УДК 621.391

О.О. Кузнецов[1], Р.В. Корольов[1], Д.О. Медведєв[2]

[1]*Харківський університет Повітряних Сил ім. І. Кожедуба, Харків*
[2]*Дніпропетровський гірський університет, Дніпропетровськ*

ТЕОРЕТИКО-КОДОВІ СХЕМИ З ПОЛІПШЕНИМИ ХАРАКТЕРИСТИКАМИ

Розробляються теоретико-кодові схеми з поліпшеними характеристиками для забезпечення достовірності і інформаційної скритності передачі даних в АСУВ. Показано, що їх застосування дозволяє скоротити розмір необхідних ключових даних.

теоретико-кодові схеми з поліпшеними характеристиками

Вступ

Постановка проблеми в загальному вигляді та аналіз літератури. Одним з напрямів розвитку сучасної криптографії є побудова і аналіз систем шифрування з відкритим ключем. Найбільше набули популярності системи, засновані на складно вирішальних

завданнях теорії чисел: розкладанні натурального числа на прості множники і обчисленні дискретного логарифма. Однієї з альтернатив таким системам в забезпечення інформаційної скритності і достовірності передачі даних є теоретико-кодові схеми – секретні системи доказової стійкості, завдання злому яких зводиться до рішення теоретико-складної задачі декодування випадкового коду [1 – 2]. Їх практичне застосування дає можливість реалізувати в одному пристрої методи канального кодування і спеціального перетворення даних [3]. Відомі методи побудови теоретико-кодових схем мають деякі недоліки: великий об'єм ключових даних та висока, по порівнянню з блоково-симетричними кріптоалгоритмами , складність реалізації. Для усунення вказаних недоліків пропонується використовувати теоретико-кодові схеми з поліпшеними характеристиками.

Метою статті є дослідження теоретико-кодових схем з поліпшеними характеристиками , оцінка необхідних для їх функціонування об'ємів ключових даних.

1. Теоретико-кодовые схеми з поліпшеними характеристиками

Запропонована теоретико-кодова схема задається таким чином. Нехай H – перевірочна матриця лінійного (n, k, d) коду над GF(q) з поліноміальною складністю декодування з елементами $h_{i,j}\ i=0,...,n-k-1, j=0.,...,n-1$. Нехай D – діагональна матриця розміру n×n з ненульовими на діагоналі елементами, P – перестановочна матриця розміру n×n. Перестановочна матриця проводить перестановку координат вектора у вигляді матричного множення і має в кожному рядку і кожному стовпчику тільки одну одиницю. Множення

$$H_X=(H\cdot P\cdot D)=\begin{vmatrix} h_{X_{0,0}} & h_{X_{0,1}} & ... & h_{X_{0,n-1}} \\ h_{X_{1,0}} & h_{X_{1,1}} & ... & h_{X_{1,n-1}} \\ ... & ... & ... & ... \\ h_{X_{n-k-1,0}} & h_{X_{n-k-1,1}} & ... & h_{X_{n-k-1,n-1}} \end{vmatrix} \quad (1)$$

задає перевірочну матрицю замаскованого еквівалентного (n, k, d) коду над GF(q)

Із співвідношення $G_x\cdot H_X^T=0$, за допомогою рішення систем лінійних рівнянь

$$\begin{cases} h_{X_{0,0}}+h_{X_{0,k}}\cdot g_{0,k}+h_{X_{0,k-1}}\cdot g_{0,k+1}+...+h_{X_{0,k-1}}\cdot g_{0,n-k-1}=0 \\ h_{X_{0,1}}+h_{X_{0,k}}\cdot g_{1,k}+h_{X_{0,k-1}}\cdot g_{1,k+1}+...+h_{X_{0,k-1}}\cdot g_{1,n-k-1}=0 \\ ... \\ h_{X_{0,k-1}}+h_{X_{0,k}}\cdot g_{k-1,k}+h_{X_{0,k-1}}\cdot g_{k-1,k+1}+...+h_{X_{0,k-1}}\cdot g_{k-1,n-k-1}=0 \\ h_{X_{1,0}}+h_{X_{1,k}}\cdot g_{0,k}+h_{X_{1,k-1}}\cdot g_{0,k+1}+...+h_{X_{1,k-1}}\cdot g_{0,n-k-1}=0 \\ h_{X_{1,1}}+h_{X_{1,k}}\cdot g_{1,k}+h_{X_{1,k-1}}\cdot g_{1,k+1}+...+h_{X_{1,k-1}}\cdot g_{1,n-k-1}=0 \\ ... \\ h_{X_{1,k-1}}+h_{X_{1,k}}\cdot g_{k-1,k}+h_{X_{1,k-1}}\cdot g_{k-1,k+1}+...+h_{X_{1,k-1}}\cdot g_{k-1,n-k-1}=0 \\ ... \\ h_{X_{n-k-1,k-1}}+h_{X_{n-k-1,k}}\cdot g_{k-1,k}+h_{X_{n-k-1,k-1}}\cdot g_{k-1,k+1}+...+h_{X_{n-k-1,k-1}}\cdot g_{k-1,n-k-1}=0 \end{cases} \quad (2)$$

Обчислюємо породжуючу матрицю G_X виду:

$$G_X=\begin{vmatrix} 1 & 0 & ... & 0 & g_{0,k} & g_{0,k+1} & ... & g_{0,n-k-1} \\ 0 & 1 & ... & 0 & g_{1,k} & g_{1,k+1} & ... & g_{1,n-k-1} \\ ... & ... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & ... & 1 & g_{k-1,k} & g_{k-1,k+1} & ... & g_{k-1,n-k-1} \end{vmatrix}$$

Секретним (закритим) ключем є матриці P, D з елементами $p_{i,j}$ і $d_{i,j}$ відповідно, де $i,j=0,...,n-1$, відкритим ключем є підматриця правої частини матриці G_X. Закрита інформація (кодограма) представляє собою вектор довжини n і обчислюється за правилом $C_X^*=i\cdot G_X+e$, де вектор $C_X^*=\{C_0,C_2...C_{n-1}\}$ належить (n, k, d) коду з породжувальною матрицею G_x; $i=(i_0,i_1,...,i_{k-1})$ – інформаційний вектор; $e=(e_0,e_1,...,e_{n-1})$ – секретний вектор помилок ваги $w(e)\le t$. Для визначення протоколу обміну секретними повідомленнями сформуємо і доведемо наступне твердження.

Твердження $(H\cdot P\cdot D)^T=D^T\cdot P^T\cdot H^T$.

Доказ. Використовуючи правила множення матриць маємо:

$$H \cdot P \cdot D = \begin{vmatrix} h_{0,0} & h_{0,1} & \dots & h_{0,n-1} \\ h_{1,0} & h_{1,1} & \dots & h_{1,n-1} \\ \dots & \dots & \dots & \dots \\ h_{n-k-1,0} & h_{n-k-1,1} & \dots & h_{n-k-1,n-1} \end{vmatrix} \cdot \begin{vmatrix} p_{0,0} & p_{0,1} & \dots & p_{0,n-1} \\ p_{1,0} & p_{1,1} & \dots & p_{1,n-1} \\ \dots & \dots & \dots & \dots \\ p_{n-1,0} & p_{n-1,1} & \dots & p_{n-1,n-1} \end{vmatrix} \cdot \begin{vmatrix} d_{0,0} & d_{0,1} & \dots & d_{0,n-1} \\ d_{1,0} & d_{1,1} & \dots & d_{1,n-1} \\ \dots & \dots & \dots & \dots \\ d_{n-1,0} & d_{n-1,1} & \dots & d_{n-1,n-1} \end{vmatrix} =$$

$$= \begin{vmatrix} \sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} h_{0,i} \cdot p_{i,j}\right) \cdot d_{j,0} & \sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} h_{0,i} \cdot p_{i,j}\right) \cdot d_{j,1} & \dots & \sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} h_{0,i} \cdot p_{i,j}\right) \cdot d_{j,n-1} \\ \sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} h_{1,i} \cdot p_{i,j}\right) \cdot d_{j,0} & \sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} h_{1,i} \cdot p_{i,j}\right) \cdot d_{j,1} & \dots & \sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} h_{1,i} \cdot p_{i,j}\right) \cdot d_{j,n-1} \\ \dots & \dots & \dots & \dots \\ \sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} h_{n-k-1,i} \cdot p_{i,j}\right) \cdot d_{j,0} & \sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} h_{n-k-1,i} \cdot p_{i,j}\right) \cdot d_{j,1} & \dots & \sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} h_{n-k-1,i} \cdot p_{i,j}\right) \cdot d_{j,n-1} \end{vmatrix}.$$

Таким чином для довільного елементу $h_{X_{i,j}}$ матриці H_x справедливо рівність:

$$h_{X_{l,m}} = \sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} h_{l,i} \cdot p_{i,j}\right) \cdot d_{j,m}$$

Розкриємо дужки і перегрупуємо додатки, одержимо:

$$h_{X_{l,m}} = \sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} h_{l,i} \cdot p_{i,j}\right) \cdot d_{j,m} =$$

$$= \sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} h_{l,i} \cdot p_{i,j} \cdot d_{j,m}\right) = \sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1} d_{j,m} \cdot p_{i,j}\right) \cdot h_{l,i}$$

звідки, після очевидних перетворень, маємо $(H \cdot P \cdot D)^T = D^T \cdot P^T \cdot H^T$, що і завершує доказ.

Протокол обміну секретними повідомленнями полягає у виконанні наступних операцій. Абонент А випадковим, рівноімовірним і незалежним від інших абонентів чином формує матриці D, P і обчислює матриці H_x і G_x. Абонент Б для даного секретного повідомлення *i* формує шифрограму $C_x^* = i \cdot G_x^* + e$. Уповноважений абонент А, одержавши вектор C_x^*, будує вектор

$$C_x^* \cdot H_x^T = (C_x + e) \cdot H_x^T = (C_x \cdot H_x^T) + (e \cdot D \cdot P^T \cdot H^T).$$

Беручи до уваги рівняння $C_x \cdot H_x^T = 0$ останній вираз прийме вигляд

$$C_x^* \cdot H_x^T = (e \cdot D \cdot P^T \cdot H^T) = S,$$

де S – вектор синдромів, який вказує на розташування і значення ненульових елементів вектора e.

Абонент А використовуючи алгоритм поліноміальної складності декодує вектор C_x^*, тобто виконує обчислення $e' = e \cdot P^T \cdot D^T$, і обчислює k-розрядний інформаційний вектор C_x. Для уповноваженого користувача (абонента А) декодування – поліноміально вирішальне завдання (при декодуванні алгоритмом Берлекемпа поліноміальна складність – $(d/2)^2$), а для зловмисника, що не знає матриць P, D, декодування випадкового коду великої довжини обчислювально недосяжно (при кореляційному декодуванні експоненціальна складність – q^k).

2. Порівняльна оцінка об'ємів необхідних ключових даних

Оцінимо об'єм ключових даних несиметричних теоретико-кодових схем Мак-Еліса і запропонованої теоретико-кодової схеми. Об'єм відкритого ключа схеми Мак-Еліса (у бітах) визначається сумою елементів породжувальної матриці, як елементів поля $GF(2^a)$, і задається виразом $L_1 = n \cdot k \cdot a$, для запропонованої схеми об'єм ключа визначається невідомими в системі (2), тобто $L_2 = (n-k) \cdot k \cdot a$.

Висновок

Таким чином, розроблені теоретико-кодові схеми мають поліпшені властивості, для їх функціонування необхідно зберігати відкритий ключ об'ємом $\frac{n \cdot k \cdot a}{(n-k) \cdot k \cdot a} = \frac{n}{n-k}$ раз меншим, ніж у класичній теоретико-кодовій схемі Мак-Еліса.

Список літератури

1. R.J. McEliece. A Public-Key Criptosystem Based on Algebraic Theory // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114-116.

2. Сидельников В.М. Криптография и теория кодирования // Мат-лы конф. Московский университет и развитие криптографии в России. – М.: МГУ. – 2002. – 22 с.

3. Стасев Ю.В., Кузнецов А.А. Кибернетика и системный анализ // Международный научно-теоретический журнал. – К.: НАНУ. – 2005. – №3. – С. 47-57.

Надійшла до редколегії 17.09.2007

Рецензент: д-р техн. наук, проф. Ю.В. Стасєв, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.