УДК 004.056.55:004.312.2

В.Г. Бабенко[1], О.Г. Мельник[2], О.Б. Нестеренко[2]

[1] *Черкаський державний технологічний університет, Черкаси*
[2] *Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України, Черкаси*

МОДЕЛЮВАННЯ ПРИМІТИВІВ КОВЗНОГО ШИФРУВАННЯ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

У даній статті синтезовано математичні моделі матричних операцій багаторазового перетворення на основі примітива ковзного шифрування. На основі використання одержаних рекурентних залежностей, які описують моделі багаторазового виконання примітива ковзного шифрування, побудовано узагальнену рекурентну модель процесу виконання багаторазового примітива ковзного шифрування для перетворення n -елементів. Використовуючи синтезовані на основі рекурентних залежностей математичні моделі чотири-, п'яти- та шестиелементного прямого правостороннього примітиву ковзного шифрування, одержано узагальнений вираз рекурентної послідовності для опису k-разового виконання примітиву ковзного шифрування при заданій кількості елементів. У роботі запропоновано підхід щодо математичного опису на основі рекурентних послідовностей моделей операцій перетворення на основі багаторазового застосування примітиву ковзного шифрування при обмеженій кількості елементів.

Ключові слова: *рекурентна послідовність, узагальнена рекурентна модель, криптографічне перетворення, система рівнянь, математична модель, багаторазове ковзне шифрування, примітив ковзного шифрування.*

Вступ

Актуальність проблеми. Сьогодні інформацію розглядають як один з основних ресурсів розвитку суспільства, а інформаційні системи і технології як засіб підвищення продуктивності та ефективності його діяльності. Інформаційна технологія визначає процеси передачі та розповсюдження, зберігання і обробки інформації, її використання з певною метою. Всі ці процеси повинні бути максимально швидкими, найменш витратними, максимально корисними, зручними, автоматизованими та водночас захищеними.

Цінність інформації визначає рівень її захисту, який потрібно забезпечити. Сучасні інформаційні технології потребують організації високого рівня захисту великого об'єму даних. Стратегічно правильним підходом щодо вирішення проблеми захисту інформації є використання досягнень криптографії, зокрема побудови систем захисту на основі операцій матричного криптографічного перетворення з можливістю їх паралельної реалізації.

Аналіз останніх досліджень і публікацій. У статтях [1, 2] наведено опис використання примітивів ковзного шифрування для симетричних блочних криптографічних алгоритмів, але, як було доведено у роботі [3], основним їх недоліком є послідовна реалізація.

У науковій роботі [3] показано, що процес реалізації примітива ковзного шифрування може бути розпаралелений за рахунок використання матричних операцій криптографічного перетворення інформації.

У статті [4] запропоновано один із способів оптимізації матричних операцій ковзного шифрування, що дозволяє зменшити апаратну складність реалізації примітивів ковзного шифрування за рахунок скорочення кількості операцій додавання за модулем два.

У роботі [5] доведено, що використання матричних операцій криптографічного перетворення, синтезованих на основі додавання за модулем два, може бути використане для підвищення криптостійкості.

Але в даних дослідженнях ковзне шифрування не достатньо вивчено для проведення багаторазових перетворень на його основі.

Формулювання мети статті. Мета роботи – побудувати моделі примітивів багаторазового ковзного щифрування для заданої кількості елементів примітиву на основі використання рекурентних залежностей.

Виклад основного матеріалу

Отримати рекурентну залежність для багаторазового ковзного шифрування виявилося достатньо складно, особливо при її визначенні для невеликої розрядності перетворення. Отримаємо рекурентні послідовності для опису матричних операцій багаторазового перетворення на основі примітива ковзного шифрування.

Нехай y_i^k – умовне позначення одного елемента примітива багаторазового ковзного шифрування, x_i – елементи вхідної інформації, де i – порядковий номер елемента, а k – кількість разів (етапів, раундів) зашифрування.

Тоді система рівнянь для виконання примітива ковзного шифрування на першому (початковому) етапі перетворення запишеться як:

$$
\begin{aligned}
y_1^1 &= y_0^1 \oplus x_1;\\
y_2^1 &= y_1^1 \oplus x_2;\\
y_3^1 &= y_2^1 \oplus x_3;\\
y_4^1 &= y_3^1 \oplus x_4;\\
y_5^1 &= y_4^1 \oplus x_5;\\
&\ldots\ldots,
\end{aligned}
$$

де $\oplus$ - операція додавання за модулем два.

Звідси отримаємо рекурентну послідовність, що описує процес виконання примітива ковзного шифрування:

$$y_i^1 = y_{i-1}^1 \oplus x_i, \qquad (1)$$

де $y_0^1 = m_1$, а m_1 - ключовий елемент першого раунду.

Система рівнянь для здійснення криптографічного перетворення інформації на основі дворазового виконання примітива ковзного шифрування має вигляд:

$$
\begin{aligned}
y_1^2 &= y_0^2 \oplus y_1^1;\\
y_2^2 &= y_1^2 \oplus y_2^1;\\
y_3^2 &= y_2^2 \oplus y_3^1;\\
y_4^2 &= y_3^2 \oplus y_4^1;\\
y_5^2 &= y_4^2 \oplus y_5^1;\\
&\ldots\ldots
\end{aligned}
$$

Звідси отримано рекурентну залежність між елементами примітива ковзного шифрування:

$$y_i^2 = y_{i-1}^2 \oplus y_i^1, \qquad 2)$$

де $y_0^2 = m_2$, а m_2 - ключовий елемент другого раунду.

Система рівнянь для триразового виконання примітива ковзного шифрування запишеться:

$$
\begin{aligned}
y_1^3 &= y_0^3 \oplus y_1^2;\\
y_2^3 &= y_1^3 \oplus y_2^2;\\
y_3^3 &= y_2^3 \oplus y_3^2;\\
y_4^3 &= y_3^3 \oplus y_4^2;\\
y_5^3 &= y_4^3 \oplus y_5^2;\\
&\ldots\ldots
\end{aligned}
$$

Звідси отримаємо рекурентну послідовність, що описує процес виконання триразового примітива ковзного шифрування:

$$y_i^3 = y_{i-1}^3 \oplus y_i^2, \qquad (3)$$

де $y_0^3 = m_3$, а m_3 - ключовий елемент третього раунду.

Чотириразове виконання примітива ковзного шифрування описується системою рівнянь:

$$
\begin{aligned}
y_1^4 &= y_0^4 \oplus y_1^3;\\
y_2^4 &= y_1^4 \oplus y_2^3;\\
y_3^4 &= y_2^4 \oplus y_3^3;\\
y_4^4 &= y_3^4 \oplus y_4^3;\\
y_5^4 &= y_4^4 \oplus y_5^3;\\
&\ldots\ldots
\end{aligned}
$$

Рекурентна послідовність, що описує процес чотириразового виконання примітива ковзного шифрування, описується як:

$$y_i^4 = y_{i-1}^4 \oplus y_i^3, \qquad (4)$$

де $y_0^4 = m_4$, а m_4 - ключовий елемент четвертого раунду.

Таким чином, на основі описаних моделей багаторазового виконання примітива ковзного шифрування, що описуються рекурентними залежностями (1)–(4), отримаємо узагальнену рекурентну модель процесу виконання багаторазового примітива ковзного шифрування для перетворення n-елементів:

$$y_i^k = y_{i-1}^k \oplus y_i^{k-1}, \qquad (5)$$

де $y_0^k = m_k$, де m_k - ключовий елемент k-того раунду.

Використаємо запропонований підхід до математичного опису на основі рекурентних послідовностей для моделювання операцій перетворення на основі багаторазового застосування примітиву ковзного шифрування при обмеженій кількості елементів.

Особливістю реалізації даного ковзного шифрування є те, що в якості вхідного раундового ключа використовується вихідний раундовий ключ попереднього етапу перетворення, який, в свою чергу, дорівняє значенню останнього порядкового елементу примітиву ковзного шифрування.

Система лінійних модульних алгебраїчних рівнянь, що описує реалізацію примітива чотириелементного прямого правостороннього ковзного шифрування (ПКШ), описується як:

$$
\begin{aligned}
y_1 &= x_1 \oplus m_1;\\
y_2 &= x_2 \oplus y_1;\\
y_3 &= x_3 \oplus y_2;\\
y_4 &= x_4 \oplus y_3,
\end{aligned}
\qquad (6)
$$

де m_1 – вхідний раундовий ключ, а $y_4 = m_2$ – вихідний раундовий ключ, що використовується в якості вхідного для наступного блока даних, що перетворюється.

Розглянемо матричну модель операції ковзного шифрування (6) у розвернутому вигляді.

Операція чотириелементного прямого ПКШ перетворює послідовність x_i у y_i, $i = 1..4$, тоді:

$$\begin{aligned} y_1 &= x_1 \oplus m_1; \\ y_2 &= x_1 \oplus x_2 \oplus m_1; \\ y_3 &= x_1 \oplus x_2 \oplus x_3 \oplus m_1; \\ y_4 &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus m_1. \end{aligned} \quad (7)$$

Рекурентна послідовність, яка описує операцію чотириелементного прямого ПКШ, має вигляд:

$$y_i^1 = y_{i-1}^1 \oplus x_i, \quad (8)$$

де $y_0^1 = m_1$ та $i \in \{1, \dots, 4\}$.

Повторне чотириелементне ковзне шифрування перетворює послідовність y_i у z_i:

$$\begin{aligned} z_1 &= y_1 \oplus m_2; \\ z_2 &= y_2 \oplus z_1; \\ z_3 &= y_3 \oplus z_2; \\ z_4 &= y_4 \oplus z_3 \end{aligned}$$

або

$$\begin{aligned} z_1 &= y_1 \oplus m_2; \\ z_2 &= y_1 \oplus y_2 \oplus m_2; \\ z_3 &= y_1 \oplus y_2 \oplus y_3 \oplus m_2; \\ z_4 &= y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus m_2, \end{aligned} \quad (9)$$

де m_2 – вхідний раундовий ключ і $m_2 = y_4$.

Підставивши у вираз (9) вираз (7), отримаємо:

$$\begin{aligned} z_1 &= (x_1 \oplus m_1) \oplus m_2; \\ z_2 &= (x_1 \oplus m_1) \oplus (x_1 \oplus x_2 \oplus m_1) \oplus m_2; \\ z_3 &= (x_1 \oplus m_1) \oplus (x_1 \oplus x_2 \oplus m_1) \oplus \\ &\quad \oplus (x_1 \oplus x_2 \oplus x_3 \oplus m_1) \oplus m_2; \\ z_4 &= (x_1 \oplus m_1) \oplus (x_1 \oplus x_2 \oplus m_1) \oplus \\ &\quad \oplus (x_1 \oplus x_2 \oplus x_3 \oplus m_1) \oplus \\ &\quad \oplus (x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus m_1) \oplus m_2. \end{aligned}$$

Здійснивши відповідні перетворення за умови, що $m_2 = y_4$, отримаємо:

$$\begin{aligned} z_1 &= x_4 \oplus x_3 \oplus x_2; \\ z_2 &= x_4 \oplus x_3 \oplus x_1 \oplus m_1; \\ z_3 &= x_4 \oplus x_2; \\ z_4 &= x_3 \oplus x_1 \oplus m_1. \end{aligned} \quad (10)$$

Рекурентна послідовність, яка описує операцію повторного (дворазового $k = 2$) чотириелементного прямого ПКШ, має вигляд:

$$y_i^2 = y_{i-1}^2 \oplus y_i^1, \quad (11)$$

де $y_0^2 = y_4^1$, а $i \in \{1, \dots, 4\}$.

Триразове чотириелементне ковзне шифрування перетворює послідовність z_i у l_i:

$$\begin{aligned} l_1 &= z_1 \oplus m_3; \\ l_2 &= z_1 \oplus z_2 \oplus m_3; \\ l_3 &= z_1 \oplus z_2 \oplus z_3 \oplus m_3; \\ l_4 &= z_1 \oplus z_2 \oplus z_3 \oplus z_4 \oplus m_3. \end{aligned} \quad (12)$$

де $m_3 = z_4$ – вхідний раундовий ключ даного етапу шифрування.

Підставимо у вираз (12) вираз (10), та, провівши скорочення змінних, отримаємо:

$$\begin{aligned} l_1 &= x_1 \oplus x_2 \oplus x_4 \oplus m_1; \\ l_2 &= x_2 \oplus x_3; \\ l_3 &= x_3 \oplus x_4; \\ l_4 &= x_1 \oplus x_4 \oplus m_1. \end{aligned} \quad (13)$$

Рекурентна послідовність, яка описує операцію триразового ($k = 3$) чотириелементного прямого ПКШ, має вигляд:

$$y_i^3 = y_{i-1}^3 \oplus y_i^2, \quad (14)$$

де $y_0^3 = y_4^2$, а $i \in \{1, \dots, 4\}$.

Отримаємо матричну модель для опису операції чотириразового чотириелементного ковзного шифрування. Чотириразове чотириелементне ковзне шифрування перетворює послідовність l_i у j_i:

$$\begin{aligned} j_1 &= l_1 \oplus m_4; \\ j_2 &= l_1 \oplus l_2 \oplus m_4; \\ j_3 &= l_1 \oplus l_2 \oplus l_3 \oplus m_4; \\ j_4 &= l_1 \oplus l_2 \oplus l_3 \oplus l_4 \oplus m_4, \end{aligned} \quad (15)$$

де $m_4 = l_4$ – вхідний раундовий ключ даного етапу шифрування.

Підставивши у вираз (15) вираз (13), отримаємо:

$$\begin{aligned} j_1 &= x_2; \\ j_2 &= x_3; \\ j_3 &= x_4; \\ j_4 &= x_1 \oplus m_1. \end{aligned}$$

Рекурентна послідовність, яка описує операцію чотириразового ($k = 4$) чотириелементного прямого ПКШ, має вигляд:

$$y_i^4 = y_{i-1}^4 \oplus y_i^3, \quad (16)$$

де $y_0^4 = y_4^3$, а $i \in \{1, \dots, 4\}$.

Операція п'ятиелементного прямого ПКШ перетворює послідовність x_i у y_i, $i = 1..5$.

Рекурентна послідовність, яка описує операцію п'ятиелементного прямого ПКШ, має вигляд:

$$y_i^1 = y_{i-1}^1 \oplus x_i, \quad (17)$$

де $y_0^1 = m_1$, а $i \in \{1, \dots, 5\}$.

Повторне п'ятиелементне ковзне шифрування перетворює послідовність y_i у z_i за умови, що

m_2 – вхідний раундовий ключ і $m_2 = y_5$. Підставивши відповідні вирази, отримаємо:

$$z_1 = x_2 \oplus x_3 \oplus x_4 \oplus x_5;$$
$$z_2 = x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus m_1;$$
$$z_3 = x_2 \oplus x_4 \oplus x_5;$$
$$z_4 = x_1 \oplus x_3 \oplus x_5 \oplus m_1;$$
$$z_5 = x_2 \oplus x_4.$$

Рекурентна послідовність, яка описує операцію дворазового п'ятиелементного прямого ПКШ, має вигляд:

$$y_i^2 = y_{i-1}^2 \oplus y_i^1, \qquad (18)$$

де $y_0^2 = y_5^1$, а $i \in \{1, \dots, 5\}$.

Отримаємо матричну модель для опису триразового застосування п'ятиелементного примітиву ковзного шифрування.

Триразове п'ятиелементне ковзне шифрування перетворює послідовність z_i у l_i за умови, що $m_3 = z_5$ – це вхідний раундовий ключ даного етапу шифрування, та описується моделлю:

$$l_1 = x_1 \oplus x_3;$$
$$l_2 = x_1 \oplus x_4 \oplus m_1;$$
$$l_3 = x_1 \oplus x_2 \oplus x_5 \oplus m_1;$$
$$l_4 = x_1 \oplus x_2 \oplus x_3 \oplus x_5;$$
$$l_5 = x_3 \oplus x_4.$$

Рекурентна послідовність, яка описує операцію триразового п'ятиелементного прямого ПКШ, має вигляд:

$$y_i^3 = y_{i-1}^3 \oplus y_i^2, \qquad (19)$$

де $y_0^3 = y_5^2$, а $i \in \{1, \dots, 5\}$.

Чотириразове п'ятиелементне ковзне шифрування перетворює послідовність l_i у j_i, де $m_4 = l_5$ – вхідний раундовий ключ даного етапу шифрування. Підставивши відповідні вирази, отримаємо:

$$j_1 = x_2 \oplus x_4;$$
$$j_2 = m_1;$$
$$j_3 = x_1 \oplus x_2 \oplus x_5;$$
$$j_4 = x_3;$$
$$j_5 = x_4.$$

Рекурентна послідовність, яка описує операцію чотириразового п'ятиелементного прямого ПКШ, має вигляд:

$$y_i^4 = y_{i-1}^4 \oplus y_i^3, \qquad (20)$$

де $y_0^4 = y_5^3$, а $i \in \{1, \dots, 5\}$.

Операція шестиелементного прямого правостороннього ковзного шифрування перетворює послідовність x_i у y_i, $i = 1..6$.

Рекурентна послідовність, яка описує операцію шестиелементного прямого правостороннього ковзного шифрування, має вигляд:

$$y_i^1 = y_{i-1}^1 \oplus x_i, \qquad (21)$$

де $y_0^1 = m_1$, а $i \in \{1, \dots, 6\}$.

Повторне шестиелементне ковзне шифрування перетворює послідовність y_i в z_i за умови, що m_2 – вхідний раундовий ключ і

$$m_2 = y_6.$$

Підставивши відповідні вирази, отримаємо:

$$z_1 = x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6;$$
$$z_2 = x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus m_1;$$
$$z_3 = x_2 \oplus x_4 \oplus x_5 \oplus x_6;$$
$$z_4 = x_1 \oplus x_3 \oplus x_5 \oplus x_6 \oplus m_1;$$
$$z_5 = x_2 \oplus x_4 \oplus x_6;$$
$$z_6 = x_1 \oplus x_3 \oplus x_5 \oplus m_1.$$

Рекурентна послідовність, яка описує операцію дворазового шестиелементного прямого ПКШ, має вигляд:

$$y_i^2 = y_{i-1}^2 \oplus y_i^1, \qquad (22)$$

де $y_0^2 = y_6^1$ та $i \in \{1, \dots, 6\}$.

Триразове шестиелементне ковзне шифрування перетворює послідовність z_i у l_i за умови, що $m_3 = z_6$ – вхідний раундовий ключ третього етапу шифрування, та описується моделлю:

$$l_1 = x_1 \oplus x_2 \oplus x_4 \oplus x_6 \oplus m_1;$$
$$l_2 = x_2 \oplus x_3 \oplus x_5;$$
$$l_3 = x_3 \oplus x_4 \oplus x_6;$$
$$l_4 = x_1 \oplus x_4 \oplus x_5 \oplus m_1;$$
$$l_5 = x_1 \oplus x_2 \oplus x_5 \oplus x_6 \oplus m_1;$$
$$l_6 = x_2 \oplus x_3 \oplus x_6.$$

Рекурентна послідовність, яка описує операцію триразового шестиелементного прямого правостороннього ковзного шифрування, має вигляд:

$$y_i^3 = y_{i-1}^3 \oplus y_i^2, \qquad (23)$$

де $y_0^3 = y_6^2$ та $i \in \{1, \dots, 6\}$.

Чотириразове шестиелементне ковзне шифрування перетворює послідовність l_i у j_i, де $m_4 = l_6$ – вхідний раундовий ключ четвертого етапу шифрування.

Підставивши відповідні вирази, отримаємо:

$$j_1 = x_1 \oplus x_3 \oplus x_4 \oplus m_1;$$
$$j_2 = x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus m_1;$$
$$j_3 = x_1 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6 \oplus m_1;$$
$$j_4 = x_2 \oplus x_3 \oplus x_4 \oplus x_6;$$
$$j_5 = x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus m_1;$$
$$j_6 = x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_6 \oplus m_1.$$

Рекурентна послідовність, яка описує операцію чотириразового шестиелементного прямого ПКШ, має вигляд:

$$y_i^4 = y_{i-1}^4 \oplus y_i^3, \qquad (24)$$

де $y_0^4 = y_6^3$ та $i \in \{1, \dots, 6\}$.

На основі виразів (8, 11, 14, 16-24) отримано узагальнений вираз рекурентної послідовності для опису виконання багаторазового (k -разового) прямого ПКШ:

$$y_i^k = y_{i-1}^k \oplus y_i^{k-1}, \qquad (25)$$

де $y_0^k = y_d^{k-1}$ та $i \in \{1, \dots, d\}$, де, в свою чергу, k – кількість раундів ковзного шифрування і $k \in \{1, \dots, n\}$, а d – розрядність перетворення.

Висновки

В результаті дослідження чотири-, п'яти- та шестиелементних прямих примітивів ковзного шифрування отримано їх математичні моделі на основі рекурентних послідовностей. В статті отримано математичні моделі багаторазового застосування даних примітивів, побудовано узагальнену рекурентну модель багаторазового примітива ковзного шифрування для перетворення заданої кількості елементів із заданою кількістю раундів зашифрування.

У роботі запропоновано підхід щодо математичного опису на основі рекурентних послідовностей моделей операцій перетворення на основі багаторазового застосування примітиву ковзного шифрування при обмеженій кількості елементів.

Список літератури

1. Белецкий А.Я. Криптографические примитивы, основанные на методе скользящего кодирования / А.Я. Белецкий, А.А. Белецкий // Вісник СумДУ. – 2006. – № 10. – С. 33–42.

2. Примитивные полиномы в криптографических приложениях / А.Я. Белецкий, А.А. Белецкий Д.А. Навроцкий, Р.Ю. Кандыба // Сучасний захист інформації. – 2011. – № 4. – С. 5–18.

3. Бабенко В.Г. Параллельная реализация скользящего шифрования / В.Г. Бабенко // Системи обробки інформації. – Х.: ХУПС, 2013. – Вип. 9 (116) – С. 131–134.

4. Бабенко В.Г. Оптимизация матричных операций скользящего шифрования / В.Г. Бабенко // Системи озброєння і військова техніка. – 2013. – № 4 (36).– С. 132–135.

5. Бабенко В.Г. Дослідження матричних операцій криптографічного перетворення на основі арифметичних операцій за модулем / В.Г. Бабенко // Системи управління, навігації та зв'язку. – 2012. – Вип. 4 (24). – С. 85–88.

Надійшла до редколегії 14.07.2015

Рецензент*:* д-р техн. наук проф. І.В. Шостак, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

МОДЕЛИРОВАНИЕ ПРИМИТИВОВ СКОЛЬЗЯЩЕГО ШИФРОВАНИЯ НА ОСНОВЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В.Г. Бабенко, О.Г. Мельник, О.Б. Нестеренко

В данной статье синтезированы математические модели матричных операций многократного преобразования на основе примитива скользящего шифрования. На основе использования полученных рекуррентных зависимостей, описывающих модели многократного выполнения примитива скользящего шифрования, построено обобщенную рекуррентную модель процесса выполнения многократного примитива скользящего шифрования для преобразования n элементов. Используя синтезированные на основе рекуррентных зависимостей математические модели четырех-, пяти- и шестиэлементного прямого правостороннего примитива скользящего шифрования, получено обобщенное выражение рекуррентной последовательности для описания k-разового выполнения примитива скользящего шифрования при заданном количестве элементов. В работе предложен подход относительно математического описания на основе рекуррентных последовательностей моделей операций преобразования на основе многократного применения примитива скользящего шифрования при ограниченном количестве элементов.

Ключевые слова: *рекуррентная последовательность, обобщенная рекуррентная модель, криптографическое преобразование, система уравнений, математическая модель, многократное скользящее шифрования, примитив скользящего шифрования.*

MODELLING OF SLIDING ENCRYPTION PRIMITIVES BASED ON RECURRING SEQUENCES

V.G. Babenko, O.G. Melnyk, O.B. Nesterenko

In this article we synthesized mathematical model of multiple transformation matrix operations based on the sliding encryption primitive. Based on the use of the obtained recurrent dependencies describing models of multiple execution of sliding encryption primitive built a generalized recurrent model of implementation of multiple primitive sliding encryption for transforming n elements. Using synthesized on the basis of mathematical models of recurrent dependencies four-, five- and six-element forward right-primitive sliding encryption produced a generalized expression of recurrent sequence to describe of the multiple perform of sliding encryption primitive for a given number of elements. This paper proposes an approach relatively the mathematical description based on recurring sequences model transformation operations based on the multiple use of sliding encryption primitive with a limited number of elements.

Keywords: *recurrent sequence, a generalized recurrent model, a cryptographic transformation, the system of equations, mathematical model, multiple sliding encryption, sliding encryption primitive.*