УДК 004.056.55 **doi: 10.32620/reks.2020.3.07**

О. С. ВАМБОЛЬ

Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

ВДОСКОНАЛЕНА ПОЛІНОМІАЛЬНО-СКЛАДНА АТАКА ВІДНОВЛЕННЯ ВІДКРИТОГО ТЕКСТУ НА РАНЦЕВИЙ ШИФР НА ОСНОВІ МАТРИЦЬ

Асиметричні шифри широко використовуються для забезпечення конфіденційності передачі даних, здійснюваної за допомогою незахищених каналів. Ці криптосистеми дозволяють сторонам комунікації сформувати спільний секретний ключ для симетричної схеми шифрування, не надаючи підслуховувачу інформацію, корисну для криптоаналізу. Протоколи мережевої безпеки, які використовують асиметричні шифри, включають TLS, S/MIME, OpenPGP, Tor та багато інших. Деякі з асиметричних схем шифрування є гомоморфними, тобто такими, що дозволяють виконувати обчислення з зашифрованими даними без потреби попереднього розшифрування. Зазначена вище властивість робить можливим використання цих криптосистем не тільки для узгодження симетричних ключів, але і в декількох інших областях застосування, зокрема в протоколах таємного голосування та хмарних обчисленнях. Ранцевий шифр на основі матриць є новою адитивно гомоморфною асиметричною схемою шифрування, що базується на властивостях ізоморфних перетворень внутрішнього прямого добутку діагональних підгруп загальної лінійної групи над полем Галуа. На відміну від класичних ранцевих схем шифрування, криптостійкість цього шифру залежить від обчислювальної складності задачі багатовимірного дискретного логарифмування. Незважаючи на ряд корисних властивостей, подальші дослідження криптостійкості ранцевого шифру на основі матриць виявили серйозні недоліки, притаманні цій криптографічній схемі. В даній статті запропоновано вдосконалену поліноміально-складну атаку відновлення відкритого тексту на ранцевий шифр на основі матриць. Застосування цього криптоаналітичного методу потребує лише загальнодоступної інформації і має часову складність $O(t^{1.34})$, де t позначає час виконання розшифрування криптосистемою, що атакується. Вищезазначена атака є продуктивнішою та простішою в програмній реалізації у порівнянні з оригінальною. Переваги запропонованого методу обумовлені використанням в його алгоритмі простої і відносно швидкої операції обчислення сліду матриці замість складніших і повільніших перетворень.

Ключові слова: *ранцевий шифр на основі матриць; криптоаналіз; обчислювальна складність; асиметричний шифр; гомоморфне шифрування; атака відновлення відкритого тексту.*

Вступ

Асиметричні шифри широко використовуються для забезпечення конфіденційності передачі даних, здійснюваної за допомогою незахищених каналів. Ці криптосистеми дозволяють сторонам комунікації сформувати спільний секретний ключ для симетричної схеми шифрування, не надаючи підслуховувачу інформацію, корисну для криптоаналізу [1, 2]. Протоколи мережевої безпеки, які використовують асиметричні шифри, включають TLS [3], S/MIME [4], OpenPGP [5], Tor [6] та багато інших [7].

Деякі з асиметричних шифрів є гомоморфними, тобто такими, що дозволяють виконувати обчислення з зашифрованими даними без потреби попереднього розшифрування. Зазначена властивість робить можливим використання цих схем шифрування не тільки для узгодження симетричних ключів, але і в декількох інших областях застосування. Зокрема, гомоморфні асиметричні шифри використовуються в протоколах таємного голосування [8] та хмарних обчисленнях [9].

Ранцевий шифр на основі матриць є новою адитивно гомоморфною асиметричною схемою шифрування, що відноситься до ранцевих шифрів на основі груп [10]. Ця криптосистема базується на властивостях ізоморфних перетворень внутрішнього прямого добутку діагональних підгруп загальної лінійної групи над полем Галуа [11]. На відміну від класичних ранцевих криптосхем, криптостійкість вищезазначеного шифру залежить від обчислювальної складності задачі багатовимірного дискретного логарифмування [10].

Зазначений шифр було запропоновано в [11]. Підхід до побудови ранцевого шифру на основі матриць над полем Галуа, яке має мультиплікативну

© О. С. Вамболь, 2020

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

підгрупу великого гладкого порядку, було запропоновано в [12]. Інший підхід, в якому даний шифр будується над малим полем Галуа, був використаний в [10], де для цієї криптосистеми було доведено властивість адитивного гомоморфізму. Також в [10] у вигляді стислого опису було запропоновано новий протокол таємного голосування, який базується на вищезгаданому шифрі.

Проте, незважаючи на ряд корисних властивостей, подальші дослідження криптостійкості ранцевого шифру на основі матриць виявили серйозні недоліки, притаманні цій криптосхемі. А саме, в [13] було запропоновано поліноміально-складну атаку відновлення відкритого тексту на даний шифр, яка використовує лише загальнодоступну інформацію. Даний метод криптоаналізу базується на властивостях характеристичних поліномів подібних матриць.

Постановка задачі

Ця стаття продовжує дослідження криптостійкості ранцевого шифру на основі матриць, яке було розпочате в [13]. Задача даної роботи полягає в розробленні вдосконаленої атаки відновлення відкритого тексту на зазначений шифр, яка у порівнянні з методом, запропонованим в [13], має вищу продуктивність і є простішою в програмній реалізації.

Ранцевий шифр на основі матриць

Дана криптосистема має два параметри [10]:

1. Порядок кінцевого поля, над яким будується шифр. Цей параметр позначений як q. Число q - 1 повинно бути малим (або принаймні гладким) і більшим за 1.

2. Порядок використовуваних невироджених квадратних матриць над GF(q). Даний параметр позначається як n. Мінімальне значення n дорівнює 2.

Генерація пари ключів включає такі кроки [10]:

1. Вибір породжуючої множини абелевої групи G, яка є діагональною підгрупою загальної лінійної групи GL(n, GF(q)). Ця множина представлена кортежем $(g_1, ..., g_n)$, отриманим з $(z_1, ..., z_n)$, де z_i є випадково обраним примітивним елементом GF(q). Елемент g_i отримується з n-вимірної одиничної матриці над GF(q) шляхом заміни (i, i)-го елементу на z_i. Оскільки порядок кожного g_i дорівнює q - 1, кожен $d \in G$ має єдине представлення у вигляді

$$d = g_1^{p_1} \cdot g_2^{p_2} \cdot ... \cdot g_n^{p_n}, \quad (1)$$

де p_i є невід'ємним цілим числом, меншим за q - 1. Нехай $ent_i(d)$ є (i, i)-им елементом матриці d, тоді не важко перевірити справедливість формули

$$ent_i(d) = z_i^{p_i}. \quad (2)$$

2. Генерація секретного ключа, який є матрицею $s \in GL(n, GF(q))$. Матриця s визначає групу H, яка є підгрупою групи GL(n, GF(q)), та пару взаємно зворотних ізоморфізмів $f: G \to H$ і $f^{-1}: H \to G$, яку можна описати в такій спосіб:

$$\begin{aligned} f &: \delta \to s^{-1} \cdot \delta \cdot s, \\ f^{-1} &: \mu \to s \cdot \mu \cdot s^{-1}. \end{aligned} \quad (3)$$

3. Обчислення відкритого ключа, який є кортежем $(e_1, ..., e_n)$. Його елементи знаходяться відповідно до формули

$$e_i = f(g_{\sigma_i}), \quad (4)$$

де $(\sigma_1, ..., \sigma_n)$ є випадковою перестановкою кортежу (1, 2, ..., n). Хоча в оригінальній версії цього шифру зазначена секретна перестановка не використовується [11], в [13] було запропоновано перемішувати елементи кортежу $(g_1, ..., g_n)$ для ускладнення криптоаналітичної атаки на ранцевий шифр на основі матриць.

Зашифрування складається з таких етапів [10]:

1. Представлення відкритого тексту цілочисельним кортежем $(x_1, ..., x_n)$, де $0 \le x_i \le q - 2$.

2. Обчислення шифротексту за формулою

$$c = e_1^{x_1} \cdot e_2^{x_2} \cdot ... \cdot e_n^{x_n}. \quad (5)$$

Оскільки $\{g_1, ..., g_n\}$ – породжуюча множина групи G, з (3), (4) та процедури зашифрування випливає, що кожен елемент групи H належить до множини шифротекстів. Отже, існує бієкція між відкритим текстами та елементами групи H.

Розшифрування можна представити нижченаведеною послідовністю кроків [10]:

1. Обчислення кортежу $(y_1, ..., y_n)$ з використанням формули

$$y_i = ent_i(f^{-1}(c)). \quad (6)$$

З огляду на (1) – (5), y_{σ_i} дорівнює z_{σ_i} в степені x_i.

2. Кортежі $(z_1, ..., z_n)$ та $(\sigma_1, ..., \sigma_n)$ знаходяться з використанням такої умови:

$$ent_k(f^{-1}(e_i)) \ne 1 \Rightarrow \sigma_i = k \wedge z_k = ent_k(f^{-1}(e_i)). \quad (7)$$

Даний підхід випливає з (3), (4) та визначення g_i. Цього кроку можна уникнути, зберігаючи вищезазначені кортежі разом з секретним ключем.

3. Відкритий текст $(x_1, ..., x_n)$ відновлюється за формулою

$$x_i = \mathrm{dlog}_{z_{\sigma_i}}(y_{\sigma_i}), \qquad (8)$$

де $\mathrm{dlog}_\beta(\alpha)$ – дискретний логарифм α за основою β. Оскільки q - 1 є невеликим (або принаймні гладким), цю операцію можна виконати ефективно.

Даний шифр є адитивно гомоморфним завдяки таким властивостям [10]:

1. Множина відкритих текстів є адитивною абелевою групою відносно операції ⊕, визначеної таким чином:

$$(u_1, ..., u_n) \oplus (v_1, ..., v_n) = \qquad (9)$$
$$= \big((u_1 + v_1) \bmod (q-1), ..., (u_n + v_n) \bmod (q-1)\big).$$

З огляду на (9), група відкритих текстів є адитивною групою n-вимірного модуля над кільцем лишків за модулем q - 1.

2. Множина шифротекстів і операція множення матриць разом утворюють мультиплікативну абелеву групу H, зазначену вище.

3. Якщо процедура зашифрування перетворює відкритий текст m_i в шифротекст c_i, то результатом розшифрування шифротексту $c_i \cdot c_j$ є відкритий текст $m_i \oplus m_j$.

Бієкція між елементами групи H та відкритими текстами разом з вищезазначеними властивостями роблять групу шифротекстів ізоморфною групі відкритих текстів.

Наведений в [13] іграшковий приклад зазначеної криптосистеми, який демонструє її адитивну гомоморфність, представлено нижче. В його випадку цей шифр побудовано для q = 13 та n = 4. З огляду на вказані значення параметрів, G є діагональною підгрупою групи GL(4, GF(13)). В якості кортежу $(z_1, ..., z_4)$ обрано (2, 6, 7, 11), тому $(g_1, ..., g_4)$ описується таким чином:

$$g_1 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \; g_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$
$$g_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \; g_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 11 \end{pmatrix}.$$

Оскільки кожен g_i має порядок 12, кортеж відкритого тексту може містити тільки числа, які належать до інтервалу [0 .. 11].

Секретний ключ s і зворотну до нього матрицю s^{-1} обрано, як вказано нижче:

$$s = \begin{pmatrix} 4 & 0 & 2 & 10 \\ 3 & 10 & 0 & 11 \\ 10 & 12 & 9 & 8 \\ 11 & 4 & 6 & 10 \end{pmatrix}, \; s^{-1} = \begin{pmatrix} 6 & 4 & 12 & 6 \\ 5 & 11 & 1 & 12 \\ 7 & 8 & 4 & 7 \\ 8 & 2 & 10 & 4 \end{pmatrix}.$$

В якості кортежу $(\sigma_1, \ldots, \sigma_4)$ обрано (2, 4, 3, 1). Отже, враховуючи (4), відкритий ключ $(e_1, ..., e_4)$ визначається таким чином:

$$e_1 = \begin{pmatrix} 9 & 5 & 0 & 12 \\ 9 & 5 & 0 & 7 \\ 3 & 10 & 1 & 11 \\ 4 & 9 & 0 & 7 \end{pmatrix}, \; e_2 = \begin{pmatrix} 11 & 6 & 9 & 2 \\ 7 & 0 & 5 & 4 \\ 3 & 7 & 5 & 11 \\ 11 & 4 & 6 & 11 \end{pmatrix},$$
$$e_3 = \begin{pmatrix} 6 & 6 & 11 & 4 \\ 8 & 8 & 2 & 9 \\ 6 & 2 & 9 & 10 \\ 2 & 5 & 7 & 0 \end{pmatrix}, \; e_4 = \begin{pmatrix} 12 & 0 & 12 & 8 \\ 7 & 1 & 10 & 11 \\ 2 & 0 & 2 & 5 \\ 6 & 0 & 3 & 3 \end{pmatrix}. \qquad (10)$$

Кортежами відкритого тексту, обраними для зашифрування, є $m_1 = (3, 8, 1, 5)$ і $m_2 = (9, 7, 4, 11)$. Відповідна пара шифротекстів c_1 і c_2 отримується, як вказано нижче:

$$c_1 = e_1^3 \cdot e_2^8 \cdot e_3^1 \cdot e_4^5 = \begin{pmatrix} 10 & 10 & 8 & 0 \\ 4 & 5 & 4 & 12 \\ 7 & 6 & 12 & 2 \\ 10 & 0 & 6 & 3 \end{pmatrix},$$
$$c_2 = e_1^9 \cdot e_2^7 \cdot e_3^4 \cdot e_4^{11} = \begin{pmatrix} 10 & 10 & 10 & 12 \\ 9 & 0 & 9 & 6 \\ 11 & 4 & 12 & 6 \\ 7 & 3 & 8 & 1 \end{pmatrix}.$$

Обраний для розшифрування шифротекст c_p визначено таким чином:

$$c_p = c_1 \cdot c_2 = \begin{pmatrix} 5 & 2 & 0 & 7 \\ 5 & 1 & 8 & 10 \\ 10 & 7 & 11 & 12 \\ 5 & 3 & 1 & 3 \end{pmatrix}. \qquad (11)$$

Процедура розшифрування починається з обчислення $f^{-1}(c_p)$ згідно з (3). Оскільки

$$f^{-1}(c) = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 11 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix},$$

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

перший крок розшифрування встановлює тотожність $(y_1, \ldots, y_4) = (3, 1, 11, 5)$. Опціональний наступний крок виконується з використанням (7), як вказано нижче:

$$\text{ent}_2(f^{-1}(e_1)) = 6 \Rightarrow \sigma_1 = 2 \wedge z_2 = 6,$$
$$\text{ent}_4(f^{-1}(e_2)) = 11 \Rightarrow \sigma_2 = 4 \wedge z_4 = 11,$$
$$\text{ent}_3(f^{-1}(e_3)) = 7 \Rightarrow \sigma_3 = 3 \wedge z_3 = 7,$$
$$\text{ent}_1(f^{-1}(e_4)) = 2 \Rightarrow \sigma_4 = 1 \wedge z_1 = 2.$$

Під час його виконання встановлюються тотожності $(\sigma_1, \ldots, \sigma_4) = (2, 4, 3, 1)$ і $(z_1, \ldots, z_4) = (2, 6, 7, 11)$. На заключному кроці відповідно до (8) обчислюється кортеж відкритого тексту $(x_1, \ldots, x_4)$, як наведено нижче:

$$x_1 = \text{dlog}_{z_{\sigma_1}}(y_{\sigma_1}) = \text{dlog}_6(1) = 0,$$
$$x_2 = \text{dlog}_{z_{\sigma_2}}(y_{\sigma_2}) = \text{dlog}_{11}(5) = 3,$$
$$x_3 = \text{dlog}_{z_{\sigma_3}}(y_{\sigma_3}) = \text{dlog}_7(11) = 5,$$
$$x_4 = \text{dlog}_{z_{\sigma_4}}(y_{\sigma_4}) = \text{dlog}_2(3) = 4.$$

Отже, результатом розшифрування c_p, визначеного як $c_1 \cdot c_2$, є кортеж (0, 3, 5, 4), який дорівнює $m_1 \oplus m_2$ завдяки тому, що використовуваний шифр є адитивно гомоморфним.

Попередня робота з криптоаналізу ранцевого шифру на основі матриць

Дотепер було запропоновано лише один поліноміально-складний метод криптоаналізу зазначеного шифру – атака відновлення відкритого тексту, наведена в [13]. Цей метод викладено на рис. 1.

На рис. 1 кортежі $(e_1, \ldots, e_n)$ і $(x_1, \ldots, x_n)$ є відкритими ключем і текстом відповідно, c позначає шифротекст. Параметри шифру q і n вважаються переданими разом з відкритим ключем. Змінні $B(\lambda)$ і $W(\lambda)$ містять поліноми від формальної змінної λ, коефіцієнти яких є елементами GF(q). Визначник матриці μ позначається як $\det(\mu)$; I – $(n \times n)$-вимірна одинична матриця над GF(q). Отже, характеристичним поліномом від змінної λ для матриці μ за визначенням є $\det(\lambda \cdot I - \mu)$ [14]. Найбільший спільний дільник $B(\lambda)$ і $W(\lambda)$ позначено як $\gcd(B(\lambda), W(\lambda))$.

Часова складність розглянутого методу становить $O(t^{1.34})$, де t позначає час, необхідний для виконання розшифрування криптосхемою, що піддається атаці. В категоріях параметрів ранцевого шифру на основі матриць часова складність зазначеної атаки може бути виражена як $O(n^4 \cdot \log^2(q) + n \cdot \log^4(q))$.

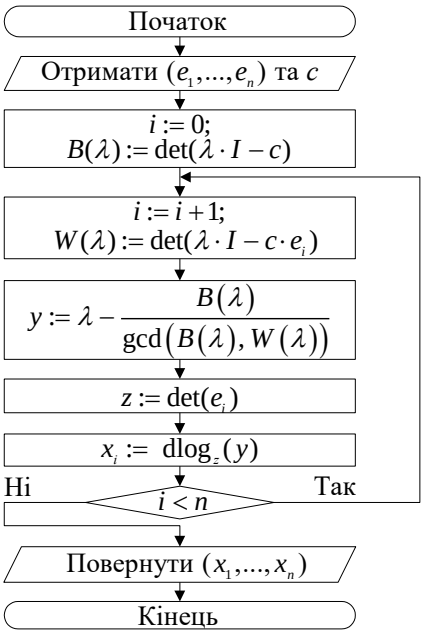

Рис. 1. Поліноміально-складна атака відновлення відкритого тексту на ранцевий шифр на основі матриць, запропонована в [13]

Вдосконалена атака відновлення відкритого тексту

На відміну від вищерозглянутої атаки, запропонований в цьому розділі метод базується на властивостях слідів подібних матриць.

Нехай μ є квадратною матрицею над довільним полем. Слід матриці μ є сумою елементів її головної діагоналі; позначається як $\text{tr}(\mu)$. Сліди подібних матриць рівні, тобто $\text{tr}(\mu) = \text{tr}(\nu \cdot \mu \cdot \nu^{-1})$, де ν є невиродженою матрицею тієї ж розмірності, що і μ [14].

Запропонована нижче теорема описує взаємозв'язок між шифротекстом, відкритим ключем, параметрами шифру та змінними процедури розшифрування.

Теорема 1. Нехай c є матрицею шифротексту, $(e_1, \ldots, e_n)$ – відкритий ключ, а $(y_1, \ldots, y_n)$, $(z_1, \ldots, z_n)$ і $(\sigma_1, \ldots, \sigma_n)$ є відповідними результатами перших двох кроків процедури розшифрування, тоді є справедливими рівності

$$z_{\sigma_i} = \text{tr}(e_i) - (n-1) \cdot \varepsilon, \tag{12}$$

$$y_{\sigma_i} = \frac{\text{tr}(c \cdot e_i) - \text{tr}(c)}{z_{\sigma_i} - \varepsilon}, \tag{13}$$

де ε – мультиплікативний нейтральний елемент кінцевого поля, над яким побудовано шифр.

Доведення. З огляду на (3) і (4), e_i подібна до g_{σ_i}, тому $\text{tr}(e_i) = \text{tr}(g_{\sigma_i})$. З визначення $(g_1, \ldots, g_n)$ ви-

пливає рівність $tr(g_{\sigma_i}) = z_{\sigma_i} + (n-1)\cdot\varepsilon$. З урахуванням вищезазначеного, рівність (12) є очевидною.

З огляду на (3) та (4), $f^{-1}(c\cdot e_i) = f^{-1}(c)\cdot g_{\sigma_i}$. Оскільки $f^{-1}(c) \in G$, з використанням (1) і (2) можна показати, що $f^{-1}(c)$ відрізняється від $f^{-1}(c)\cdot g_{\sigma_i}$ тільки σ_i-им елементом головної діагоналі, причому $ent_{\sigma_i}(f^{-1}(c)\cdot g_{\sigma_i}) = z_{\sigma_i}\cdot ent_{\sigma_i}(f^{-1}(c))$. Отже, з наведеного вище випливає справедливість тотожності $tr(f^{-1}(c\cdot e_i)) - tr(f^{-1}(c)) = (z_{\sigma_i} - \varepsilon)\cdot ent_{\sigma_i}(f^{-1}(c))$. Цей вираз, враховуючи (6), дозволяє обґрунтувати рівність $tr(f^{-1}(c\cdot e_i)) - tr(f^{-1}(c)) = (z_{\sigma_i} - \varepsilon)\cdot y_{\sigma_i}$. Подібність μ і $f^{-1}(\mu)$ при всіх μ, обумовлена (3), у сукупності з властивостями слідів подібних матриць робить можливим отримання з зазначеної рівності тотожності $tr(c\cdot e_i) - tr(c) = (z_{\sigma_i} - \varepsilon)\cdot y_{\sigma_i}$. З цієї формули випливає істинність (13). ■

Пропоновану вдосконалену атаку відновлення відкритого тексту викладено на рис. 2.

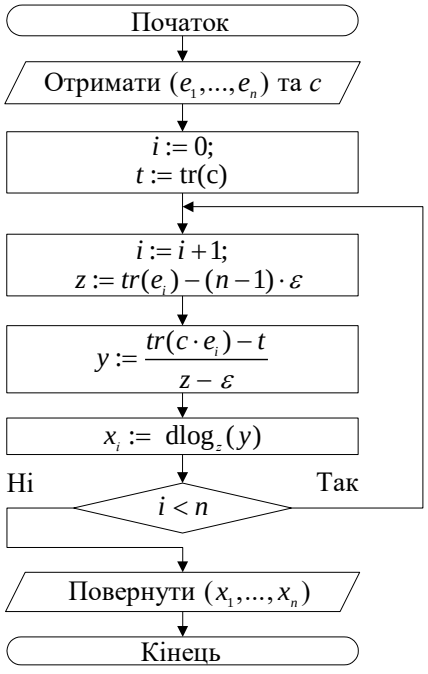

Рис. 2. Вдосконалена поліноміально-складна атака відновлення відкритого тексту на ранцевий шифр на основі матриць.

Зазначений метод застосовує (12) та (13) для знаходження значень змінних перших двох кроків процедури розшифрування і використовує отримані дані для здійснення операцій, які виконуються на останньому кроці цієї процедури. Відкриті ключ і текст позначені відповідно як $(e_1, ..., e_n)$ та $(x_1, ..., x_n)$, c є шифротекстом. Параметри шифру q та n є необхідними для інтерпретації даних відкритого ключа і тому вважаються переданими разом з ним. Мультиплікативний нейтральний елемент поля GF(q) позначено за допомогою символу ε.

Наведений нижче іграшковий приклад зазначеної атаки побудовано на основі розглянутого прикладу розшифрування. Вхідні дані представлені шифротекстом c, що дорівнює c_p в (11), і відкритим ключем $(e_1, ..., e_4)$, визначеним (10). Параметрами q та n є 13 і 4 відповідно. Отже, в результаті атаки має бути відновлено відкритий текст (0, 3, 5, 4).

Проміжні обчислення, які проводяться підчас виконання алгоритму, дають такі результати:

$$c\cdot e_1 = \begin{pmatrix} 0 & 7 & 0 & 6 \\ 1 & 5 & 8 & 4 \\ 0 & 4 & 11 & 10 \\ 9 & 12 & 1 & 9 \end{pmatrix},\ c\cdot e_2 = \begin{pmatrix} 3 & 6 & 6 & 4 \\ 1 & 9 & 7 & 4 \\ 12 & 3 & 5 & 2 \\ 8 & 10 & 5 & 1 \end{pmatrix},$$

$$c\cdot e_3 = \begin{pmatrix} 8 & 3 & 4 & 12 \\ 2 & 0 & 4 & 5 \\ 11 & 3 & 8 & 5 \\ 1 & 6 & 0 & 5 \end{pmatrix},\ c\cdot e_4 = \begin{pmatrix} 12 & 2 & 10 & 5 \\ 0 & 1 & 12 & 4 \\ 3 & 7 & 1 & 1 \\ 10 & 3 & 10 & 9 \end{pmatrix},$$

$$tr(c) = 7,\ tr(e_1) = 9,\ tr(e_2) = 1,\ tr(e_3) = 10,\ tr(e_4) = 5,$$
$$tr(c\cdot e_1) = 12,\ tr(c\cdot e_2) = 5,\ tr(c\cdot e_3) = 8,\ tr(c\cdot e_4) = 10.$$

Обчислення, виконувані на останньому кроці тіла циклу, можна описати таким чином:

$$x_1 := dlog_6(1),\ x_2 := dlog_{11}(5),$$
$$x_3 := dlog_7(11),\ x_4 := dlog_2(3).$$

Повернеким значенням є (0, 3, 5, 4). Отже, атака здійснена успішно.

Продуктивність вдосконаленої атаки відновлення відкритого тексту

Найбільш обчислювально складною базовою операцією над елементами GF(q) є ділення, яке для кінцевого поля є множенням на елемент, що є мультиплікативно зворотним до дільника. Обчислювальна складність цієї операції, як і у випадку множення, становить $O(\log^2(q))$ [15]. Додавання та віднімання елементів GF(q) потребує $O(\log(q))$ часу [15]. Отже, множення (n×n)-вимірних матриць над зазначеним полем має часову складність $O(n^3\cdot\log^2(q))$. Очевидно, що часова складність обчислення сліду для даних матриць становить $O(n\cdot\log(q))$. Дискретний логарифм в GF(q) можна знайти методом Поліга-Геллмана, виконавши $O(\log^2(q))$ базових операцій в цьому полі, оскільки число q - 1 є гладким або малим [16]. Тому, в GF(q) часова складність дискрет-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

ного логарифмування становить $O(\log^4(q))$. Тіло циклу в алгоритмі на рис. 2 виконується n разів.

Враховуючи рис. 2, з вищенаведеного випливає, що часова складність вдосконаленої атаки становить $O(n^4 \cdot \log^2(q) + n \cdot \log^4(q))$. Отже, з цього боку вдосконалений метод не відрізняється від оригінального, і його застосування також потребує $O(t^{1.34})$ часу, де t є часом виконання розшифрування криптосистемою, що атакується.

Проте, рівність виражених через нотацію великого O часових складностей не є достатньою умовою для однаковості продуктивностей. З огляду на рис. 1 та рис. 2, оригінальна атака виконує ряд таких перетворень з матрицями і поліномами над GF(q), які не потрібні для здійснення вдосконаленої атаки. Зазначені операції включають отримання характеристичного поліному (n×n)-вимірної матриці, обчислення визначника матриці того ж порядку і знаходження найбільшого спільного дільника двох поліномів степеня n. Сукупна кількість їх виконань становить 3n + 1. Часова складність кожної з них є не меншою за $O(n^2 \cdot \log^2(q))$ [13]. Замість цих операцій вдосконалена атака здійснює 2n + 1 обчислень слідів (n×n)-вимірних матриць над GF(q), кожен з яких можна отримати за $O(n \cdot \log(q))$ часу. Зазначені особливості роблять вдосконалену атаку продуктивнішою і простішою в програмній реалізації у порівнянні з оригінальною.

Висновки

Вдосконалена атака відновлення відкритого тексту, запропонована в цій роботі, має часову складність $O(t^{1.34})$, де t позначає час виконання розшифрування криптосистемою, що атакується. В категоріях параметрів ранцевого шифру на основі матриць часова складність застосування цього криптоаналітичного методу становить $O(n^4 \cdot \log^2(q) + n \cdot \log^4(q))$. Запропонована атака не відрізняється від оригінальної за вираженою через нотацію великого O часовою складністю, проте має вищу продуктивність і є простішою в програмній реалізації. Зазначені переваги вдосконаленої атаки обумовлені використанням в її алгоритмі простої і відносно швидкої операції обчислення сліду матриці замість складніших і повільніших перетворень.

Література

1. Schneier, B. Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th edn. [Text] / B. Schneier. – John Wiley & Sons, 2015. – 784 p.

2. Van Tilborg, H. Encyclopedia of Cryptography and Security, 2nd edn. [Text] / H. van Tilborg, S. Jajodia. – Springer, 2011. – 1416 p.

3. On the Security of the Pre-Shared Key Ciphersuites of TLS [Text] / Y. Li, S. Schäge, Z. Yang, F. Kohlar, J. Schwenk // Proceedings of the 17th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2014). – Buenos Aires, Argentina, March 26-28, 2014. – P. 669-684.

4. Schillinger, F. End-to-End Encryption Schemes for Online Social Networks [Text] / F. Schillinger, C. Schindelhauer // Proceedings of the 12th International Conference on Security, Privacy, and Anonymity in Computation, Communication, and Storage (SpaCCS 2019). – Atlanta, USA, July 14-17, 2019. – P. 133-146.

5. Format Oracles on OpenPGP [Text] / F. Maury, J.-R. Reinhard, O. Levillain, H. Gilbert // Proceedings of the Cryptographer's Track at the RSA Conference 2015 (CT-RSA 2015). – San Francisco, USA, April 20-24, 2015. – P. 220-236.

6. Ghosh, S. Post-Quantum Forward Secure Onion Routing (Future Anonymity in Today's Budget) [Text] / S. Ghosh, A. Kate // Proceedings of the 13th International Conference on Applied Cryptography and Network Security (ACNS 2015). - New York, USA, June 2-5, 2015. – P. 263-286.

7. ETSI White Paper No. 8. Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges [Text] / M. Campagna et al. – European Telecommunications Standards Institute, 2015. – 64 p.

8. Damgård, I. The Theory and Implementation of an Electronic Voting System [Text] / I. Damgård, J. Groth, G. Salomonsen // Secure Electronic Voting. – Springer, 2003. – P. 77-99.

9. Liu, J. Partially homomorphic encryption schemes over finite fields [Text] / J. Liu, L. Chen, S. Mesnage // Proceedings of the 6th International Conference on Security, Privacy and Applied Cryptography Engineering (SPACE 2016). – Hyderabad, India, December 14-18, 2016. – P. 109-123.

10. Vambol, A. The matrix-based knapsack cipher in the context of additively homomorphic encryption [Text] / A. Vambol // Proceedings of the 3rd International Conference on Computational Linguistics and Intelligent Systems (COLINS). – Kharkiv, Ukraine, April 18-19, 2019. – P. 344-354.

11. Животова, А. Модификация криптосистемы с открытым ключом на основе «задачи о рюкзаке» [Текст] / А. Животова, Н. Зюляркина, Ю. Костыгина // Вестник УрФО. Безопасность в информационной сфере. – 2014. – № 1(11). – С. 16-20.

12. Vambol, A. The Prospects for Group-based Knapsack Ciphers in the Post-Quantum Era [Text] / A. Vambol // Proceedings of the 9th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT). – Kyiv, Ukraine, May 24-27, 2018. – P. 271-275.

13. Vambol, A. Polynomial-Time Plaintext-Recovery Attack on the Matrix-Based Knapsack Cipher / A. Vambol // International Journal of Computing. – 2020. – Accepted for publication.

14. Roman, S. Advanced Linear Algebra, 2nd edn. / S. Roman. – Springer, 2005. – 482 p.

15. Menezes, A. Handbook of Applied Cryptography / A. Menezes, P. van Oorschot, S. Vanstone. – CRC Press, 1996. – 816 p.

16. Pohlig, S. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance [Text] / S. Pohlig, M. Hellman // IEEE Transactions on Information Theory. – 1978. – vol. 24, no. 1. – P. 106-110.

References

1. Schneier, B. *Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th edn*. John Wiley & Sons Publ., 2015. 540 p.

2. Van Tilborg, H., Jajodia, S. *Encyclopedia of Cryptography and Security, 2nd edn*. Springer Publ., 2011. 1416 p.

3. Li, Y., Schäge, S., Yang, Z., Kohlar, F., Schwenk, J. On the Security of the Pre-Shared Key Ciphersuites of TLS. *Proceedings of the 17th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2014)*. Buenos Aires, Argentina, March 26-28, 2014, pp. 669-684.

4. Schillinger, F., Schindelhauer, C. End-to-End Encryption Schemes for Online Social Networks. *Proceedings of the 12th International Conference on Security, Privacy, and Anonymity in Computation, Communication, and Storage (SpaCCS 2019)*, Atlanta, USA, July 14-17, 2019, pp. 133-146.

5. Maury, F., Reinhard, J.-R., Levillain, O., Gilbert, H. Format Oracles on OpenPGP. *Proceedings of the Cryptographer's Track at the RSA Conference 2015 (CT-RSA 2015)*. San Francisco, USA, April 20-24, 2015, pp. 220-236.

6. Ghosh, S., Kate, A. Post-Quantum Forward Secure Onion Routing (Future Anonymity in Today's Budget). *Proceedings of the 13th International Conference on Applied Cryptography and Network Security (ACNS 2015)*. New York, USA, June 2-5, 2015, pp. 263-286.

7. Campagna, M. et al. *ETSI White Paper No. 8. Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges*. European Telecommunications Standards Institute, 2015. 64 p.

8. Damgård, I., Groth, J., Salomonsen, G. The Theory and Implementation of an Electronic Voting System, Editor(s): D. Gritzalis. *Secure Electronic Voting*, Springer Publ., 2003, pp. 77-99.

9. Liu, J., Chen, L., Mesnage, S. Partially homomorphic encryption schemes over finite fields. *Proceedings of the 6th International Conference on Security, Privacy and Applied Cryptography Engineering (SPACE 2016)*. Hyderabad, India, December 14-18, 2016, pp. 109-123.

10. Vambol, A. The matrix-based knapsack cipher in the context of additively homomorphic encryption. *Proceedings of the 3rd International Conference on Computational Linguistics and Intelligent Systems (COLINS)*. Kharkiv, Ukraine, April 18-19, 2019, pp. 344-354.

11. Zhivotova, A., Zyulyarkina, N., Kostygina, Yu. Modifikatsiya kriptosistemy s otkrytym klyuchom na osnove «zadachi o ryukzake» [Modification of the cryptosystem with public key on the basis of knapsack problem]. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere* [UrFR Newsletter. Information Security], 2014, no. 1(11), pp. 16-20. (In Russian).

12. Vambol, A. The Prospects for Group-based Knapsack Ciphers in the Post-Quantum Era. *Proceedings of the 9th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT)*. Kyiv, Ukraine, May 24-27, 2018, pp. 271-275.

13. Vambol, A. Polynomial-Time Plaintext-Recovery Attack on the Matrix-Based Knapsack Cipher. *International Journal of Computing*, 2020. (Accepted for publication).

14. Roman, S. *Advanced Linear Algebra, 2nd edn*. Springer Publ., 2005. 482 p.

15. Menezes, A., van Oorschot, P., Vanstone, S. *Handbook of Applied Cryptography*. CRC Press Publ., 1996. 816 p.

16. Pohlig, S., Hellman, M. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Transactions on Information Theory*, 1978, vol. 24, no. 1, pp. 106-110.

Поступила в редакцию 30.07.2020, рассмотрена на редколлегии 15.09.2020

УСОВЕРШЕНСТВОВАННАЯ ПОЛИНОМИАЛЬНО-СЛОЖНАЯ АТАКА ВОССТАНОВЛЕНИЯ ОТКРЫТОГО ТЕКСТА НА РАНЦЕВЫЙ ШИФР НА ОСНОВЕ МАТРИЦ

А. С. Вамболь

Асимметричные шифры широко используются для обеспечения конфиденциальности передачи данных, осуществляемой с помощью незащищенных каналов. Эти криптосистемы позволяют сторонам коммуникации сформировать общий секретный ключ для симметричной схемы шифрования, не предоставляя подслушивателю информацию, полезную для криптоанализа. Протоколы сетевой безопасности, использующие асимметричные шифры, включают TLS, S/MIME, OpenPGP, Tor и многие другие. Некоторые из асимметричных схем шифрования являются гомоморфными, то есть позволяющими выполнять вычисления с зашифрованными данными без необходимости предварительного расшифрования. Указанное выше свойство делает возможным использование этих криптосистем не только для согласования симметричных ключей, но и в нескольких других областях применения, в частности в протоколах тайного голосования и облачных

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

вычислениях. Ранцевый шифр на основе матриц является новой аддитивно гомоморфной асимметричной схемой шифрования, основанной на свойствах изоморфных преобразований внутреннего прямого произведения диагональных подгрупп общей линейной группы над полем Галуа. В отличие от классических ранцевых схем шифрования, криптостойкость этого шифра зависит от вычислительной сложности задачи многомерного дискретного логарифмирования. Несмотря на ряд полезных свойств, дальнейшие исследования криптостойкости ранцевого шифра на основе матриц обнаружили серьёзные недостатки, присущие этой криптографической схеме. В данной статье предложена усовершенствованная полиномиально-сложная атака восстановления открытого текста на ранцевый шифр на основе матриц. Применение этого криптоаналитического метода требует только общедоступной информации и имеет временную сложность $O(t^{1.34})$, где t обозначает время выполнения расшифрования атакуемой криптосистемой. Вышеуказанная атака производительнее и проще в программной реализации по сравнению с оригинальной. Преимущества предложенного метода обусловлены использованием в его алгоритме простой и относительно быстрой операции вычисления следа матрицы вместо более сложных и более медленных преобразований.

Ключевые слова: ранцевый шифр на основе матриц; криптоанализ; вычислительная сложность; асимметричный шифр; гомоморфное шифрование; атака восстановления открытого текста.

IMPROVED POLYNOMIAL-TIME PLAINTEXT-RECOVERY ATTACK ON THE MATRIX-BASED KNAPSACK CIPHER

A. Vambol

Asymmetric ciphers are widely used to ensure the confidentiality of data transmission via insecure channels. These cryptosystems allow the interacting parties to create a shared secret key for a symmetric cipher in such a way that an eavesdropper gets no information useful for cryptanalysis. Network security protocols that use asymmetric ciphers include TLS, S/MIME, OpenPGP, Tor, and many others. Some of the asymmetric encryption schemes are homomorphic, that is, that they allow calculations on encrypted data to be performed without preliminary decryption. The aforesaid property makes possible using these cryptosystems not only for symmetric key establishment but also in several areas of application, in particular in secret voting protocols and cloud computing. The matrix-based knapsack cipher is a new additively homomorphic asymmetric encryption scheme, which is based on the properties of isomorphic transformations of the inner direct product of diagonal subgroups of a general linear group over a Galois field. Unlike classic knapsack encryption schemes, the cryptographic strength of this cipher depends on the computational complexity of the multidimensional discrete logarithm problem. Despite some useful properties, further research into the cryptographic strength of the matrix-based knapsack cipher has found serious drawbacks inherent in this cryptographic scheme. In the given paper an improved polynomial-time plaintext-recovery attack on the matrix-based knapsack cipher is proposed. Applying this cryptanalytic method requires only public information and has time complexity O(t1.34), where t denotes the decryption time of the attacked cryptosystem. The aforementioned attack is more productive and easier to implement in software in comparison with the original one. The advantages of the proposed method are due to using in its algorithm the simple and relatively fast matrix trace operation instead of more complex and slower transformations.

Keywords: matrix-based knapsack cipher; cryptanalysis; computational complexity; an asymmetric cipher; homomorphic encryption; plaintext-recovery attack.

Вамболь Олексій Сергійович – магістр спеціалізованих комп'ютерних систем, аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Aleksei Vambol – Master of Specialized Computer Systems, a PhD student at the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine,
e-mail: o.vambol@csn.khai.edu, ORCID Author ID: 0000-0003-1929-7783, Scopus Author ID: 57202441469, ResearcherID: X-5473-2018.