогою функції $\gamma_{d_4}(S, K)$, вхідні значення якої є результатом виконання функції γ над значеннями S та K, де S, K $\in GF(2)^n$, називається складною функцією парності, якщо вона приймає значення 1, в тому випадку, коли число елементів qi містить парну кількість 1 та значення 0, в протилежному випадку, а фунція $\gamma_{d_4}(S, K)$ визначається керуючим оператором d_4. Якщо $d_4 = 0$, то

$$H = \gamma_{d_4}(S, K) = S \oplus K,$$

якщо $d_4 = 1$, то

$$H = \gamma_{d_4}(S, K) = (S + K) \bmod 2^n.$$

Визначення 7. Для вхідного блоку даних $H \in GF(2)^n$, керуючий параметр $d_i \in GF(2)$, $i = \overline{1 \div 4}$, задається простою функцією парності $d_i = \psi(H)$.

Модель 1. Узагальнена модель шифрування в режимі попереднього зчеплення.

Виконується етап ініціалізіції, на якому задаються основні керуючі параметри d_1, …, d_4, проходить початкове розгортання секретного ключа, задається порядок формування вектора даних S та обирається процедура зчеплення блоків, в залежності від параметрів d_1 та d_2 відповідно.

Для заданого вектора підключів K та вектора даних S, формується керуючий параметр d_4 та вектор V .

Виконується процедура формування блоків зчеплення, отримується вектор даних W, який зчеплюється та отримується блок даних Z_{d_3}(W).

До інформаційного блоку даних x_l, $l = \overline{1 \div p}$ додається отримане значення Z_{d_3}(W).

Виконується безпосередньо зашифрування зчепленого блоку даних із одночасним розгортанням підключів зашифрування.

В векторах S, V і K виконується зсув всіх елементів на одну позицію вліво та запис нового елемента даних для кожного із векторів, в кінець кожного із векторів.

Дії 2-6 виконуються доти, поки в результаті не отримається множина шифротексту C = {c_1, c_2, …, c_n}.

Розшифрування виконується аналогічним чином, з тією різницею, що після виконання розшифрування, розпочинається процес розчеплення розшифрованого блоку даних.

Модель 2. Узагальнена модель шифрування в режимі фіксуючого зчеплення.

Процес зашифрування, в режимі фіксуючого зчеплення, проходить аналогічно процесу зашифруванню, в режимі попереднього зчеплення, але спочатку виконується зашифрування блоку даних, а потім для заданого параметра d3 виконується функція зчеплення блоків даних.

Перед розшифруванням блока повідомлення, виконується процес розчеплення блока шифротексту, який потім розшифровується.

Модель 3. Узагальнена модель шифрування в режимі комбінованого зчеплення.

На етапі ініціалізіції, задаються основні керуючі параметри d_1, …, d_4, проходить початкове розгортання секретного ключа, задається порядок формування вектора даних S обирається процедура зчеплення блоків в залежності від параметрів d_1 та d_2.

Для заданоого вектора підключів K та множини даних S, формується керуючий параметр d_4 та пари векторів V_1 та V_2.

Виконується процедура формування блоків зчеплення, отримуються вектори даних W_1 та W_2, які зчеплюються за допомогою функції зчеплення блоків та отримуються блоки даних Z_{d_3} (W_1) та Z_{d_3} (W2).

До інформаційного блоку даних x_l, $l = \overline{1 \div p}$ додається отримане значення Z_{d_3} (W_1).

Виконується безпосередньо зашифрування зчепленого блоку даних із одночасним розгортанням підключів зашифрування.

До блоку шифротекста c_l, $l = \overline{1 \div p}$ додається отримане значення Z_{d_3} (W_2).

В векторах S, V_1, V_2 і K виконується зсув всіх елементів на одну позицію вліво та запис нового елемента даних для кожного із векторів, в кінець кожного із векторів.

Дії 2-8 виконують доти, поки в результаті не отримається множина шифротексту C .

Розшифрування проходить в тій же послідовності, що й зашифирування з тією різницею, що під час розшифрування одночасно із зашифруванням розгортаються підключі зашифрування та(або) розшифрування і проходить розчеплення блоків на початку розшифрування та після.

Висновки

В ході проведених досліджень, було проаналізовано структуру роботи блокових симетричних шифрів в режимі зчеплення блоків шифра. Виділено основні етапи роботи симетричних блокових шифрів в CBC. На підставі проведеного аналізу, розроблено керовані процедури формування блоків зчеплення, а саме просту, ускладнену та комбіновані процедури.

В якості формування керуючих векторів, для керованих елементів, використовуються проста та складна функції парності, які на виході видаються значення 0 або 1 для відповідного вхідного елемента даних. Подальшим вектором наукових досліджень є розроблення алгоритмів шифрування, проведення їхнього криптографічного аналізу.

Література:

[1] Блоковий щифр на основі арифметичних операцій за модулем: матеріали міжнар. наук.-практ. конф., Вінниця, Україна, 15–17 травня 2007 р.: тези доповідей / [відпов. ред.: В.А. Лужецький]. – В.: ВНТУ, 2007. – 140 с. – С. 69-70.

[2] Machado, A.W. The nimbus cipher. A proporsal for NESSIE: [Электрон. ресурс]. – Режим доступа: http://www.cosic.esat.kuleuven.be/nessie/workshop.

[3] Сокирук, В. В. Побудова статистично безпечного БСШ на основі арифметичних операцій за модулем / В. В. Сокирук, В. А. Лужецький // Інформаційні технології та комп'ютерна інженерія. – 2006. – №1. – С. 158–163.

[4] El-Fishawy, Nawal Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms / Nawal El-Fishawy, Osama M. Abu Zaid Quality // International Journal of Network Security. – 2007. –Vol. 5. – No. 3. – PP. 241–251

[5] Рябко Б.Я. Криптографические методы защиты инофрмации: учебн. пособие для вузов / Б. Я. Рябко, А. Н. Фионов. – М.: Горячая линия-Телеком, 2005. – 229 с.: ил.