ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КОМП'ЮТЕРНА ТЕХНІКА

УДК 004.056.55

О. В. Дмитришин, асп.;
В. А. Лужецький, д. т. н., проф.

РЕЖИМ КЕРОВАНОГО ЗЧЕПЛЕННЯ БЛОКІВ ЗАШИФРОВАНОГО ТЕКСТУ

В контексті дослідження структури роботи блокових симетричних шифрів запропоновано модель керованого режиму зчеплення блоків зашифрованого тексту. Виділено основні етапи роботи симетричних блокових шифрів в режимі зчеплення блоків зашифрованого тексту, на підставі якого отримано режим симетричного блокового шифрування, що виконує одночасне шифрування в режимі керованого CBC та режимі ECB.

Вступ

Більшість сучасних блокових симетричних шифрів підтримують п'ять режимів обробки даних [1], а саме:

— режим електронної кодової книги (The Electronic Codebook Mode (ECB);
— режим зчеплення блоків зашифрованого тексту (The Cipher Block Chaining Mode (CBC);
— режим зворотного зв'язку за зашифрованим текстом (The Cipher Feedback Mode);
— режим зворотного зв'язку за виходом (The Output Feedback Mode);
— режим лічильника (The Counter Mode).

Блокові шифри на основі арифметичних операцій за модулем, такі як блокові шифри, що запропоновані в роботі [2], Nimbus [3] та БСШ [4], які працюють в режимі електронної кодової книги, мають нелодіки, які характерні для даного режиму [1]. В блокових шифрах RC6, MRC6 та Rijndael [5] за рахунок використання режиму зчеплення блоків шифру, який пов'язує кожний наступний блок шифротекста з попереднім блоком шифротекста або блоком вхідних даних, проблеми, які виникають в режимі ECB — відсутні.

Метою роботи є аналіз структури роботи блокових симетричних шифрів в режимі CBC та підвищення ефективності шифрування за рахунок одночасного використання режиму керованого CBC та режиму ECB.

Режим зчеплення блоків зашифрованого тексту

Класична ідея шифрування, в режимі CBC, полягає у виконанні такого правила [6]: інформаційне повідомлення $X = \{x_1, x_2, \ldots, x_p\}$ розбивається на p блоків фіксованої довжини, кожен наступний n-розрядний блок відкритого повідомлення $x_l \left(l = \overline{1 \div p}\right)$ зчіплюється з попереднім зашифрованим блоком c_{l-1} на секретному підключи k_l, тобто $c_l = E_{k_l}\left(x_l \oplus c_{l-1}\right)$.

В роботі [7], розроблено процедури формування блоків зчеплення, в залежності від вмісту блоків, на підставі якого створено функції зчеплення для запропонованих процедур формування блоків зчеплення та математичні моделі блокових шифрів в режимі керованого CBC.

Процедури формування блоків зчеплення

Оскільки зчеплення блоків даних виконується як на попередніх блоках зашифрованого тексту, так і на попередніх блоках відкритого тексту, тому використовуються такі процедури формування блоків зчеплення [7].

Визначення 1. Для вхідного вектора даних $S = \{s_1, s_2, \ldots, s_t\}$ та керувального вектора $V = \{v_1, v_2, \ldots, v_t\}$, $s_i \in \mathrm{GF}(2)^n$, $v_i \in \mathrm{GF}(2)$, $i = \overline{1 \div t}$, $t \in \mathrm{N}$, функція $f_1(S)$ називається *простою процедурою формування блоків зчеплення*, яка формує вектор вихідних даних $W = \{v_1 s_1, v_2 s_2, \ldots, v_t s_t\}$, $w_i \in \mathrm{GF}(2)^n$.

Визначення 2. Для вхідного вектора даних $S = \{s_1, s'_1, s_2, s'_2, \ldots, s_{t/2}, s'_{t/2}\}$ і керувального вектора $V = \{v_1, v_2, \ldots, v_t\}$, $s_i, s'_i \in \mathrm{GF}(2)^n$, $v_j \in \mathrm{GF}(2)$, $i = \overline{1 \div t/2}$, $j = \overline{1 \div t}$, $t = 2^q$, $q \in N$, функція $f_1(S, S')$ називається *ускладненою процедурою формування блоків зчеплення*, яка формує вектор вихідних даних $W = \{v_1 s_1, v_2 s'_1, v_3 s_2, v_4 s'_2, \ldots, v_{t-1} s_{t/2}, v_t s'_{t/2}\}$, $w_j \in \mathrm{GF}(2)^n$.

Визначення 3. Для вектора функції $P = \{f_1(S), f_1(S, S')\}$ та керувального параметра d_2, функція $F_{d_2}(P)$, $d_2 \in \mathrm{GF}(2)$ називається *комбінованою процедурою формування блоків зчеплення*, в якій при $d_2 = 0$ використовується проста процедура формування блоків $f_1(S)$, а при $d_2 = 1$ — складна процедура формування блоків $f_1(S, S')$.

Функція зчеплення блоків та функції перевірки на парність

Наступним етапом шифрування є зчеплення елементів отриманого вектора вихідних даних W за допомогою операції виключного-АБО або операції додавання за модулем 2^n.

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

$$Z_{d_3}(W) = w_1 \oplus w_2 \oplus \ldots \oplus w_t,$$

якщо $d_3 = 1$, то

$$Z_{d_3}(W) = \sum_{i=1}^{t} w_i \bmod 2^n.$$

Для визначення значень керувальних векторів використовується функція перевірки на парність.

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 $\psi(H)$, де вектор $H = \{q_1, q_2, \ldots, q_n\}$, $q_i \in GF(2)$, $i = \overline{1 \div n}$, 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 q_i містить парну кількість 1 та значення 0, в протилежному випадку, а функція $\gamma_{d_4}(S, K)$ визначається керувальним оператором d_4. Якщо $d_4 = 0$, то

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

якщо $d_4 = 1$, то

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

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

Блокові шифри в режимі керованого CBC та режимі ECB

Особливостями режиму ECB є те, що кожен блок даних шифрується, на функції шифрування, незалежно від інших блоків даних, що в свою чергу дозволяє підтримувати можливість розпаралелювання, тобто виконується одночасне шифрування декількох блоків даних. Недоліком використання

режиму ECB є те, що однакові блоки відкритого тексту зумовлюють появу однакових блоків зашифрованого тексту при фіксованому ключі.

До переваг режиму CBC відноситься така властивість даного режиму: однакові блоки відкритого тексту зумовлюють появу різних блоків зашифрованого тексту при фіксованому ключі. Проте, недоліком такого режиму є те, що кожен наступний блок зашифрованого тексту (окрім першого) зашифровується із урахуванням попереднього блока зашифрованого тексту, тому розпаралелення процесу шифрування не можливе.

Поєднання режиму керованого CBC та режиму ECB дозволяє поєднати переваги кожного із режимів за рахунок шифрування групи з t блоків даних та звільнитися від недоліків, які притаманні кожному із режимів.

Висновки

Запропоновано режим керованого CBC, що дозволяє ускладнити процес криптоаналізу за рахунок зчеплення блока даних, що зашифровується з групою попередніх блоків даних, набір якої залежить від самого блока даних, що шифрується? та секретного ключа.

Розглянуто можливість одночасного шифрування в режимі керованого CBC та режимі ECB, що дозволяє розпаралелювати процес шифрування не більше як на t потоків.

СПИСОК ЛІТЕРАТУРИ

1. FIPS PUB 197 Advanced Encryption Standard. — 2001. — 51 p. — Режим доступу до стандарту: http://csrc.nist.gov/publications/PubsTC.html.

2. Лужецький В. А. Блоковий шифр на основі арифметичних операцій за модулем / В. А. Лужецький , О. В. Дмитришин // Методи та засоби кодування, захисту й ущільнення інформації: Міжнар. наук.-практ. конф., 15—17 травня 2007 р.: тези доп. — В.: ВНТУ, 2007. — 140 с. — С. 69—70.

3. Machado A. W. The nimbus cipher: A proporsal for NESSIE (Competition of New European Schemes for Signatures, Integrity, and Encryption) / A. W. Machado. — 2000. — 7 p. — Режим доступу: https://www.cosic.esat.kuleuven.be/nessie/workshop /submissions.html.

4. 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.

5. Nawal El-F. Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms / El-F. Nawal, M. A. Zaid Osama // International Journal of Network Security. — 2007. — Vol. 5. — No .3. — P. 241—251.

6. 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.

7. Організація зчеплення блоків для шифрів на основі арифметичних операцій за модулем : зб. мат. конф., 7—11 жовтня, 2008 р., Вінниця. Т. 2 / відп. ред. В. В. Грабко. — В.: УНІВЕРСУМ–Вінниця, 2008. — С. 396—398.

Рекомендована кафедрою захисту інформації

Надійшла до редакції 8.09.08
Рекомендована до друку 20.10.08

Дмитришин Олександр Васильович — аспірант, ***Лужецький Володимир Андрійович*** — завідувач кафедри.

Кафедра захисту інформації Вінницького національного технічного університету