ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

УКРАЇНА

(19) UA (11) 62306 (13) U

(51) МПК (2011.01)
H03M 13/00

ОПИС
ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під відповідальність власника патенту

(54) СПОСІБ ПОЄДНАННЯ ЗАВАДОСТІЙКОГО КОДУВАННЯ ДИСКРЕТНОЇ ІНФОРМАЦІЇ І ПОТОКОВОГО ШИФРУВАННЯ ІЗ СЕАНСОВИМ КЛЮЧЕМ

(21) u201100690
(22) 21.01.2011
(24) 25.08.2011
(46) 25.08.2011, Бюл.№ 16, 2011 р.
(72) СЕМЕРЕНКО ВАСИЛЬ ПЕТРОВИЧ, ДУБРОВ ОЛЕКСАНДР ФЕДОРОВИЧ
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(57) Спосіб поєднання завадостійкого кодування дискретної інформації і потокового шифрування із сеансовим ключем, в якому на боці передавача кодують k-розрядні інформаційні вектори множенням на k-розрядний породжувальний поліном циклічного k-коду і шифрують їх, а на боці приймача дешифрують отримані з каналу зв'язку n-розрядні кодові вектори і декодують їх діленням на $(n-k)$-розрядний породжувальний поліном циклічного (n,k)-коду, який **відрізняється** тим, що на боці передавача після кодування шифрують $(l-m)$-розрядні кодові вектори приєднанням до них $(l-m)$-розрядного сеансового ключа і подальшим діленням на $(l-m)$-розрядний породжувальний поліном циклічного (l,m)-коду $(l-m \geq n)$, а на боці приймача дешифрують $(l-m)$-розрядні кодові вектори порозрядним модульним додаванням $(l-m)$-розрядного вектора паролю, який обчислюється як $(m-1)$-а остача від ділення зсунутого на $(l-m)$ розрядів вліво сеансового ключа на $(l-m)$-розрядний породжувальний поліном циклічного (l,m)-коду, причому для кожного кодового вектора використовується свій сеансовий ключ, який обчислюється почерговим діленням заданого секретного базового ключа на $(l-m)$-розрядний породжувальний поліном циклічного (l,m)-коду і його подальшим нелінійним перетворенням.

Корисна модель належить до техніки передавання даних і може бути використана в інформаційно-вимірювальних системах, комп'ютерних мережах та в засобах шифрування даних.

Відомий спосіб стохастичного кодування з виправленням помилок і захистом інформації при передачі даних по каналах зв'язку. Цей спосіб включає в себе власне кодування і декодування, а також і стохастичне перетворення на основі псевдовипадкових чисел. [Осмоловский С. А. Стохастические методы защиты информации. М.: Радио и связь, 2003].

Недоліком відомого способу є те, що операції кодування і декодування виконуються окремо від операцій шифрування і дешифрування, що вимагає великих витрат часу для передачі даних і не дозволяє його ефективне використання в системах реального часу.

Найбільш близьким по технічній суті є спосіб завадостійкого кодування дискретної інформації із захистом [Патент України на корисну модель № 50203 М. кл., H03M13/00, Бюл. № 10, 2010], в якому на боці передавача кодують k-розрядні інформаційні вектори множенням на $(n-k)$-розрядний породжувальний поліном циклічного (n,k)-коду і шифрують їх, а на боці приймача декодують отримані з каналу зв'язку n-розрядні кодові вектори діленням на $(n-k)$-розрядний породжувальний поліном циклічного (n,k)-коду, і дешифрують їх, після кодування шифрують n-розрядні кодові вектори порозрядним додаванням по модулю два до них секретного n-розрядного вектора паролю, а перед декодуванням дешифрують порозрядним додаванням по модулю два до отриманих з каналу зв'язку n-розрядних кодових векторів цього ж n-розрядного вектора паролю.

Недоліком цього способу є низька криптостійкість через використання одного пароля протягом всього процесу передавання даних, а також вико-

(19) UA (11) 62306 (13) U

ристання тільки лінійних перетворень при обчисленні паролю.

В основу корисної моделі поставлена задача створення способу поєднання завадостійкого кодування дискретної інформації і потокового шифрування із сеансовим ключем, в якому за рахунок використання для шифрування кожного кодового вектора свого сеансового ключа, який обчислюється на основі лінійних операцій із заданим секретним базовим ключем і його подальшим нелінійним перетворенням, в результаті чого зберігається початкова завадостійкість кодування, збільшується ступінь захисту, зменшуються загальні витрати часу на виконання операцій декодування і дешифрування.

Поставлена задача вирішується тим, що в способі поєднання завадостійкого кодування дискретної інформації і потокового шифрування із сеансовим ключем, в якому на боці передавача кодують k-розрядні інформаційні вектори множенням на $(n-k)$-розрядний породжувальний поліном циклічного (n,k)-коду і шифрують їх, а на боці приймача дешифрують отримані з каналу зв'язку n-розрядні кодові вектори і декодують їх діленням на $(n-k)$-розрядний породжувальний поліном циклічного (n,k)-коду, причому на боці передавача після кодування шифрують $(l-m)$-розрядні кодові вектори приєднанням до них $(l-m)$-розрядного сеансового ключа і подальшим діленням на $(l-m)$-розрядний породжувальний поліном циклічного (l,m)-коду $(l-m\geq n)$, а на боці приймача дешифрують $(l-m)$-розрядні кодові вектори порозрядним модульним додаванням $(l-m)$-розрядного вектора паролю, який обчислюють як $(m-1)$-а остачу від ділення зсунутого на $(l-m)$ розрядів вліво сеансового ключа на $(l-m)$-розрядний породжувальний поліном циклічного (l,m)-коду, причому для кожного кодового вектора використовують свій сеансовий ключ, який обчислюють почерговим діленням заданого секретного базового ключа на $(l-m)$-розрядний породжувальний поліном циклічного (l,m)-коду і його подальшим нелінійним перетворенням.

Спосіб здійснюється наступним чином. Спочатку на боці передавача виконують завадостійке кодування заданих інформаційних векторів $I(x)$ за допомогою циклічного (n,k)-коду над полем Галуа GF(2) з мінімальною кодовою відстанню d_{min}, який задають $(n-k)$-розрядним породжувальним поліномом

$$g(x)=g_r x^r+g_{r-1}x^{r-1}+\ldots+g_1x+g_0, r=n-k.$$

Для завадостійкого кодування використовують несистематичне кодування циклічних кодів, тобто для отримання n-розрядного кодового вектора $C(x)$ необхідно протягом n тактів часу заданий k-розрядний інформаційний вектор $I(x)$ перемножити на породжувальний поліном $g(x)$:

$$C(x)=I(x)\times g(x), \quad (1)$$

Перевагою несистематичного кодування в циклічних кодах є нероздільність інформаційних і контрольних розрядів, що забезпечує одночасно і першу ступінь захисту даних в каналі зв'язку.

Подальший захист даних забезпечують завдяки їх наступному шифруванню. Для цього задають $(l-m)$-розрядний базовий ключ K_b, який залишають незмінним протягом всього інтервалу часу передачі масиву кодових векторів $(l-m\geq n)$. Для передачі кожного окремого кодового вектора $C_i(x)$ обчислюють свій сеансовий ключ $K_{S,i}$ за допомогою циклічного (l,m)-коду над полем Галуа GF(2), який задають $(l-m)$-розрядним породжувальним поліномом

$$h(x)=h_r x^r+h_{r-1}x^{r-1}+\ldots+hx+h_0, r=l-m.$$

Сеансовий ключ $K_{S,i}$ формують за два етапи: лінійний та нелінійний. На першому етапі для i-го сеансу обчислюють лінійний сеансовий ключ $K_{lin\,i}$ як i-а остачу від модульного ділення над полем Галуа GF(2) базового ключа K_b на породжувальний поліном $h(x)$ циклічного (l,m)-коду:

$$K_{lin\,i}=\left(K_b x^i\right)\bmod(h(x)), \quad (2)$$

На другому етапі для i-го сеансу обчислюють нелінійний сеансовий ключ $K_{S,i}$ як результат перетворення лінійного сеансового ключа $K_{lin\,i}$ за допомогою булевої нелінійної функції $\varphi(\,)$:

$$K_{S,i}=\varphi\left(K_{lin\,i}^{(i)}\right), \quad (3)$$

Прикладом булевої нелінійної функції можуть бути бент-функції. Лінійний та нелінійний етапи обчислення сеансового ключа $K_{S,i}$ забезпечують відповідно другий та третій ступені захисту даних і тривають по одному такту часу.

Зашифрований $(l-m)$-розрядний кодовий вектор $T_i(x)$ формують як $(l-m-1)$-а остачу від модульного ділення над полем Галуа GF(2) сеансового ключа $K_{S,i}$ і приєднаного до нього кодового вектора $C_i(x)$ на породжувальний поліном $h(x)$ циклічного (l,m)-коду:

$$T_i(x)=\left(K_{S,i}x^{l-m}+C_i(x)\right)\bmod(h(x)), \quad (4)$$

Процес шифрування кодового вектора відбувається одночасно із його кодуванням, з затримкою лише на один такт. Далі кодовий вектор $T_i(x)$ передають по каналу зв'язку.

На боці приймача отриманий із каналу зв'язку вектор $T_{ch,i}(x)$ спочатку дешифрують, тобто з нього виділяють кодовий вектор $C_{ch,i}(x)$. Для цього на стороні приймача спочатку формують такий же нелінійний сеансовий ключ $K_{S,i}$, як і на стороні передавача.

Далі формують $(l-m)$-розрядний сеансовий пароль $P_{S,i}$ як $(l-m-1)$-а остачу від модульного ділення над полем Галуа GF(2) зсунутого на $(l-m)$ розрядів вліво нелінійного сеансового ключа $K_{S,i}$ на породжувальний поліном $h(x)$ циклічного (l,m)-коду:

$$P_{S,i} = \left(K_{S,i}x^{l-m}\right) \bmod (h(x)), \quad (5)$$

Формування сеансового паролю $P_{S,i}$ відбувається протягом такого інтервалу часу, поки триває передача кодового вектора $T_i(x)$ по каналу зв'язку.

Дешифрування полягає в модульному порозрядному додаванню над полем Галуа GF(2) сформованого сеансового паролю $P_{S,i}$ до отриманого із каналу зв'язку кодового вектора $T_{ch,i}(x)$, в результаті чого буде отримано кодовий вектор $C_{ch,i}(x)$:

$$C_{ch,i}(x) = T_{ch,i}(x) + P_{S,i}(x), \quad (6)$$

При декодуванні із кодового вектора $C_{ch,i}(x)$ виділяється початковий інформаційний вектор $I(x)$ модульним діленням кодового вектора $C_{ch,i}(x)$ на породжувальний поліном $g(x)$:

$$I_i(x) = \frac{C_{ch,i}(x)}{g(x)} + R_i(x), \quad (7)$$

Якщо в результаті ділення (4) буде отримано нульовий вектор синдрому $R(x)$, це буде свідчити, що передача даних по каналу зв'язку виконана без τ_{min} помилок $\left(\tau_{min} = \frac{d_{min}-1}{2}\right)$, тобто $C_{ch,i}(x) = C_i(x)$. При отриманні ненульового вектора синдрому $R(x)$ далі виконують процедуру пошуку помилок в кодовому векторі в межах коректуючої здатності вибраного коду.

Основну роль в захисті даних відіграє секретний базовий ключ K_b і ступінь криптостійкості залежить від величини його розрядності. Оскільки $(l-m)$-розрядний вектор ключа K_b може бути довільним, існує 2^{l-m} варіантів такого вибору.

Розрядність ключа K_b визначають розрядністю породжувального полінома циклічного (l,m)-коду, що використовують для шифрування. Тому вказаний поліном має бути примітивним і максимально можливої розрядності, що зробить випадковий підбір ключа K_b практично неможливим.

У запропонованому способі поєднання завадостійкого кодування дискретної інформації і потокового шифрування із сеансовим ключем підвищується криптостійкість завдяки тому, що використовується триступенева система захисту і при обчисленні сеансового паролю $P_{S,i}$ використовуються лінійні та нелінійні перетворення.

Оскільки сеансовий вектор паролю $P_{S,i}$ змінюється для кожного нового кодового вектора $C_i(x)$, тому неможливо розшифрувати весь масив кодових векторів навіть тоді, коли буде одночасно відома деяка кількість зашифрованих та відкритих кодових векторів.

Розглянемо спосіб поєднання завадостійкого кодування дискретної інформації і потокового шифрування із сеансовим ключем на прикладі циклічного (7,4)-коду з породжувальним поліномом $g(x) = x^3 + x + 1$ та циклічного (255,247)-коду з породжувальним поліномом $p(x) = x^8 + x^6 + x^5 + x^4 + 1 (n = 7, l = 255, m = 247)$.

Нехай задано 4-розрядний інформаційний вектор $I_1(x) = x^3 + x^2 + x = 1110$. Виконаємо несистематичне кодування для отримання 7-розрядного кодового вектора $C_1(x)$ згідно з (1) використанням породжувального полінома $g(x)$:

$$C_1(x) = \left(x^3 + x^2 + x\right) \times \left(x^3 + x + 1\right) = x^6 + x^5 + x = 1100010, \quad (8)$$

Для криптографічного захисту задано 8-розрядний $(m = 8)$ базовий ключ $K_b = x^7 + x^4 + x + 1 = 10010011$. Згідно з (2) знайдемо першу остачу від модульного ділення над полем Галуа GF(2) на породжувальний поліном $h(x)$, тобто обчислимо для першого сеансу лінійний сеансовий ключ $K_{lin\,i}$:

$$\left(\left(x^7+x^4+x+1\right)x\right)\bmod\left(x^8+x^6+x^5+x^4+1\right)=\frac{x^8+0+0+x^5+0+0x^2+x+0\,\big|\,x^8+x^6+x^5+x^4+1}{x^8+0+x^6+x^5+x^4+0+0+0+1\qquad 1}.$$

Отже, $K_{lin1}=x^6+x^4+x^2+x+1=01010111$. Для формування нелінійного сеансового ключа $K_{s,1}$ скористаємось такою булевою нелінійною функцією $\varphi()$:

$$\varphi(a)=a_j\,\&\,a_{j-1}\vee a_{j-2},\quad j=0,1,\ldots,n_2-1, \qquad (9)$$

де a_j - j -й розряд ключа $K_{lin1}, a_{-1}=a_{-2}=0$.

Результати перетворення лінійного сеансового ключа K_{lin1} за допомогою булевої нелінійної функції (9) подамо у вигляді таблиці.

Таблиця

Формування розрядів нелінійного сеансового ключа $K_{s,1}$

№	Розряди ключа K_{lin1}	Розряди ключа $K_{s,1}$
0	1	$1\&0\vee0=0$
1	1	$1\&1\vee0=1$
2	1	$1\&1\vee1=0$
3	0	$0\&1\vee1=1$
4	1	$1\&0\vee1=1$
5	0	$0\&1\vee0=0$
6	1	$1\&0\vee1=1$
7	0	$0\&1\vee0=0$

Отже, таким чином ми отримали нелінійний сеансовий ключ

$$K_{s,1}=x^6+x^4+x^3+x=01011010, \qquad (10)$$

Тепер за допомогою ключа (10) можна зашифрувати кодовий вектор (8) і отримати 8-розрядний кодовий вектор $T_1(x)$ згідно з (4). Спочатку приєднаємо до ключа (10) кодовий вектор (8):

$$\left(x^6+x^4+x^3+x\right)x^8+x^6+x^5+x=x^{14}+x^{12}+x^{11}+x^9+x^6+x^5+x=1011010011\,00010.$$

Далі необхідно виконати обчислення

$$\left(x^{14}+x^{12}+x^{11}+x^9+x^6+x^5+x\right)=\bmod\left(x^8+x^6+x^5+x^4+1\right).$$

В результаті ділення цих поліномів буде отримана остача, яка і являє собою зашифрований кодовий вектор:

$$T_1(x)=x^6+x^5+x^4+x^2+1=01110101.$$

На боці приймача для розшифрування потрібно спочатку сформувати нелінійний сеансовий ключ $K_{s,i}$, аналогічно, як на боці передавача, а потім - 8-розрядний сеансовий пароль $P_{s,1}$ згідно з (5).

В даному випадку необхідно виконати такі обчислення:

$$\left(\left(x^6+x^4+x^3+x\right)x^8\right)\bmod\left(x^8+x^6+x^5+x^4+1\right)=\left(x^{14}+x^{12}+x^{11}+x^9\right)\bmod\left(x^8+x^6+x^5+x^4+1\right).$$

В результаті ділення цих поліномів буде отримана остача, яка і являє собою зашифрований сеансовий пароль:

$$P_{s,1}(x)=x^4+x^2+x+1=00010111.$$

Виконаємо дешифрування кодового вектора згідно з (6):

$$C_{ch,1}(x)=T_{ch,1}(x)\oplus P_{s,,1}(x)=x^6+x^5+x=$$
$$=1100010.$$

Згідно з (7), при декодуванні із кодового вектора $C_{ch,i}(x)$ виділяється інформаційний вектор $I_1(x)$ діленням кодового вектора $C_{ch,i}(x)$ на породжувальний поліном $g(x)$:

$$I_1(x) = \frac{x^6 + x^5 + x}{x^3 + x + 1} = x^3 + x^2 + x = 1110, \quad (11)$$

Оскільки в результаті ділення (11) отримана нульова остача, тобто отримано нульовий вектор синдрому $R_i(x)$, це свідчить, що передача даних по каналу зв'язку виконана без τ_{min} помилок, тобто $C_{ch}(x) = C(x)$ і отримано початковий інформаційний вектор $I_1(x)$.

Комп'ютерна верстка Л. Ціхановська Підписне Тираж 23 прим.

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601