УДК 621

О.А. МЯСІЩЕВ, В.М. МУРАВА, В.П. НЕЗДОРОВИН
Хмельницький національний університет

ПОБУДОВА АЛГОРИТМУ ПСЕВДО-ЙМОВІРНІСНОГО ШИФРУВАННЯ НА ОСНОВІ БЛОКОВИХ ШИФРІВ

Розглядається вирішення завдань забезпечення інформаційної безпеки сучасних інформаційно-телекомунікаційних систем, досить широко застосовуються симетричні захисні перетворення інформації. Даний вид перетворень перетворює вихідні тексти в псевдовипадкові послідовності знаків залежно від деякої інформації порівняно малого обсягу (від ключа) недоступною потенційному порушнику. Зазвичай під час оцінювання рівня безпеки, забезпечуваної алгоритмами захисних перетворень, приймається модель порушника, в якій вважається, що ключ є невідомим порушнику. Проте порівняно недавно було дано обґрунтування актуальності розгляду так званих атак з примусом до розкриття ключа і запропоновано загальний підхід до захисту від таких атак, який полягає у застосуванні захисних алгоритмів, що формують перетворений текст, який допускає неоднозначне відновлення осмисленого тексту. Практична важливість захисних перетворень такого типу в першу чергу пов'язана з можливістю реалізації на їх основі механізмів захисту інформації нового типу, які дозволяють, зокрема, направити порушника помилковим шляхом і нав'язати йому неправдиву інформацію. Предметом дослідження є механізми, примітиви, алгоритми та протоколи захисних перетворень і аутентифікації інформації в засобах і системах інформаційної безпеки. Мета даної роботи полягає у підвищенні рівня інформаційної безпеки інформаційно-телекомунікаційних технологій за рахунок поліпшення продуктивності варіантів реалізації псевдо-ймовірнісних захисних перетворень, придатних для апаратної та програмної реалізації в засобах захисту інформації.

Ключові слова: псевдо-ймовірнісне шифрування, блокові шифри, інформаційна безпека, інформаційно-телекомунікаційні системи, ключ, алгоритм, захисні перетворення.

A.A. MYASISCHEV, V.M. MURAVA, V.P. NEZDOROVIN
Khmelnytsky National University

CREATION OF AN ALGORITHM OF PSEUDO-PROBABILISTIC ENCIPHERING ON THE BASIS OF BLOCK CODES

Symmetric protective transformations of information are rather widely applied to the solution of problems of ensuring information security of modern information and telecommunication systems. This type of transformations will be transformed by source texts to the pseudorandom sequences of signs depending on some information of rather small volume (from a key) is inaccessible to the potential violator. Usually at assessment of level of safety ensured by algorithms of protective transformations the model of the violator in which it is considered that the key is unknown to the violator is accepted. However rather justification of relevance of consideration of the so-called attacks with coercion to disclosure of a key has been given recently and the general approach to protection against such attacks which consists in application of protective algorithms which form the transformed text which allows ambiguous recovery of the intelligent text is offered. Practical importance of protective transformations of this kind first of all is connected with a possibility of realization on their basis of mechanisms of information security of new type which allow to direct, in particular, the violator on a false way and to impose him false information. Object of research are mechanisms, primitives, algorithms and protocols of protective transformations and authentication of information in means and information security systems. The purpose of this work consists in increase in level of information security of information and telecommunication technologies due to improvement of productivity of options of realization of pseudo-probabilistic protective transformations suitable for hardware and program realization in means of information protection.

Key words: pseudo-probabilistic encryption, block ciphers, information security, information and telecommunication systems, key, algorithm, protective transformations.

Постановка завдань. Теоретична значущість роботи полягає в розробці методів побудови продуктивних алгоритмів захисних перетворень з альтернативним відновленням вихідного повідомлення, що задовольняють критерію обчислювальної непомітності від імовірнісного перетворення і володіють досить високою продуктивністю. Практична значимість полягає в тому, що розроблені алгоритми на основі запропонованих методів можуть бути застосовані для вбудовування нових захисних механізмів в комплексні засоби забезпечення комп'ютерної безпеки.

Основна частина. Метод симетричного шифрування, заснований на обчисленні деякої хеш-функції, на підставі якого будується алгоритм імовірнісного шифрування. Він, у свою чергу, дає можливість побудови алгоритму псевдо-ймовірнісного перетворення. Розроблено метод псевдо-випадкового блочного захисного перетворення, який задовольняє додаткової вимоги до схем псевдо-ймовірнісного захисного перетворення, що забезпечує безпеку до примусових атакам з виміром часу розшифрування. Описаний алгоритм, заснований на обчисленні значень хеш-функції, і наведена таблиця з ймовірностями збою під час шифрування. Отриманий алгоритм псевдо-ймовірнісного захисного перетворення, заснований на блокових шифрах.

У відомому методі для імовірнісного блочного шифрування використовується b-бітова функція шифрування C, а зашифроване повідомлення розділяється на q-розрядні блоки даних (q <b). Для перетворення блоку відкритого повідомлення M генерується w-бітовий випадковий блок A (w= b − q), за яким слідує складання b-бітового вхідного блоку даних B = A || M, де знак || позначає операцію конкатенації двох довічних векторів A і M і обчислює блок зашифрованого повідомлення S = C_K (B), де K є ключем

шифрування. Раціональність практичного застосування алгоритму імовірнісного шифрування відноситься до наступних елементів:

1) він забезпечує більший захист від атак з використанням backdoor в використовуваних блок-шифри;

2) він потенційно запобігає атаки з використанням деяких непередбачених вразливостей алгоритму блочного шифрування.

Слід зазначити, що в реальних пристроях шифрування використовується генератор випадкових чисел (ГВЧ) повинен бути впроваджений в якості внутрішньої частини, наприклад, в електронному циклі, що реалізує алгоритм блочного шифрування С.

Таким чином, підвищення безпеки забезпечується тільки в тому випадку, коли потенційний супротивник не в стані модифікувати ГВЧ або його вихідні дані. При використанні різних значень відносини b / q для деякої даної функції шифрування С, можна вибрати необхідний компроміс між безпекою та швидкістю шифрування. Чим більше це відношення, тим більше підвищується рівень безпеки і тим нижче швидкість шифрування даних. Останнє можна грубо оцінити за допомогою формули d = d_0 (b - w) / b, де d_0 – швидкість шифрування. Загальна схема ймовірного блочного шифрування показана на схемі 1. Схема бути легко перетворена в схему псевдо-можливого блочного шифрування, яка може бути використана для одночасного шифрування двох незалежних повідомлень, фіктивних і секретних, з використанням двох різних ключів K і Q відповідно. Для цієї мети можна замінити ГВЧ деякої блокової функцією шифрування C′ з блоком w-бітних вхідних даних. Замість генерації q-бітного випадкового числа A, це зашифрований q-бітний блок T секретного повідомлення (схема 2).

При використанні блокового алгоритму шифрування C′ для перетворення блоку даних T з ключем Q, отриманий проміжний блок шифр-тексту $S_T = C_Q(T)$ є обчислювально не відрізняються від рівномірно випадкового q-бітового двійкового вектора. Потім блок S_T об'єднується з блоком фіктивного повідомлення M і перетворюється у вихідний блок зашифрованого повідомлення:

$$S = C_k * (K_T || M)$$

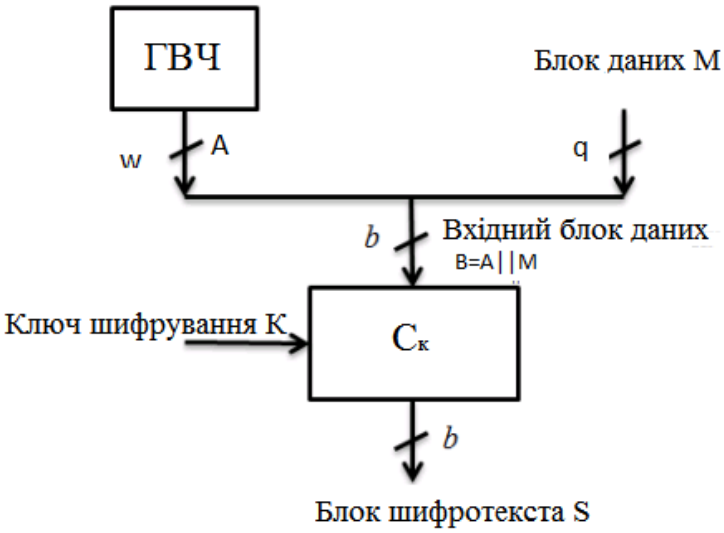

Рис. 1. Загальна схема ймовірного блочного шифрування

Коли примусово відправник і одержувач повідомлення можуть відкривати фіктивне повідомлення M і підроблений ключ K і оголошувати про використання блочного імовірнісного алгоритму шифрування. Таким чином, під час примушує атаки обидві сторони мають можливість без підозр використовувати фіктивні дані. Пропонований псевдо-імовірнісний метод шифрування забезпечує заперечення. У монографії представлені кілька методів імовірнісного шифрування з деякою детермінованою функцією блочного шифрування. Для кожного з цих методів можна запропонувати відповідну псевдо-вірогідну схему блочного шифрування, яка безпечна для атак з примусом. Такі псевдо-імовірнісні схеми шифрування відносяться до запланованих алгоритмам і протоколам заперечення шифрування. Вони забезпечують двосторонній захист до тих пір, поки противник не зможе перевірити час розшифрування, необхідне для розкриття секретного повідомлення. Якщо у нього є така можливість, то він зможе встановити, що час дешифрування підробленого повідомлення менше часу дешифрування секретного повідомлення. Крім того, можна припустити, що в деяких випадках противник порівнює функції кодування, які використовуються для дешифрування фіктивних і секретних повідомлень.

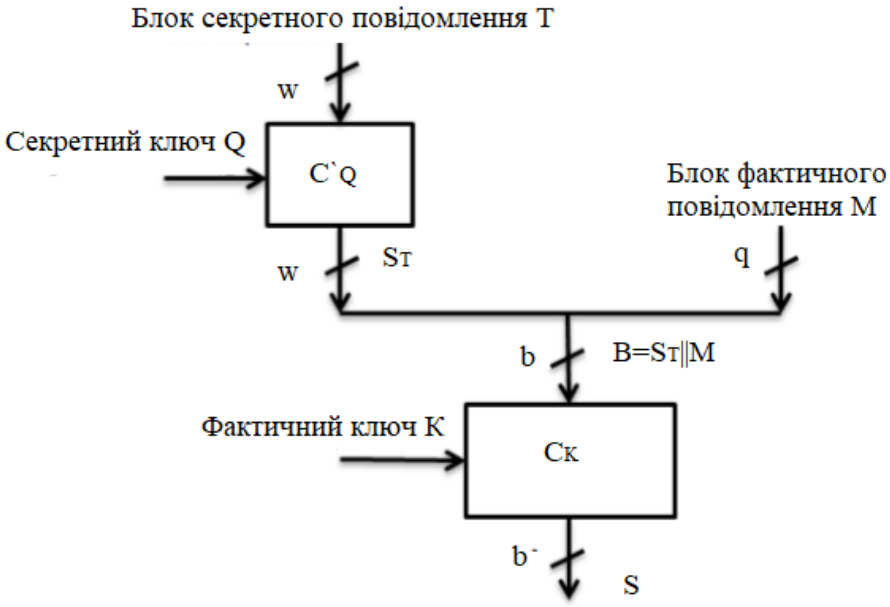

Рис. 2. Загальна схема псевдо-ймовірного блочного шифрування

Щоб забезпечити заперечення під час атак, скоєних противником, які мають зазначені можливості, можна запропонувати наступний додатковий критерій алгоритму шифрування: фіктивні і секретні повідомлення повинні бути розшифровані одним і тим же алгоритмом дешифрування. Цей критерій може бути виконаний за допомогою додавання додаткового перетворення фіктивного блоку повідомлення M з блочною функцією шифрування C' і установкою значень q = w = b / 2, як показано на малюнку 2.3, де блок Transp (e) виконує керовану перестановку двох блоків даних w -біт S_T і S_M: якщо e = 1, то $Transp^{(e)}(S_T||S_M) = S_M||S_T$; якщо e = 0, то $Transp^{(e)}(S_T||S_M) = S_T||S_M$. Передбачається, що ключі K і Q задовольняють умові (K mod 2) xor (Q mod 2) = 1, де і значення e залежить від ключа наступним чином (ключі K і Q генеруються так, що вони мають різну парність): e = K mod 2 і e = Q mod 2. у цьому випадку наступний алгоритм розкриває фіктивні або секретні повідомлення в залежності від використовуваного ключа K і Q.

Імовірнісний алгоритм шифрування, який може бути пов'язаний з псевдо-імовірнісним алгоритмом шифрування (Схема 3), показаний на схемі 4. Легко бачити, що зашифроване повідомлення, створене першим алгоритмом під час одночасного шифрування секретного повідомлення T з секретним ключем Q і фіктивним повідомленням M з фіктивним ключем K, потенційно може бути отриманий другим алгоритмом, використовуваним для шифрування фіктивного повідомлення по фіктивному ключу. Щоб відрізнити псевдо-розподіл усіх шифрування від ймовірного, вимагається розкриття секретного повідомлення T. При використанні функцій блочного шифрування C' і C, наприклад TripleDES [40], з блоком вхідних даних, які мають розмір w = 64 і AES [40], з блоком вхідних даних, які мають розмір b = 128, обчислювально важко відрізнити заперечувальну схему шифрування (рис. 3) від ймовірнісної схеми (рис. 4).

Алгоритм розшифрування, який відповідає як заперечуваний, так і імовірнісним схем шифрування, виглядає наступним чином:

1. Встановити ключ K* = (K, K`), де K` = K (для розкриття фіктивного повідомлення) і K' = Q (для розкриття секретного повідомлення).

2. Обчислити біт e = K' mod 2.

3. Розшифрувати блок зашифрованого повідомлення S: B = ($B_1||B_2$) $C_{K'}^{-1}(S)$, де проміжний блок B зашифрованого повідомлення представлений як поєднання u-бітних підблоків даних B_1 і B_2.

4. Виконати операцію транспонування$Transp^{(e)}(B_1||B_2) : (B`_1||B`_2) = Transp^{(e)}(B_1||B_2)$.

5. Обчислити u-бітний блок відкритого повідомлення M`:M` – $C_{K'}^{-1}(B`_2)$.

Висновки. Представлений метод псевдо-ймовірнісного блочного шифрування, який задовольняють додаткової вимоги до схем заперечного шифрування, яке забезпечує безпеку примусових атак з виміром часу дешифрування. Додаткова вимога формується як розшифрування, як секретного повідомлення, так і підробленого повідомлення одним і тим же алгоритмом розшифрування. Розроблено блочний алгоритм псевдо-ймовірнісного шифрування. Досягається додаткове покращення статистичних властивостей одержуваної криптограми. Застосування блокових шифрів в порівнянні з хеш функціями забезпечують більш високу продуктивність алгоритмів.

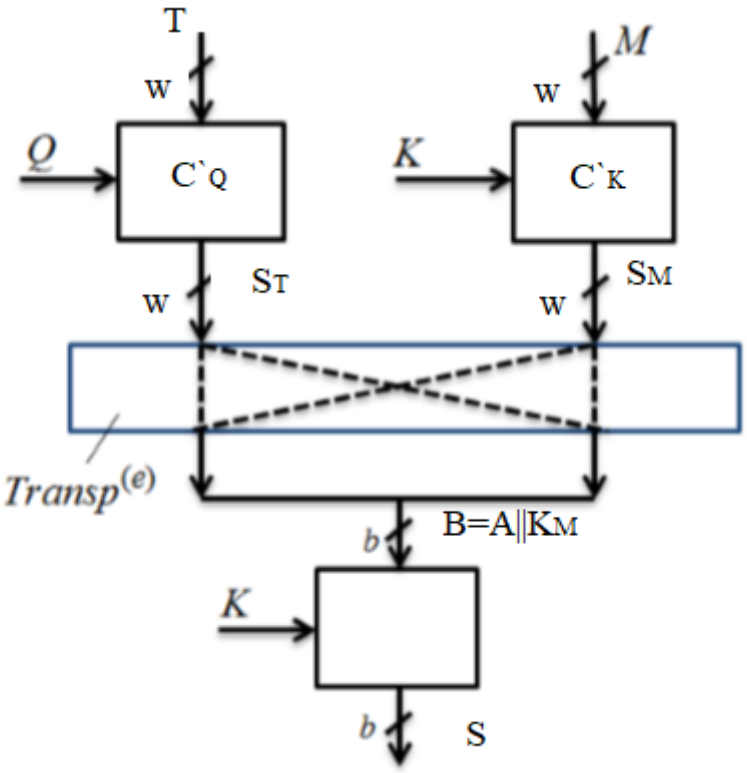

Рис. 3. Загальна схема псевдо-ймовірного блочного шифрування

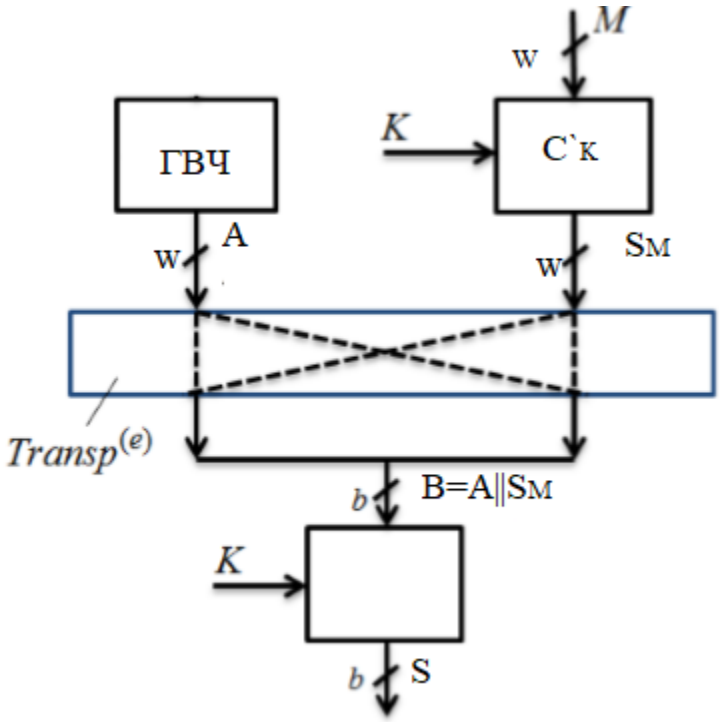

Рис. 4. Загальна схема псевдо-ймовірного блочного шифрування

Література

1. Молдовян Н. А. Протокол отрицаемого шифрования по открытому ключу, включающий процедуру аутентификации пользователей / Н. А. Молдовян, М. С. Михтеев, Кім Нгуєн Туан // Вопросы защиты информации. – 2016. – № 3. – С. 9–15.

2. Михтеев М. С. Гибридный протокол отрицаемого шифрования, основанный на процедуре аутентификации // М. С. Михтеев, Н.А. Молдовян // Вопросы защиты информации. – 2017. – № 1. – С. 12–17.

3. Шнайдер Б. Прикладна криптографія. Протоколи, алгоритми, вихідні тексти на мові СІ / Шнайдер Б. – М. : Изд. ТРІУМФ, 2002. – С. 816.

4. Молдовян Н.А. Протокол стійкого шифрування по ключу малого розміру / Н.А. Молдовян, А. А. Горячев, А. В. Мурах // Питання захисту інформації. – 2015. – № 1. – С. 3–8.

5. V. Lyubashevsky , A. Palacio, G. Segev. Public-Key Cryptographic Primitives Provably as Secure as Subset Sum // TCC 2010, LNCS 5978, Zurich, 2010. – P. 382–400.

6. ГОСТ Р 34.12-2015 Інформаційна технологія. Криптографічний захист інформації. Блокові шифри. – М. : Стандартинформ, 2015.

7. Венбо Мао. Сучасна криптографія. Теорія і практика / Венбо Мао. – М., СПб, Київ : Видавничий будинок «Вільямс», 2005. – С. 763.

8. Мельников В. П. Захист інформації / Мельников В. П., Купріянов А. В., Схіртладзе А. Р. – Academia, 2014. – С. 304.

9. Аграновський А. В. Практична криптографія: алгоритми та їх програмування / Аграновський А. В., Хаді Р. А. – Солон-Прес, 2009.

10. Молдовян Н.А. Практикум з криптосистемам з відкритим ключем / Молдовян Н.А. – СПб : «БХВ-Петербург», 2007. – С. 298.

11. Сюань Чжоу. Приховування даних, доступ до стеганографічної файлової системи / Сюань Чжоу, HweeHwa Панг, Кіан-Чи Тан // ICDE. – Бостон, Массачусетс, Березень 2004 Року. – ПП. 572-583.

12. Березін А. Н. Спосіб заперечного шифрування / А. Н. Березін, А. Р. Биричевский, Н. А. Молдов'ян, А. В. Рижков // Питання захисту інформації. – 2013. – № 2. – С. 18–21.

References

1. Moldovyan N. A., Mateev M. S., Kim Nguyen Tuan. Deny Protocol encryption public key, includes the procedure of user authentication. The protection of information. 2016. No. 3. – S. 9-15.

2. Mateev M. S., Moldovyan N. Hybrid encryption Protocol reject based on the authentication procedure. The protection of information. 2017. No. 1. – P. 12-17.

3. Schneider Would. Applied cryptography. Protocols, algorithms, and source code in C language. – M: Izd. TRIUMF, 2002. – S. 816.

4. Moldovyan N. A. Goryachev A. A., Muravyov A. V. Protocol strong encryption key small size // Problems of information security. — 2015. — No. 1. — P. 3-8.

5. V. Lyubashevsky, A. Palacio, and G. Segev. Public-Key Cryptographic Primitives Provably as Secure as Subset Sum// TCC 2010, LNCS 5978, Zurich, 2010. – Pp. 382 – 400

6. GOST R 34.12-2015 Information technology. Cryptographic protection of information. Block ciphers. — M.: STANDARTINFORM, 2015.

7. Wenbo Mao. Modern cryptography. Theory and practice. – M., SPb, Kiev, Ukraine. Publishing house "Williams", 2005. – C. 763.

8. Melnikov V. P., A. V. Kupriyanov, A. G. Skhirtladze. Academia, 2014. – C. 304.

9. Agranovsky A. B., Hadi, G. A., Practical cryptography: algorithms and their programming, Solon-Press – 2009.

10. Moldovyan N.. Workshop on public-key cryptosystems. St. Petersburg, "BHV-Petersburg", 2007. – C. 298.

11. Xuan Zhou, HweeHwa Pang, Kian-Lee Tan. Hiding data accesses in steganographic file system // ICDE. Boston, Massachusetts, March 2004. – Pp. 572-583.

12. Berezin A. N., Birichevskiy A. G., Moldav Ian N. A., Ryzhkov, A.V., Method zapretnogo encryption the protection of information. No. 2. 2013. – Pp. 18-21.