



УКРАЇНА

(19) UA (11) 42531 (13) A

(51) 7 H04L9/06

МІНІСТЕРСТВО ОСВІТИ  
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІОПИС  
ДО ДЕКЛАРАЦІЙНОГО ПАТЕНТУ  
НА ВИНАХІДвидається під  
відповідальність  
власника  
патенту

(54) СПОСІБ ШИФРУВАННЯ ДАНИХ ДЛЯ СИСТЕМ ОБРОБКИ В ЕОМ

(21) 2001032062

(22) 28 03 2001

(24) 15 10 2001

(33) UA

(46) 15 10 2001, Бюл. № 9, 2001 р

(72) Долгов Віктор Іванович, Лисицька Ірина Вікторівна, Цепуріт Тетяна Володимирівна, Руженцев Віктор Ігорович, Мелецький Олексій Петрович, Пінчук Максим Валентинович

(73) ХАРКІВСЬКИЙ ДЕРЖАВНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ, UA

(57) Спосіб шифрування даних для систем обробки в ЕОМ, який полягає в тому, що послідовність двійкових символів відкритого тексту розбивають на 64-бітні блоки, кожен з яких розбивають на правий і лівий півблоки по 32 біти, які розміщують у відповідних накопичувачах, зашифрування котрих включає 16 циклів, при цьому дані з виходу нако-

пичувача правого півблока і відповідного підключа кожного циклу надходять на вхід циклової функції перетворення, вихідні дані котрої підсумовують у відповідному побітному суматорі за модулем 2 з даними лівого півблока, дані накопичувача правого блока теперішнього циклу переносять у накопичувач лівого півблока, а результатом підсумовування заповнюють накопичувач правого півблока чергового циклу, який відрізняється тим, що додатково задають визначені п'ять бітів з 32 бітів на вході або виході циклової функції, перетворюють їх в відповідне число зсувних імпульсів, за допомогою яких виконують циклічний зсув результату порозрядного підсумовування вихідних даних циклової функції з даними лівого півблока перед тим, як заповнити ім накопичувач правого півблока чергового циклу

Винахід відноситься до галузі обчислювальної техніки, а саме до способів та пристроїв, що використовують реєстри зсуву та накопичуючі пристрої для блочного кодування такі, наприклад, як стандарт шифрування даних DES та інші DES-подібні алгоритми

Відомий спосіб шифрування даних, такий як ГОСТ 28147-89, що використовується у режимах простої заміни, гамування зі зворотним зв'язком та вироблення імтовставки (див. ГОСТ 29147-89 Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования. Введ. 01.01.89 - М. Изд-во стандартов, 1989 - 78 с.)

При цьому способі інформацію розбивають на 64-розрядні блоки  $T_0$ , зашифрування яких включає в себе 32 цикли ( $j=1, 2, \dots, 32$ ). У ключовий запам'ятовуючий пристрій (КЗП) вводять 256 біт ключа  $K$  у вигляді восьми 32-ох розрядних підключів ( $K_0, K_1, \dots, K_7$ ). Кожний блок бітів, наприклад, у режимі простої заміни, розбивають на ліві або старші біти і праві або молодші біти, які вводять, відповідно, у накопичувачі  $N_1$  і  $N_2$ . Біти з виходу накопичувача  $N_1$  разом з 32-розрядним підключем  $K_0$ , зчитаним з КЗП проходять циклове перетворення, в ході якого виконується їх підсумовування за модулем  $2^{32}$  і результат підсумовування подається на блок підстановок. Далі виконують детермінований цикліч-

ний зсув вихідної послідовності бітів за допомогою реєстра зсуву, результат підсумовують за модулем 2 з змістом накопичувача  $N_1$  і записують у накопичувач  $N_2$ , а старе значення  $N_2$  переписують у накопичувач  $N_1$ . Перший цикл завершений. В другому циклі використовують нове значення  $N_2$  із КЗП зчитують заповнення - підключ  $K_1$ , у третьому циклі - підключ  $K_2$  і т. д. Так продовжується 24 цикли. В останніх восьми циклах розглянута процедура повторюється як і раніше, тільки порядок зчитування підключів з КЗП зворотний  $K_7, K_6, \dots, K_0$ .

Найбільш близьким за сукупністю ознак до запропонованого є спосіб шифрування даних, що реалізується американським стандартом і шифрування даних DES (Data Encryption Standard), наприклад, у режимі електронної кодової книги (ECB) (див. Sheier B. Applied Cryptography. Second Edition. protocols, algorithms, and source code in C. Published by John Wiley & Sons Inc, New York, Chichester, Brisbane, Toronto, Singapore, 1996 - 158 p). У цьому режимі послідовність двійкових символів відкритого тексту розбивається на 64-бітні блоки  $M_1, M_2, M_3, \dots, M_n$ , кожен з котрих розбивають на правий та лівий півблоки по 32 біти і розміщують у відповідних накопичувачах. Далі над цими півблоками виконують 16 циклів ідентичних перетворень, які укладаються в тому, що дані з виходу накопичувача правого півблока і відповід-

(19) UA (11) 42531 (13) A

ного циклового підключа кожного циклу поступають на вхід циклової функції перетворення, вихідні дані котрої порозрядно підсумовуються у відповідному суматорі за модулем 2 з даними лівого півблока, далі дані накопичувача правого півблока теперішнього циклу переносять у накопичувач лівого півблока чергового циклу, а результатом підсумовування заповнюють накопичувач правого півблока чергового циклу.

Однак, як свідчить практика, описані шифри сьогодні вважаються вже не достатньо надійними у зв'язку зі знайденими за останні роки атаками диференційного і лінійного криптоаналізу, які опинились менш складними, ніж прямий перебір ключів.

В основу винаходу поставлена задача створення такого способу шифрування даних для систем обробки в ЕОМ, при котрому шляхом введення додаткових операцій досягнути підвищення захищеності шифрів від атак диференційного та лінійного криптоаналізу.

Такий технічний результат може бути досягнутий за способом шифрування даних для систем обробки в ЕОМ, який міститься у тому, що послідовність двійкових символів відкритого тексту розбивають на 64-бітні блоки, кожний з котрих розбивають, у свою чергу, на правий та лівий півблоки по 32 біти, розміщують їх у відповідних накопичувачах, і піддають зашифровуванню, котре включає в себе 16 циклів, при цьому дані з виходу накопичувача правого півблока і відповідного підключа кожного циклу поступають на вхід циклової функції перетворення, вихідні дані котрої порозрядно підсумовують у відповідному суматорі за модулем 2 з даними лівого півблока, дані накопичувача правого півблока теперішнього циклу переносять у накопичувач лівого півблока чергового циклу, а результатом підсумовування заповнюють накопичувач правого півблока чергового циклу, відповідно до винаходу, додатково задають визначені п'ять бітів з 32 бітів на входи або виходи циклової функції, перетворюють їх у відповідне число зсувних імпульсів, за допомогою яких виконують циклічний зсув результату порозрядного підсумовування вихідних даних циклової функції з даними лівого півблока перед тим як заповнити ім накопичувач правого півблока чергового циклу.

Таким чином, додатна операція алгоритму шифрування, а саме визначення п'ятьох бітів із ряду 32-ох бітів на входи чи виходи циклової функції і потім їх перетворення у відповідне число зсувних імпульсів, за допомогою яких виконують циклічний зсув результату порозрядного підсумовування вихідних даних циклової функції з даними лівого півблока перед тим як заповнити ім накопичувач правого півблока чергового циклу, робить переходи,

що виникають між сусідніми циклами, не детермінованими, а випадковими, а це підвищує захищеність модифікованого шифру від атак диференційного та лінійного криптоаналізу.

Запропоноване вдосконалення орієнтовано на порушення самої основи реалізації відмічених атак - введення випадкового (параметричного) зсуву призводить до того, що поняття диференційних та лінійних характеристик у тому змісті, котрий вкладався в них розробниками відповідних атак, зникає. Тепер можна говорити про характеристики тільки у ймовірнісному змісті. Дійсно, навіть якщо узяти деяку (статичну) характеристику, котра може бути одержана при використанні класичного алгоритму DES, в модифікованому варіанті зшивки мов виникнення такої характеристики може трапитись лише у тому випадку, коли всі значення зсувів (у всіх циклах) будуть дорівнюватися нулю, що при випадкових однакових розповсюджених у заданому діапазоні значень зсувів півблоків даних кожного із циклів може виникнути з ймовірністю

$$\left(\frac{1}{2^5}\right)^{16} = 2^{-80} \quad (\text{для 13-циклової характеристики,}$$

$$\text{що використана в атаці Еді Біхама } \left(\frac{1}{2^5}\right)^{13} = 2^{-65})$$

З'явлення такого коефіцієнта перед значеннями ймовірностей можливих характеристик робить атаки диференційного та лінійного криптоаналізу на модифіковані шифри практичним безглуздом.

Спосіб шифрування даних для систем обробки в ЕОМ може бути реалізований таким чином. Послідовність двійкових символів відкритого тексту розбивають на 64-бітні блоки, кожний з котрих розбивають, у свою чергу, на правий та лівий півблоки по 32 біти, розміщують їх у відповідних накопичувачах, і піддають зашифровуванню, котре включає в себе 16 циклів, при цьому дані з виходу накопичувача правого півблока і відповідного підключа кожного циклу подають на вхід циклової функції перетворення, вихідні дані котрої порозрядно підсумовують у відповідному суматорі за модулем 2 з даними лівого півблока, при цьому обирають п'ять визначених бітів з 32 бітів на входи або виходи циклової функції, перетворюють їх у відповідне число зсувних імпульсів, і з їх допомогою виконують циклічний зсув результату порозрядного підсумовування вихідних даних циклової функції з даними лівого півблока, котрими заповнюють накопичувач правого півблока чергового циклу. Дані накопичувача правого півблока теперішнього циклу при цьому переносять у накопичувач лівого півблока чергового циклу.

---

ДП "Український інститут промислової власності" (Укрпатент)  
Україна, 01133, Київ-133, бульв. Лесі Українки, 26  
(044) 295-81-42, 295-61-97

---

Підписано до друку \_\_\_\_\_ 2002 р. Формат 60х84 1/8  
Обсяг \_\_\_\_\_ обл.-вид арк. Тираж 50 прим. Зам. \_\_\_\_\_

---

УкрІНТЕІ, 03880, Київ-39 МСП, вул. Горького, 180  
(044) 268-25-22

---