



УКРАЇНА

(19) UA (11) 84125 (13) C2
(51) МПК (2006)
H03M 7/46

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС ДО ПАТЕНТУ НА ВІНАХІД

(54) СПОСІБ ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ ТА ПРИСТРІЙ ДЛЯ ЙОГО ЗДІЙСНЕННЯ

1

2

(21) 20040706265

(22) 27.07.2004

(24) 25.09.2008

(46) 25.09.2008, Бюл.№ 18, 2008 р.

(72) ПИЛИПЕНКО МИКОЛА ВАДИМОВИЧ, UA, ХОДАКОВ ВІКТОР ЄГОРОВИЧ, UA, ЕРЕССКО ОЛЕГ, ЛУНЕГОВ МАКСІМ, БАРАНЕНКО РОМАН ВАСИЛЬОВИЧ, UA, ШАГАНЯН СЕРГІЙ МИКОЛАЙОВИЧ, UA, ЦИВІЛЬСЬКИЙ ФЕДІР МИКОЛАЙОВИЧ, UA, РАБЧЕВСЬКА КСЕНІЯ ВАСИЛІВНА, UA, КОРЧЕВСЬКА ЛІЛІЯ ОЛЕКСАНД-
~~РІВНА~~ ПІСОНСЬКИЙ ДЕРЖАВНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ, UA

(56) SU 1651385 A1, 23.05.1991

KR 20010070313, 25.07.2001

SU 1807565 A1, 07.04.1993

RU 2219655 C2, 20.12.2003

RU 2141166 C1, 10.11.1999

RU 99127450 A, 27.09.2001

KR 20030043621, 02.06.2003

(57) 1. Спосіб перетворення інформації, при якому на підготовчому етапі генерують ключ, який на вирішальному етапі накладають на вихідну інформацію за заданим законом, а зворотне перетворення для одержання вихідного тексту виконують повторним генеруванням ключа, який накладають на перетворену інформацію за тим же законом, який **відрізняється** тим, що на підготовчому етапі з бітових елементів вихідної інформації і ключа дискретно формують масиви у вигляді тривимірних геометричних об'єктів

$$V_1 = \begin{cases} x = (x_1, x_2, \dots, x_g) \\ y = (y_1, y_2, \dots, y_h) \\ z = (z_1, z_2, \dots, z_k) \end{cases}$$

та

$$V_2 = \begin{cases} x' = (x'_1, x'_2, \dots, x'_m) \\ y' = (y'_1, y'_2, \dots, y'_q) \\ z' = (z'_1, z'_2, \dots, z'_r) \end{cases}$$

відповідно кожен із яких, принаймні один, із заданою дискретною орієнтацією в тривимірному просторі, причому всі елементи з дійсними значеннями просторового розподілу в системах координат $\forall i \in \{0, 1, 2, \dots, \omega\}$; $\omega \rightarrow \max\{g, h, k, m, q, r\}$, додатково містить проміжний етап, що передусє вирішальному

етапу - операції взаємодії між бітовими елементами зазначених тривимірних геометричних об'єктів, на зазначеному проміжному етапі виконують керовану дискретну зміну форми тривимірних геометричних об'єктів, їхніх напрямків орієнтації в тривимірній системі координат та/або їхнє обертання із можливістю керованого незалежного дискретного обертання кожного з зазначених тривимірних об'єктів навколо вершини осі координат одного з

$$\text{елементів зазначених об'єктів } V_{1,2} = \prod_{i=1}^3 A_{x_i, y_i, z_i},$$

де A_{x_i} - матриця значень місця розташування об'єкта відносно осі x , A_{y_i} - матриця значень місця розташування об'єкта відносно осі y , A_{z_i} - матриця значень місця розташування об'єкта відносно осі z із можливістю керованого незалежного дискретного обертання систем координат зазначених об'єктів та з можливістю керованої дискретної просторової зміни кроку переміщення і взаємодії їхніх елементів, причому керування дискретною зміною кроку виконують за додатковим параметром періодичності, наприклад, $\forall i \in \{1; n\}$, де l - крок, τ - параметр періодичності, причому $\forall i \in \{1; n\}$ та $\forall V_{1,2} \in V_{1,2} \in V_{1,2}$ керування незалежним дискретним обертанням кожного з зазначених тривимірних об'єктів навколо осі координат виконують за додатковим параметром періодичності, наприклад,

$$V_{1,2} = \begin{cases} x = \forall x \in (\tau_x, \pm s\psi) \\ y = \forall y \in (\tau_y, \pm s\psi) \\ z = \forall z \in (\tau_z, \pm s\psi) \end{cases}$$

де ψ - кут обертання об'єкта, s - керований показник величини кута обертання при його дійсних значеннях, тобто, $s \in (0, 1, 2, \dots, u)$, τ - параметр періодичності, при цьому з можливістю керованого незалежного дискретного обертання деяких елементів тривимірних об'єктів навколо вершини осі координат одного з елементів зазначених об'єктів за параметром періодичності

(13) C2

(11) 84125

(19) UA

$$\diamond \exists v_{1,2} = \prod_{i=1}^3 A_{x_i, y_i, z_i} \forall (x_i, y_i, z_i) \in (\tau_{x_i, y_i, z_i} \pm s \psi),$$

де $s \in (0, 1, 2, \dots, u)$ та $\forall v_{1,2} \in V_{1,2}$.

2. Спосіб за п. 1, який **відрізняється** тим, що дискретність значення кута обертання дорівнює при-

наймні 90° , тобто, $\psi = \frac{\pi}{2}$.

3. Спосіб за п. 1, який **відрізняється** тим, що зміну форми зазначених об'єктів виконують методом перестановок.

4. Спосіб за п. 1, який **відрізняється** тим, що керовану дискретну зміну форми зазначених об'єктів виконують за формулою ангармонійного коливання.

5. Пристрій перетворення інформації, який містить операційний пристрій, дві інформаційні вхідні шини якого зв'язані з виходами першого та другого інформаційних регістрів, вхідна шина керування зв'язана із виходом регістра керування, вхідна шина мікрокоманд через регістр мікрокоманд зв'язана із вихідною шиною блока керуючої пам'яті, виходом операційного пристрою є шина сигнальних ознак і вихідна інформаційна шина, виходом пристрою є основна шина процесора, який **відрізняється** тим, що додатково містить регістр сигнальних ознак, формувач адреси, регістр адреси, буферний регістр, перший і другий регістри фіксованих адрес, перший і другий мультиплексори, перший і другий оперативні запам'ятовуючі пристрої, регістр завдання і результату, зазначені дві інформаційні вхідні шини операційного пристрою виконані у вигляді інформаційного регістра та регістра ключа, відповідно, зазначена основна шина процесора виконана у вигляді двонаправленої шини обчислювальної системи, зазначений блок керуючої пам'яті виконаний у вигляді змінного блока керуючої пам'яті, вихідна шина якого виконана у вигляді першої вихідної шини, зазначена шина сигнальних ознак зв'язана з входом регістра сигнальних ознак, перший вихід якого зв'язаний із керуючим входом регістра ключа, другий вихід - із керуючим входом інформаційного регістра, третій вихід - із керуючим входом формувача адреси, четвертий вихід - із керуючими входами першого і другого мультиплексорів, п'ятий і шостий виходи - із керуючими входами запис/зчитування першого і другого оперативних запам'ятовуючих пристроїв, відповідно, сьомий вихід - із керуючим входом запису регістра завдання і результату, восьмий вихід - із керуючими входами першого і другого регістрів

фіксованих адрес і буферного регістра, вхід зазначеного регістра керування зв'язаний із другою вихідною шиною змінного блока керуючої пам'яті, вхідна шина якого зв'язана через регістр адреси з виходом формувача адреси, зазначена вихідна інформаційна шина операційного пристрою зв'язана із входами буферного регістра і першого та другого регістрів фіксованих адрес, вихідні шини яких зв'язані з адресними вхідними шинами першого та другого оперативних запам'ятовуючих пристроїв, відповідно, інформаційні вхідні шини яких зв'язані з виходом буферного регістра та із входом регістра завдання і результату, сигнальний вихід готовності даних якого зв'язаний з аналогічним входом операційного пристрою, інформаційні вихідні шини першого і другого запам'ятовуючих оперативних пристроїв зв'язані з першими входами першого і другого мультиплексорів, відповідно, другі входи яких зв'язані з вихідною шиною регістра завдання і результату, вихідні шини першого і другого мультиплексорів зв'язані з входами інформаційного регістра та регістра ключа, відповідно, а шинний двонаправлений вхід/вихід регістра завдання і результату зв'язаний із двонаправленою шиною обчислювальної системи, входом і виходом пристрою є двонаправлена шина обчислювальної системи.

6. Пристрій за п. 5, який **відрізняється** тим, що, операційний пристрій виконаний у вигляді мікропроцесорного пристрою.

7. Пристрій за п. 5, який **відрізняється** тим, що двонаправлена шина обчислювальної системи виконана у вигляді COM порту за стандартом RS-232C.

8. Пристрій за п. 5, який **відрізняється** тим, що двонаправлена шина обчислювальної системи виконана у вигляді універсального послідовного USB порту.

9. Пристрій за п. 5, який **відрізняється** тим, що двонаправлена шина обчислювальної системи виконана у вигляді інтерфейсу ATA.

10. Пристрій за п. 5, який **відрізняється** тим, що двонаправлена шина обчислювальної системи виконана у вигляді інтерфейсу Centronics - IEEE-1284 із специфікацією режимів LPT порту.

11. Пристрій за п. 5, який **відрізняється** тим, що, двонаправлена шина обчислювальної системи виконана у вигляді інтерфейсу IrDA.

12. Пристрій за п. 5, який **відрізняється** тим, що, змінний блок керуючої пам'яті виконаний у вигляді постійного запам'ятовуючого пристрою, або перепрограмуючого запам'ятовуючого пристрою.

Винахід відноситься до методів перетворення коду, у якому інформація подана заданою послідовністю цифр або чисел, у код, де та ж інформація подана цифрами або числами, відмінними від заданої шляхом кодування за допомогою кодового слова, вираженого цифрами або числами; і може бути використаний при побудові систем опрацювання інформації.

Відомий спосіб перетворення вихідної інформації в шифрований текст методом Вернама [Защита программного обеспечения: Пер. с англ. / Д.Гроувер, Р.Сатер, Дж.Фипс и др. / Под редакцией Д.Гроувера. - М.: Мир, 1992. - С.100-103], [Сколов А.В., Степанюк О.М. Методы информационной защиты объектов и компьютерных сетей. - М.: ООО "Фирма "Издательство АСТ"; СПб.: ООО "Издательство "Полигон", 2000. - ("Шпионские

штуки"). - С.209-210.], у якому перетворення вихідної інформації, поданої заданою двійковою послідовністю, виконують побітним додаванням за модулем 2 із набором двійкових ключів, а дешифрування у вихідну інформацію виконують побітним додаванням за модулем 2 шифрованого тексту з набором тих же двійкових ключів.

Недоліком зазначеного способу є необхідність рівності довжини вихідної двійкової послідовності з довжиною набору двійкових ключів.

Цього недоліку позбавлений спосіб шифрування Віжинера [Раздел 2.12. Система шифрования Вижинера. В кн.: Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. - К.: "Корнейчук", 2000. - С.30-32.], при якому, на підготовчому етапі, ключ кінцевої довжини $k=(k_0, k_1, \dots, k_{n-1})$ продовжують до нескінченної послідовності, повторюючи ланцюжок, у результаті чого одержують робочий ключ $K=(k_0, k_1, \dots, k_{n-1}, k_n, k_{n+1}, k_{n+2}, \dots)$, при $K_j=k(j \bmod n)$, а $0 \leq j < \infty$, потім, на вирішальному етапі, перетворення вихідного тексту $Xf(x_0, x_1, \dots, x_{n-1})$ у шифрований текст $Yf(y_0, y_1, \dots, y_{n-1})$ виконують додаванням за модулем Z при рівній довжині вихідного тексту X та ключа K за формулою VIG: $(x_0, x_1, \dots, x_{n-1}) \Rightarrow (y_0, y_1, \dots, y_{n-1}) = [(x_0+k_0) \bmod Z, \dots, (x_{n-1}+k_{n-1}) \bmod N]$, де, N - кількість символів в алфавіті; X - вихідний текст; K - робочий ключ; Y - шифрований текст; відновлення вихідного тексту виконують у зворотному порядку.

Недоліком системи шифрування є та обставина, що за короткий час методом перебору слів і фраз можна відновити ключ. Тому для одержання ключів повинні використовуватися програмні або апаратні засоби випадкової генерації ключів.

Найбільш близьким за технічною сутністю є спосіб перетворення вихідної інформації в шифрований текст методом гамування [Раздел 2.13. Гаммирование. В кн.: Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. - К.: "Корнейчук", 2000. - С.32-33], у якому, на підготовчому етапі, генерують гаму ключа, яку, на вирішальному етапі, накладають на вихідну інформацію за заданим законом, наприклад, використовуючи побітне додавання за модулем 2. Зворотне перетворення для одержання вихідного тексту виконують повторним генеруванням гами ключа, яку накладають на перетворену інформацію за тим же законом.

Недоліком зазначеного способу є можливість виявлення повторюваного фрагменту ключа існуючими методами криптоаналізу, що дозволить встановити цілком весь ключ, а потім дешифруванням відновити вихідну інформацію.

Відомо пристрій керування мікропрограмованим операційним пристроєм [Рис. 44, "Вычислительное устройство микропрограммируемой ЦВМ. В кн.: Рабинович З.Л., Раманускас В.А. Типовые операции в вычислительных машинах. - К.: Техніка, 1980. - С.207-210], який містить операційний пристрій, обидві інформаційні вхідні шини якого зв'язані з виходами першого і другого інформаційних регістрів, вхідна шина керування зв'язана з виходом регістра керування, вхідна шина мікрокоманд через регістр мікрокоманд зв'язана з виходом керування мікрокомандами блока керуючої

пам'яті, виходом операційного пристрою є шина сигнальних ознак, а вихідна інформаційна шина зв'язана з основною шиною процесора.

Недоліком даного пристрою є неможливість одночасного високошвидкісного опрацювання зі складними комбінаційними операціями великих масивів інформації для її перетворення.

Задачею винаходу є одержання способу перетворення інформації та пристрою для його здійснення, за допомогою яких можна було б із високою швидкістю опрацювання перетворити вихідну інформацію до транспортування, а несанкціоноване розкриття було б неможливим навіть при наявності ключа.

Поставлена задача вирішується тим, що спосіб перетворення інформації та пристрій для його здійснення, при яких, на підготовчому етапі, генерують ключ, який, на вирішальному етапі, накладають на вихідну інформацію за заданим законом, а зворотне перетворення для одержання вихідного тексту виконують повторним генеруванням ключа, який накладають на перетворену інформацію за тим же законом, на підготовчому етапі з бітових елементів вихідної інформації і ключа дискретно формують масиви у вигляді тривимірних геометричних об'єктів

$$V_1 = \begin{cases} x = (x_1, x_2, \dots, x_g) \\ y = (y_1, y_2, \dots, y_h) \\ z = (z_1, z_2, \dots, z_k) \end{cases}$$

та

$$V_2 = \begin{cases} x' = (x_1, x_2, \dots, x_m) \\ y' = (y_1, y_2, \dots, y_q) \\ z' = (z_1, z_2, \dots, z_r) \end{cases},$$

відповідно, кожен із яких, принаймні, один, із заданою дискретною орієнтацією в тривимірному просторі, причому всі елементи з дійсними значеннями просторового розподілу в системах координат, тобто $\forall i \in \{0, 1, 2, \dots, \omega\}; \omega \rightarrow \max\{g, h, k, m, q, r\}$, додатково містить проміжний етап, що передує вирішальному етапу - операції взаємодії між бітовими елементами зазначених тривимірних геометричних об'єктів, на зазначеному проміжному етапі виконують керовану дискретну зміну форми тривимірних геометричних об'єктів, їхніх напрямків орієнтації в тривимірній системі координат та/або їхнє обертання, із можливістю керованого незалежного дискретного обертання кожного з зазначених тривимірних об'єктів навколо вершини осі координат одного з елементів зазначених об'єктів, напри-

клад, $V_{1,2} = \prod_{i=1}^3 A_{x,y,z_i}$, де, A_{x_i} - матриця зна-

чень місця розташування об'єкта відносно осі x ; A_{y_i} - матриця значень місця розташування об'єкта відносно осі y ; A_{z_i} - матриця значень місця розташування об'єкта відносно осі z , із можливістю керованого незалежного дискретного обертання систем координат зазначених об'єктів та з можливістю керованої дискретної просторової зміни кроку переміщення і взаємодії їхніх елементів, причому керування дискретною зміною кроку виконують за додатковим параметром періодичності, напри-

клад, $v_{1,2}(\forall l \in \tau_{x,y,z})$, де, l - крок; τ - параметр періодичності; причому $\forall i \in \{1;n\}$ та $\forall v_{1,2} \in V_{1,2}$, керування незалежним дискретним обертанням кожного з зазначених тривимірних об'єктів навколо осі координат виконують за додатковим параметром

$$\text{періодичності, наприклад, } V_{1,2} = \begin{cases} x = \forall x \in (\tau_x, \pm s\psi) \\ y = \forall y \in (\tau_y, \pm s\psi) \\ z = \forall z \in (\tau_z, \pm s\psi) \end{cases}$$

де, ψ - кут обертання об'єкта; s - керований показник величини кута обертання при його дійсних значеннях, тобто, $s \in (0,1,2,...,u)$; τ - параметр періодичності, при цьому з можливістю керованого незалежного дискретного обертання деяких елементів тривимірних об'єктів навколо вершини осі координат одного з елементів зазначених об'єктів за параметром періодичності, наприклад,

$$\exists v_{1,2} = \bigcup_{i=1}^3 A_{x_i, y_i, z_i} \forall (x_i, y_i, z_i) \in (\tau_{x_i, y_i, z_i} \pm s\psi),$$

де, $s \in (0,1,2,...,u)$, та $\forall v_{1,2} \in V_{1,2}$. Дискретність значення кута обертання дорівнює, принаймні, 90° ,

тобто, $\psi = \frac{\pi}{2}$. Зміну форми зазначених об'єктів

виконують методом перестановок. Керовану дискретну зміну форми зазначених об'єктів виконують за формулою ангармонійного коливання. Пристрій перетворення інформації, який містить операційний пристрій, обидві інформаційні вхідні шини якого зв'язані з виходами першого та другого інформаційних регістрів, вхідна шина керування зв'язана із виходом регістра керування, вхідна шина мікрокоманд через регістр мікрокоманд зв'язана із вихідною шиною блока керуючої пам'яті, виходом операційного пристрою є шина сигнальних ознак і вихідна інформаційна шина, виходом пристрою є основна шина процесора, додатково містить регістр сигнальних ознак, формувач адреси, регістр адреси, буферний регістр, перший і другий регістри фіксованих адрес, перший і другий мультиплексори, перший і другий оперативні запам'ятовуючі пристрої, регістр завдання і результату, зазначені обидві інформаційні вхідні шини операційного пристрою виконані у вигляді інформаційного регістра та регістра ключа, відповідно, зазначена основна шина процесора виконана у вигляді двонаправленої шини обчислювальної системи, зазначений блок керуючої пам'яті виконаний у вигляді змінного блока керуючої пам'яті, вихідна шина якого виконана у вигляді першої вихідної шини, зазначена шина сигнальних ознак зв'язана з входом регістра сигнальних ознак, перший вихід якого зв'язаний із керуючим входом регістра ключа, другий вихід - із керуючим входом інформаційного регістра, третій вихід - із керуючим входом формувача адреси, четвертий вихід - із керуючими входами першого і другого мультиплексорів, п'ятий і шостий виходи - із керуючими входами запис/зчитування першого і другого оперативних запам'ятовуючих пристроїв, відповідно, сьомий вихід - із керуючим входом запису регістра завдання і результату, восьмий вихід - із керуючими входами першого і другого регістрів фіксованих адрес і буферного регістра, вхід зазначеного регістра керування зв'язаний із другою ви-

хідною шиною змінного блока керуючої пам'яті, вхідна шина якого зв'язана через регістр адреси з виходом формувача адреси, зазначена вихідна інформаційна шина операційного пристрою зв'язана із входами буферного регістра і першого та другого регістрів фіксованих адрес, вихідні шини яких зв'язані з адресними вхідними шинами першого та другого оперативних запам'ятовуючих пристроїв, відповідно, інформаційні вхідні шини яких зв'язані з виходом буферного регістра та із входом регістра завдання і результату, сигнальний вихід готовності даних якого зв'язаний з аналогічним входом операційного пристрою, інформаційні вихідні шини першого і другого запам'ятовуючих оперативних пристроїв зв'язані з першими входами першого і другого мультиплексорів, відповідно, другі входи яких зв'язані з вихідною шиною регістра завдання і результату, вихідні шини першого і другого мультиплексорів зв'язані з входами інформаційного регістра та регістра ключа, відповідно, а шинний двонаправлений вхід/вихід регістра завдання і результату зв'язаний із двонаправленою шиною обчислювальної системи, входом і виходом пристрою є двонаправлена шина обчислювальної системи. Операційний пристрій виконаний у вигляді мікропроцесорного пристрою. Двонаправлена шина обчислювальної системи виконана у вигляді COM порту за стандартом RS-232C. Двонаправлена шина обчислювальної системи виконана у вигляді універсального послідовного USB порту. Двонаправлена шина обчислювальної системи виконана у вигляді інтерфейсу ATA. Двонаправлена шина обчислювальної системи виконана у вигляді інтерфейсу Centronics - IEEE-1284 із специфікацією режимів LPT порту. Двонаправлена шина обчислювальної системи виконана у вигляді інтерфейсу IrDA. Змінний блок керуючої пам'яті виконаний у вигляді постійного запам'ятовуючого пристрою, або перепрограмуючого запам'ятовуючого пристрою.

Оскільки зазначені відмітні ознаки відсутні в прототипу, запропонований спосіб перетворення інформації та пристрій для його здійснення відповідають критерію "новизна".

Таким чином, в отриманого способу з'являється властивість, яка дозволяє за рахунок просторового розподілу інформації і методів взаємодії з ключовими компонентами, виконувати перетворення інформації, цілісність якої буде надійно захищена, а пристрій забезпечить швидке перетворення.

На Фіг.1 зображена вихідна інформація і ключ, а також їх складові елементи. Фіг.2 ілюструє етапи формування з вихідної інформації (або ключа) масиву у вигляді тривимірного геометричного об'єкта. На Фіг.3 поданий тривимірний геометричний об'єкт у системі координат. На Фіг.4 подані координати вершин і позначення граней елемента тривимірного геометричного об'єкта. На Фіг.5 подані позначення кутів між осями координат елемента тривимірного геометричного об'єкта. На Фіг.6 зображені координати вершин елементів тривимірного геометричного об'єкта, найближчих до початку координат. На Фіг.7 зображені координати вершин елементів тривимірного геометричного об'єкта, віддалених від початку координат. Фіг.8

ілюструє координати вершин елементів тривимірного геометричного об'єкта до та після дискретного обертання групи елементів навколо вершини осі координат одного з елементів. На Фіг.9 подані знову придбані значення координат тривимірного геометричного об'єкта після його обертання. На Фіг.10 поданий приклад зміни форми тривимірного геометричного об'єкта шляхом переміщення його елементів (початковий етап). На Фіг.11 поданий приклад зміни форми тривимірного геометричного об'єкта шляхом переміщення його елементів (наступний етап). Фіг.12 ілюструє початок взаємодії масиву вихідної інформації і ключового масиву на прикладі тривимірних геометричних об'єктів. На Фіг.13 поданий варіант взаємодії масиву вихідної інформації і ключового масиву на прикладі тривимірних геометричних об'єктів, один із яких із змінною формою. На Фіг.14 подана структурна схема пристрою перетворення інформації.

Спосіб перетворення інформації полягає в тому, що, на підготовчому етапі, генерують ключ, який на вирішальному етапі, накладають на вихідну інформацію за заданим законом, наприклад, використовуючи побітне додавання за модулем 2. Зворотне перетворення для одержання вихідного тексту виконують повторним генеруванням ключа, який накладають на перетворену інформацію за тим же законом. На цьому ж підготовчому етапі з бітових елементів 1 (Фіг.1) вихідної інформації 2 і ключа 3 дискретно формують масиви (Фіг.2) у вигляді тривимірних геометричних об'єктів 2 -

$$V_1 = \begin{cases} x = (x_1, x_2, \dots, x_g) \\ y = (y_1, y_2, \dots, y_h) \\ z = (z_1, z_2, \dots, z_k) \end{cases}$$

та 3 -

$$V_2 = \begin{cases} x' = (x_1, x_2, \dots, x_m) \\ y' = (y_1, y_2, \dots, y_q) \\ z' = (z_1, z_2, \dots, z_r) \end{cases},$$

відповідно, кожен із яких, принаймні, один, із заданою дискретною орієнтацією в тривимірному просторі. Причому всі елементи 1 із дійсними значеннями просторового розподілу в системах координат, тобто $\forall i \in \{0, 1, 2, \dots, \omega\}$; $\omega \rightarrow \max\{g, h, k, m, q, r\}$. Спосіб перетворення інформації додатково містить проміжний етап, що передувє вирішальному етапу - операції взаємодії між бітовими елементами 1 зазначених тривимірних геометричних об'єктів 2 і 3. На зазначеному проміжному етапі виконують керовану дискретну зміну форми тривимірних геометричних об'єктів 2 і 3, їхніх напрямків орієнтації в тривимірній системі координат та/або їхнє обертання. На цьому ж етапі можливо виконувати і кероване незалежне дискретне обертання кожного з зазначених тривимірних об'єктів 2 і 3 навколо вершини осі координат 000 (Фіг.8а) одного з елементів 1 (уявна вісь обертання δ , що проходить через точки 000-111-222) зазначених об'єктів 2 і 3, наприклад,

$$V_{1,2} = \prod_{i=1}^3 A_{x_i, y_i, z_i} \text{ де, } A_{x_i} - \text{матриця значень місця}$$

розташування об'єкта відносно осі x ; A_{y_i} - матри-

ця значень місця розташування об'єкта відносно осі y ; A_{z_i} - матриця значень місця розташування об'єкта відносно осі z . На цьому ж етапі, можливо виконання керованого незалежного дискретного обертання систем координат зазначених об'єктів (у графічних матеріалах не подане). Також можливо виконувати керовану дискретну просторову зміну кроку переміщення і взаємодії елементів тривимірних геометричних об'єктів 2 і 3. Керування дискретною зміною кроку виконують за додатковим параметром періодичності, наприклад, $v_{1,2} (\forall i \in \tau_{x_i, y_i, z_i})$, де, l - крок; τ - параметр періодичності; причому $\forall i \in \{1; n\}$, а $\forall v_{1,2} \in V_{1,2}$. Керування незалежним дискретним обертанням кожного з зазначених тривимірних об'єктів 2 і 3 навколо осі координат виконують за додатковим параметром

$$\text{періодичності, наприклад, } V_{1,2} = \begin{cases} x = \forall x \in (\tau_x, \pm s\psi) \\ y = \forall y \in (\tau_y, \pm s\psi) \\ z = \forall z \in (\tau_z, \pm s\psi) \end{cases}$$

де, ψ - кут обертання об'єкта; s - керований показник величини кута обертання при його дійсних значеннях, тобто, $s \in (0, 1, 2, \dots, u)$; τ - параметр періодичності. На цьому ж етапі, можливе виконання керованого незалежного дискретного обертання деяких елементів 1 тривимірних геометричних об'єктів 2 і 3 навколо вершини осі координат (наприклад, 000) одного з елементів 1 зазначених об'єктів 2 і 3 за параметром періодичності, наприклад,

$$\diamond \exists v_{1,2} = \prod_{i=1}^3 A_{x_i, y_i, z_i} \forall (x_i, y_i, z_i) \in (\tau_{x_i, y_i, z_i} \pm s\psi),$$

де, $s \in (0, 1, 2, \dots, u)$, та $\forall v_{1,2} \in V_{1,2}$. Дискретність значення кута обертання дорівнює, принаймні, 90° ,

тобто, $\psi = \frac{\pi}{2}$. Зміну форми зазначених об'єктів 2 і

3 виконують методом перестановок. Керовану дискретну зміну форми зазначених об'єктів 2 і 3 виконують за формулою ангармонійного коливання.

Пристрій перетворення інформації містить двонаправлену шину 5 (Фіг.14) обчислювальної системи 6 зв'язану із шинним двонаправленим входом/виходом 7 регістра завдання і результату 8, вихідна шина 9 якого сполучена з другими входами 10 і 11 першого 12 і другого 13 мультіплексорів, відповідно, вихідні шини 14 і 15 яких зв'язані з входами 16 і 17 інформаційного регістра 18 та регістра ключа 19, відповідно, виходи яких приєднані до першої 20 і другої 21 шин, відповідно, операційного пристрою 22. Вхідна шина керування 23 операційного пристрою 22 зв'язана з виходом регістра керування 24. Вхідна шина мікрокоманд 25 операційного пристрою 22 через регістр мікрокоманд 26 зв'язана з першою вихідною шиною 27 змінного блока керуючої пам'яті 28, друга вихідна шина 29 якого зв'язана з входом регістра керування 24. Шина сигнальних ознак 30 операційного пристрою 22 зв'язана із входом 31 регістра сигнальних ознак 32, перший 33 і другий 34 виходи якого сполучені з керуючими входами 35 і 36 регістра ключа 19 та інформаційного регістра 18, відповідно. Третій вихід 37 регістра сигнальних ознак 32

сполучений із керуючим входом формувача адреси 38, вихід якого через регістр адреси 39 зв'язаний із вхідною шиною 40 змінного блока керуючої пам'яті 28. Четвертий вихід 41 регістра сигнальних ознак 32 сполучений із керуючими входами 42 і 43 першого 12 і другого 13 мультиплексорів, відповідно. П'ятий 44 і шостий 45 виходи регістра сигнальних ознак 32 сполучені з керуючими входами запис/зчитування 46 і 47 першого 48 і другого 49 оперативних запам'ятовуючих пристроїв, відповідно. Сьомий вихід 50 регістра сигнальних ознак 32 сполучений із керуючим входом 51 запису регістра завдання і результату 8. Восьмий вихід 52 регістра сигнальних ознак 32 сполучений із керуючими входами 53 і 54 першого 55 і другого 56 регістрів фіксованих адрес та керуючим входом 57 буферного регістра 58, відповідно. Вихідна інформаційна шина 59 операційного пристрою 22 зв'язана з входами буферного регістра 58 і першого 55 та другого 56 регістрів фіксованих адрес, вихідні шини 60 та 61 яких зв'язані з адресними входами першого 48 і другого 49 оперативних запам'ятовуючих пристроїв. Інформаційні вхідні шини 62 першого 48 і другого 49 оперативних запам'ятовуючих пристроїв зв'язані з виходом буферного регістра 58 і з входом 63 регістра завдання і результату 8. Сигнальний вихід готовності даних 64 регістра завдання і результату 8 зв'язаний з аналогічним входом 65 операційного пристрою 22. Інформаційні вихідні шини 66 та 67 першого 48 і другого 49 оперативних запам'ятовуючих пристроїв зв'язані з першими входами 68 та 69 першого 12 і другого 13 мультиплексорів, відповідно. Входом і виходом пристрою є двонаправлена шина 5 обчислювальної системи 6. Операційний пристрій виконаний у вигляді мікропроцесорного пристрою. Двонаправлена шина обчислювальної системи виконана у вигляді COM порту за стандартом RS-232C. Двонаправлена шина обчислювальної системи виконана у вигляді універсального послідовного USB порту. Двонаправлена шина обчислювальної системи виконана у вигляді інтерфейсу ATA. Двонаправлена шина обчислювальної системи виконана у вигляді інтерфейсу Centronics - IEEE-1284 із специфікацією режимів LPT порту. Двонаправлена шина обчислювальної системи виконана у вигляді інтерфейсу IrDA. Змінний блок керуючої пам'яті виконаний у виді постійного запам'ятовуючого пристрою або перепрограмуючого запам'ятовуючого пристрою.

У процесі перетворення інформації на підготовчому етапі, генерують ключ для взаємодії з вихідною інформацією за заданим законом, наприклад, використовуючи побітне додавання за модулем 2. Для забезпечення цілісності інформації і захисту її від навмисного спотворення або розкриття, - на цьому ж підготовчому етапі з бітових елементів 1 (Фіг.1) вихідної інформації 2 і ключа 3 дискретно формують масиви (Фіг.2) у вигляді тривимірних геометричних об'єктів 2 і 3, кожен із яких, принаймні, один, із заданою дискретною орієнтацією в тривимірному просторі. Проміжний етап містить ряд різноманітних перетворень усередині кожного з зазначених тривимірних геометричних об'єктів 2 і 3, що забезпечує додатковий захист від небажаного використання інформації. Це також

керована дискретна зміна форми тривимірних геометричних об'єктів 2 і 3, їхніх напрямків орієнтації в тривимірній системі координат та/або їхнє обертання; кероване незалежне дискретне обертання кожного з зазначених тривимірних об'єктів 2 і 3 навколо вершини осі координат 000 (Фіг.8a) одного з елементів 1; кероване незалежне дискретне обертання систем координат зазначених об'єктів 2 і 3; керована дискретна просторова зміна кроку переміщення і взаємодії елементів тривимірних геометричних об'єктів 2 і 3. Також виконується керування дискретною зміною кроку за додатковим параметром періодичності; керування незалежним дискретним обертанням кожного з зазначених тривимірних об'єктів 2 і 3 навколо осі координат виконують за додатковим параметром періодичності; кероване незалежне дискретне обертання деяких елементів 1 тривимірних геометричних об'єктів 2 і 3 навколо вершини осі координат (наприклад, 000) одного з елементів 1 зазначених об'єктів 2 і 3 за параметром періодичності. 3 цією ж метою змінюють форми зазначених об'єктів 2 і 3 методом перестановок (Фіг.10 та Фіг.11); керують дискретною зміною форми зазначених об'єктів 2 і 3 за формулою ангармонійного коливання (у графічних матеріалах не подане).

Двонаправлена шина 5 (Фіг.14) забезпечує зв'язок обчислювальної системи 6 з пристроєм перетворення інформації за допомогою двонаправленого входу/виходу 7 регістра завдання і результату 8, який виконує функції буферного регістра між обчислювальною системою 6 і пристроєм перетворення інформації для одержання завдання і для видачі готового результату. Вихідна шина 9 зв'язує регістр завдання і результату 8 із другими входами 10 і 11 першого 12 та другого 13 мультиплексорів, відповідно, які служать для переключення вихідної шини на одну з двох вхідних. Вихідні шини 14 і 15 першого 12 та другого 13 мультиплексорів, зв'язані з входами 16 і 17 інформаційного регістра 18 і регістра ключа 19, відповідно, які служать для проміжного збереження вихідної інформації і ключової послідовності. Виходи цих регістрів приєднані до першої 20 і другої 21 шин, відповідно, операційного пристрою 22, який призначений для виконання логічних, математичних і спеціальних операцій із вхідними змінними. Вхідна шина керування 23 зв'язує операційний пристрій 22 із виходом регістра керування 24, який призначений для проміжного збереження керуючих параметрів вхідних змінних при їхньому опрацюванні в операційному пристрої 22. Вхідна шина мікрокоманд 25, операційного пристрою 22, зв'язує його з регістром мікрокоманд 26, який служить для проміжного збереження мікрокоманд, що надходять за допомогою першої вихідної шини 27 із виходу змінного блока керуючої пам'яті 28. Змінний блок керуючої пам'яті 28 містить команди перетворення вихідної інформації. За рахунок виконання блока керуючої пам'яті у вигляді змінного, - пристрій перетворення інформації набуває властивості універсальності. Друга вихідна шина 29 змінного блока керуючої пам'яті 28 зв'язує його із входом регістра керування 24. Шина сигнальних ознак 30 операційного пристрою 22 з'єднує його із входом 31 регістра сигнальних ознак 32, який служить для

тимчасового збереження керуючих сигналів, які керують процесом опрацювання інформації. Перший 33 і другий 34 виходи регістра сигнальних ознак 32 сполучені з керуючими входами 35 і 36 регістра ключа 19 та інформаційного регістра 18, відповідно, забезпечуючи керування записом та їхнє індивідуальне обнуління при виконанні "перемішування" елементів масиву в одному із регістрів. Третій вихід 37 регістра сигнальних ознак 32 сполучений із керуючим входом формувача адреси 38, який через регістр адреси 39 генерує адреси вибірки вмісту зі змінного блока керуючої пам'яті 28 за допомогою його вхідної шини 40. Четвертий вихід 41 регістра сигнальних ознак 32 сполучений із керуючими входами 42 і 43 першого 12 та другого 13 мультиплексорів, відповідно, керуючи перенаправленням даних, які надходять до регістру ключа 19 та до інформаційного регістру 18. П'ятий 44 і шостий 45 виходи регістра сигнальних ознак 32 сполучені з керуючими входами запис/зчитування 46 і 47 першого 48 і другого 49 оперативних запам'ятовуючих пристроїв, відповідно, керуючи ними при запису та зчитуванні інформації. Перший 48 і другий 49 оперативні запам'ятовуючі пристрої служать для збереження початкових, проміжних і кінцевих значень вихідної (перетворюваної та перетвореної) інформації і ключа, відповідно. Сьомий вихід 50 регістра сигнальних ознак 32 сполучений із керуючим входом запису 51 регістра завдання і результату 8, здійснюючи запис результату перетворення в зазначений регістр. Восьмий вихід 52 регістра сигнальних ознак 32 сполучений із керуючими входами 53 і 54 першого 55 і другого 56 регістрів фіксованих адрес та керуючим входом 57 буферного регістра 58, відповідно, для їхньої активізації. Перший 55 і другий 56 регістри фіксованих адрес призначені для проміжного збереження проміжних адрес звертання до оперативних запам'ятовуючих пристроїв 48 і 49. Буферний регістр 58 служить для проміжного збереження результатів опрацювання інформації та пересилки результатів. Вихідна інформаційна шина 59 зв'язує операційний пристрій 22 із входами буферного регістра 58 та регістрами фіксованих адрес 55 і 56, вихідні шини 60 і 61 яких зв'язують регістри фіксованих адрес 55 і 56 з адресними входами першого 48 і другого 49 оперативних запам'ятовуючих пристроїв. Адресні входи оперативних запам'ятовуючих пристроїв 48 і 49 служать для вибірки адреси збереженої інформації. Інформаційні вхідні шини 62 першого 48 і другого 49 оперативних запам'ятовуючих пристроїв служать для надходження проміжної інформації з виходу буферного регістра 58, який, у свою чергу зв'язаний із входом 63 регістра завдання і результату 8 для запису в нього результатів обчислень. Сигнальний вихід 64 готовності даних DSR (Data Set Ready) регістра завдання і результату 8 і аналогічний вхід 65 готовності даних операційного пристрою 22, служать для керування стартом перетворення інформації при одержанні вихідних даних, завантажених у регістр завдання і результату 8. Інформаційна вихідна шина 66 першого оперативного запам'ятовуючого пристрою 48 зв'язана з першим входом 68 першого мультиплексора 12 для перенаправлення даних в інформацій-

ний регістр 18 при запису перетворюваної інформації на підготовчому, проміжному і вирішальному етапах. Інформаційна вихідна шина 67 другого оперативного запам'ятовуючого пристрою 49 зв'язана з першим входом 69 другого мультиплексора 13 для перенаправлення даних в регістр ключа 19 при запису що перетворюваного ключа на підготовчому, проміжному і вирішальному етапах. Входом і виходом пристрою є двонаправлена шина 5 обчислювальної системи 6. Як варіант виконання, операційний пристрій 22 виконаний у вигляді мікропроцесорного пристрою. Двонаправлена шина 5 обчислювальної системи 6 може бути виконана у вигляді COM порту (Communication Port) за стандартом RS-232C, що відповідає вітчизняному аналогу стику С-2. Двонаправлена шина 5 обчислювальної системи 6 може бути виконана у вигляді універсального послідовного USB порту (Universal Serial Bus), що дозволяє забезпечити обмін інформацією до 1Мбайта/сек. Двонаправлена шина 5 обчислювальної системи 6 може бути виконана у вигляді інтерфейсу ATA (Advanced Technology Attachment) для підключення пристроїв IDE (Integrated Drive (Disk) Electronics). На цьому інтерфейсі, в основному, забезпечується обмін даними до 100Мбайт/сек (при невідповідності пристроями - до 66Мбайт/сек) між жорсткими дисками й обчислювальною системою. Двонаправлена шина 5 обчислювальної системи 6 може бути виконана у вигляді інтерфейсу Centronics - IEEE-1284 із специфікацією режимів LPT порту (Line Printer), наприклад, SPP, ECP, EPP. Цей протокол взаємодії відповідає вітчизняному аналогу ІРПР-М. Двонаправлена шина 5 обчислювальної системи 6 може бути виконана у вигляді інтерфейсу IrDA (Infrared Data Association), який дозволяє цим каналом передавати інформацію понад 1Гбайта/сек. Змінний блок керуючої пам'яті виконаний у вигляді постійного запам'ятовуючого пристрою або перепрограмуючого запам'ятовуючого пристрою із метою розширення можливостей пристрою перетворення інформації.

Для одержання важливих відомостей злочинцями активно розробляються численні методи витягу інформації. До цих методів відносяться, наприклад, прослуховування телефонних розмов і аналіз документів, таємне копіювання файлів і недостатньо захищених комп'ютерів. Існують спеціальні засоби перехоплення, що дозволяють розшифрувати закодовану інформацію, яка пересилається корпоративними каналами зв'язку. Особливо уразливі повідомлення, зашифровані з використанням застарілих технологій, що дозволяє регулярно аналізувати телекомунікаційний трафік, а також інформацію, яка пересилається між комп'ютерами, у тому числі й електронною поштою.

"Ади Шамир, один из трех авторов разработки методологии шифрования с открытыми ключами, и Эли Бихам утверждают, что они могут получить даже 168-разрядный секретный ключ Triple-DES. 56-разрядный стандарт DES использовался до 2001 года в США для использования в банковской сфере и широко реализован в программных и аппаратных продуктах, и именно после того, как стала найдена методика расшифровки этого стандарта, США отказались от использования стандарта

DES [Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. Справочное пособие. - СПб.: БХВ - Петербург; Арлит, 2002. - С.11]."

Щоб уникнути небажаного розкриття інформації, пропонується спосіб перетворення інформації та пристрій для його здійснення. Важливою особливістю запропонованого способу перетворення інформації, крім відомих етапів перетворення, є введення проміжних етапів, на яких провадиться трансформація (різноманітні переміщення елементів усередині повідомлення). Але тому що ці переміщення і перемішування (а також піднесення до ступеня та логарифмування) давно відомі і цілком успішно розпізнаються криптоаналітиками, знадобився час для пошуку недоліків існуючих методів.

Криптоаналітичні методи достатньо успішно справляються з такими структурами, можна умовно назвати "лінійними". Не мається на увазі їх математична властивість, а за структурою розташування елементів повідомлення витягнутого в одну лінію.

Тому на підготовчому етапі з бітових елементів 1 (Фіг.1 - Фіг.2а, Фіг.2б, Фіг.2в) вихідної інформації 2 і ключа 3 дискретно формують масиви у вигляді тривимірних геометричних об'єктів 2 (Фіг.3)

$$V_1 = \begin{cases} x = (x_1, x_2, \dots, x_g) \\ y = (y_1, y_2, \dots, y_h) \\ z = (z_1, z_2, \dots, z_k) \end{cases} \quad (1)$$

та 3 -

$$V_2 = \begin{cases} x' = (x_1, x_2, \dots, x_m) \\ y' = (y_1, y_2, \dots, y_q) \\ z' = (z_1, z_2, \dots, z_r) \end{cases} \quad (2)$$

відповідно, кожний із яких, принаймні, один, із заданою дискретною орієнтацією в тривимірному просторі (координати x, y, z). У висловленні "принаймні, один", розуміється, що і вихідна інформація 2 і ключ 3 можуть мати розосереджені в тривимірному просторі свої тривимірні геометричні фрагменти. З заданою дискретністю всі елементи 1 мають дійсні значення просторового розподілу в системах координат, тобто,

$$\forall i \in \{0, 1, 2, \dots, \omega\}; \omega \rightarrow \max\{g, h, k, m, q, r\} \quad (3)$$

Додатково введений проміжний етап, що передуює вирішальному етапу (операції взаємодії між бітовими елементами 1 зазначених тривимірних геометричних об'єктів 2 і 3). На проміжному етапі виконують керовану дискретну зміну форми тривимірних геометричних об'єктів 2 та 3, їхніх напрямків орієнтації в тривимірній системі координат та/або їхнє обертання. Для орієнтації об'ємних тривимірних масивів вихідної інформації 2 і ключа 3 та їхніх елементів 1 запозичена система відліку з [Рис. 1.12, Рис. 1.14. Символи узлов, рядов и плоскостей. В кн.: Пенкаля Т. Очерки кристаллохимии. Польша, 1972. / Пер. с польск. под ред. проф.

Франк-Каменецкого В.А. - Л.: Химия, 1974. - С.22-32], що відображена на Фіг.4-9. Також дається можливість виконувати кероване незалежне дискретне обертання кожного з зазначених тривимірних об'єктів 2 і 3 навколо вершини осі координат 000 (Фіг.8а) одного з елементів 1 (уявна вісь обертання S , що проходить через точки 000-111-222) зазначених об'єктів, наприклад,

$$V_{1,2} = \prod_{i=1}^3 A_{x_i, y_i, z_i} \quad (4)$$

де, A_{x_i} - матриця значень місця розташування об'єкта відносно осі x ; A_{y_i} - матриця значень місця розташування об'єкта відносно осі y ; A_{z_i} - матриця значень місця розташування об'єкта відносно осі z .

При цьому праві обертання тривимірних геометричних об'єктів 2 і 3 навколо позитивних координатних осей будуть описуватися такими матрицями їхніх значень:

1) обертання об'єктів 2 і 3 на кут ψ навколо осі x

$$A_{x_i}(\psi) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \psi & -\sin \psi \\ 0 & \sin \psi & \cos \psi \end{pmatrix} \quad (5)$$

2) обертання об'єктів 2 і 3 на кут ψ навколо осі y

$$A_{y_i}(\psi) = \begin{pmatrix} \cos \psi & 0 & \sin \psi \\ 0 & 1 & 0 \\ -\sin \psi & 0 & \cos \psi \end{pmatrix} \quad (6)$$

3) обертання об'єктів 2 і 3 на кут ψ навколо осі z

$$A_{z_i}(\psi) = \begin{pmatrix} \cos \psi & -\sin \psi & 0 \\ \sin \psi & \cos \psi & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (7)$$

У процесі проміжного етапу передбачена можливість керованого незалежного дискретного обертання систем координат зазначених об'єктів 2 і 3 (у графічних матеріалах не відбите), а також можливість керованої дискретної просторової зміни кроку переміщення і взаємодії їхніх елементів 1. Причому керування дискретною зміною кроку виконують за додатковим параметром періодичності, наприклад,

$$v_{1,2}(\forall l \in \tau_{x_i, y_i, z_i}) \quad (8)$$

де, l - крок; τ - параметр періодичності; причому $\forall i \in \{1, n\}$, а $\forall v_{1,2} \in V_{1,2}$. Під параметром періодичності тут приймається участь (або неучасть) елемента 1 або групи елементів 1 у даній конкретній

операції (переміщення, обертання, взаємодія вихідної інформації 2 із ключем 3). Тлумаченням параметра періодичності обертання можна вважати аналогію з безупинним обертанням і кутовою швидкістю [14.10-7. Бесконечно малые вращения, непрерывное вращение и угловая скорость. В кн.: Корн Г., Корн Т. Справочник по математике (для научных работников и инженеров). - Издание четвертое / Пер. со второго амер. перераб. изд. И.Г.Арамановича, А.М.Березмана, И.А.Вайнштейна, Л.З.Румшиского, Л.Я.Цлафа. Под ред. И.Г.Арамановича. - М.: Наука, Главная редакция физико-математической литературы, 1977. - С.452-454], де формулами (14. 10-38) та (14. 10-39) описуються положення елементів 1 при керованому незалежному дискретному обертанні системи координат зазначених об'єктів 2 і 3.

На проміжному етапі є можливість виконувати керування незалежним дискретним обертанням кожного з зазначених тривимірних об'єктів 2 і 3 навколо осі координат за додатковим параметром періодичності, наприклад,

$$V_{1,2} = \begin{cases} x = \forall x \in (\tau_x, \pm s\psi) \\ y = \forall y \in (\tau_y, \pm s\psi) \\ z = \forall z \in (\tau_z, \pm s\psi) \end{cases} \quad (9)$$

де, ψ - кут обертання об'єкта; s - керований показник величини кута обертання при його дійсних значеннях, тобто, $s \in (0, 1, 2, \dots, u)$; τ - параметр періодичності

Також є можливість керувати незалежним дискретним обертанням деяких елементів 1 тривимірних об'єктів 2 і 3 навколо вершини осі координат (Фіг.8) одного з елементів 1 зазначених об'єктів за параметром періодичності, наприклад,

$$\diamond \exists v_{1,2} = \prod_{i=1}^3 A_{x_i, y_i, z_i} \forall (x_i, y_i, z_i) \in (\tau_{x_i, y_i, z_i} \pm s\psi) \quad (10)$$

де, \diamond - модальний оператор "можливо"; \exists - квантор існування; $s \in (0, 1, 2, \dots, u)$, та $\forall v_{1,2} \in V_{1,2}$. На Фіг.8а поданий тривимірний геометричний об'єкт 2 або 3 до повороту навколо уявної осі обертання 8, що проходить через точки 000-111-222, а на Фіг.8б - після повороту. У таблиці 1 подана процедура зміни положення вузлових точок тривимірного геометричного об'єкта в тривимірній системі координат.

Таблиця 1

Процедура зміни положення вузлових точок тривимірного геометричного об'єкта в тривимірній системі координат

Значення положення вузлових точок за Фіг.8а до обертання	Значення положення вузлових точок за Фіг.8б після обертання
002	200
012	201
022	202
102	210

112	211
122	212
202	220
212	221
222	222
001	100
011	101
021	102
101	110
111	111
121	112
201	120
211	121
221	122
000	000
010	001
020	002
100	010
110	011
120	012
200	020
210	021
220	022

З таблиці 1 видно, що вузлові точки 000, 111 і 222 залишилися на місці. На Фіг.9 поданий тривимірний геометричний об'єкт із знову надбаними значеннями вузлових точок (по відношенню до Фіг.8б).

Дискретність значення кута обертання дорівнює, принаймні, 90° , тобто, $\psi = \frac{\pi}{2}$. Зміну форми зазначених об'єктів виконують методом керованих π перестановок k або їхнього об'єднання, наприклад,

$$\pi_{n/m}(i, V) (\{1, 2, \dots, n\} \times GF(2)^m \rightarrow \{1, 2, \dots, n\}) \quad (11)$$

що уявляє собою об'єднання 2^m перестановок $\pi_V = \pi^{(i)} \in S_n$, якщо для кожного фіксованого значення $V \in GF(2)^m$ задана деяка перестановка $\pi_V = \pi^{(\alpha(V))} \in S_n$, така, що $\pi_{n/m}(i, V) = \pi_V(i) = \pi^{(\alpha(V))}(i)$ [Определение 3.11. В кн.: Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография: скоростные шифры. - СПб.: БХВ-Петербург, 2002. - С.168]. Зміна форми тривимірних геометричних об'єктів 2 і 3 подана на Фіг.10 та Фіг.11.

На Фіг.12 поданий процес взаємодії тривимірного геометричного об'єкта вихідної інформації 2 і об'єкта ключа 3, де виділений елемент спільної взаємодії 4, над яким виконується операція перетворення (сума за модулем 2 та ін.). На Фіг.13 також проілюстрована взаємодія об'єктів 2 і 3, де один із них поданий із зміненою формою (зроблені керовані перестановки).

Керовану дискретну зміну форми зазначених об'єктів виконують за формулою ангармонійного коливання, що є результатом накладення (суперпозиції) двох гармонійних коливань $x_1 = A_1 \cos(\omega_1 t + \varphi_1)$ та $x_2 = A_2 \cos(\omega_2 t + \varphi_2)$, що мають різноманітні частоти й амплітуди, де $x(t)$ - періодична функція часу; A - максимальна амплітуда ко-

ливання; φ_1 - фаза коливання; $\omega = \frac{2\pi}{T} = 2\pi\nu$ - кругова або циклічна частота [Механические колебания. В кн.: Яворский Б.М., Детлаф А.А. Справочник по физике (для инженеров и студентов вузов). - Изд. седьмое, испр. - М.: Наука, Главная редакция физико-математической литературы, 1977. - С.109-113]. Результирує негармонійне коливання буде виглядати в такий спосіб

$$x = x_1 + x_2 = A(t) \cos[\omega_1 t + \varphi(t)] \quad (12)$$

де

$$A^2(t) = A_1^2 + A_2^2 + 2A_1A_2 \cos[\psi(t) - \varphi_1] \quad (13)$$

$$\operatorname{tg} \varphi(t) = \frac{A_1 \sin \varphi_1 + A_2 \sin \psi(t)}{A_1 \cos \varphi_1 + A_2 \cos \psi(t)} \quad (14)$$

та

$$\psi(t) = (\omega_2 - \omega_1)t + \varphi_1 \quad (15)$$

Пристрій перетворення інформації працює такою уявою.

У вихідному стані в змінному блоці керуючої пам'яті 28 утримуються команди перетворення інформації. Перед початком роботи пристрою, формувач адреси 38, формуючи адресу, указує на неінформативну частину змінного блока керуючої пам'яті 28. Операційний пристрій 22 знаходиться в режимі очікування. Регістри інформації 18 і ключа 19 обнулені. Перший 48 і другий 49 оперативні запам'ятовуючі пристрої не містять даних. Регістр завдання і результату 8 - не містить даних.

Після завантаження даних з обчислювальної системи 6 через двонаправлену шину 5 та через шинний двонаправлений вхід/вихід 7 у регістр завдання і результату 8, - активізується його вихід 64 готовності даних DSR, у результаті чого, за допомогою входу готовності даних 65 операційного пристрою 22, зміниться стан шини 30 сигнальних ознак. Далі, із третього виходу 37 регістра сигнальних ознак 32 активізується формувач адреси 38, і, через регістр адреси 39 вибираються зі змінного блока керуючої пам'яті 28 адреси, за якими в оперативні запам'ятовуючі пристрої 48 та 49 будуть розміщені дані. З виходу першої вихідної шини 27 змінного блока керуючої пам'яті 28, через регістр мікрокоманд 26, через вхідну шину мікрокоманд 25, а також із другого виходу 29 через регістр керування 24, через вхідну шину керування 23, - операційний пристрій 22 сформує адреси, які за допомогою його вихідної шини 59 будуть подані до входів регістрів фіксованих адрес 55 та 56. Завантаження адрес в них відбудеться при подачі на їхні керуючі входи 53 і 54 керуючого сигналу з восьмого виходу 52 регістра сигнальних ознак 32. З вихідних шин 61 та 62 адреси будуть подані до адресних входів першого 48 та другого 49 оперативних запам'ятовуючих пристроїв.

Через вхід 31 активізується регістр сигнальних ознак 32, який через третій його вихід 37 видасть керуючий сигнал формувачеві адреси 38. У результаті цього на виході регістра адреси 39 з'яв-

иться адреса вибірки зі змінного блока керуючої пам'яті 28. Мікрокоманда, що зберігається в змінному блоці керуючої пам'яті 28 за цією адресою, через його першу вихідну шину 27, через регістр мікрокоманд 26, через вхідну шину мікрокоманд 25, - надійде в операційний пристрій 22. Крім цього, через другу вихідну шину 29 змінного блока керуючої пам'яті 28, через регістр керування 24, через вхідну шину керування 23 в операційний пристрій 22 надійде команда керування, що характеризує параметри даних, які надходитимуть. При цьому операційний пристрій 22 за допомогою шини сигнальних ознак 30, через регістр сигнальних ознак 32, через його четвертий вихід 41, за допомогою керуючих входів 42 і 43 переключить перший 12 і другий 13 мультиплексори для передачі даних із регістра завдання і результату 8, через його вихідну шину 9, через другі входи 10 та 11 мультиплексорів 12 і 13 на їхні виходи 14 і 15. Дані ключа з вихідної шини 15 через вхід 17 регістра ключа 19, а також дані вихідної інформації з вихідної шини 14 через вхід 16 інформаційного регістра 18, - зможуть у них завантажитися при надходженні керуючих сигналів на керуючі входи 35 і 36, які надійдуть із першого 33 та другого 34 виходів регістра сигнальних ознак 32.

При виборі наступної мікрокоманди із змінного блока керуючої пам'яті 28 через регістр мікрокоманд 27 і через регістр керування 24, - операційний пристрій 22 через буферний регістр 58 (під впливом керуючого входу 57 від восьмого виходу 52 регістра сигнальних ознак) на інформаційні шини 62 оперативних запам'ятовуючих пристроїв 48 та 49 надішле дані, які під впливом керуючих сигналів запису 46 і 47 від регістра сигнальних ознак 32 запишуться у вигляді вихідної інформації в перший оперативний запам'ятовуючий пристрій 48, а дані ключа - у другий оперативний запам'ятовуючий пристрій 49. Після обнулення інформаційного регістра 18 та регістра ключа 19 через керуючі входи 36 і 35, відповідно, від регістра сигнальних ознак 32 (та зняття керуючих сигналів з інших компонентів пристрою), операція завантаження і перша частина підготовчого етапу вважаються завершеними.

Друга частина підготовчого етапу полягає в тому, що з вихідної інформації і ключа формують тривимірні геометричні об'єкти 2 і 3 (Фіг.2а-в). У пристрої перетворення інформації ця процедура, як і процедури проміжного етапу, буде виконуватися зчитуванням фрагментів даних з оперативних запам'ятовуючих пристроїв 48 і 49 (Фіг.14) через перші входи 68 та 69 першого 12 і другого 13 мультиплексорів (завантаження провадилося, як було зазначено вище, через другі входи 10 та 11) у регістри 18 та 19. З оперативних запам'ятовуючих пристроїв 48 і 49 для зчитування даних, потрібно з регістрів фіксованих адрес 55 та 56 задати адреси даних, які необхідно зчитувати, і далі, під впливом керуючих сигналів зчитування з регістра сигнальних ознак 32, подаваних на керуючі входи 46 і 47 оперативних запам'ятовуючих пристроїв 48 та 49. Потім під керуванням змінного блока керуючої пам'яті 28 операційним пристроєм 22 виконується процедура пересилки даних за новими адресами (формування яких описано вище), у такому поряд-

ку: вихідна інформаційна шина 59 операційного пристрою 22, буферний регістр 58, інформаційні вхідні шини 62 (адреси даних вибираються в тій же послідовності, як і при завантаженні даних в оперативні запам'ятовуючі пристрої 48 і 49). Точно так само виконується процедура зміни форми тривимірних геометричних об'єктів 2 і 3 (Фіг.10-11).

Вирішальний етап полягає в тому, що між даними вихідної інформації 2 і ключа 3 (Фіг.12-13), витягнутими з оперативних запам'ятовуючих пристроїв 48 і 49 (Фіг.14) та записаними в регістри 18 і 19, виконуються елементарні математичні і логічні операції, а змінені дані перетвореної інформації знову записуються в перший оперативний запам'ятовуючий пристрій 48. Ключ 3 (Фіг.1-13) при взаємодії з інформаційним повідомленням 2, може тільки змінювати координати і форму, а інформаційне повідомлення 2, крім того, - змінює власні значення (перетворюється).

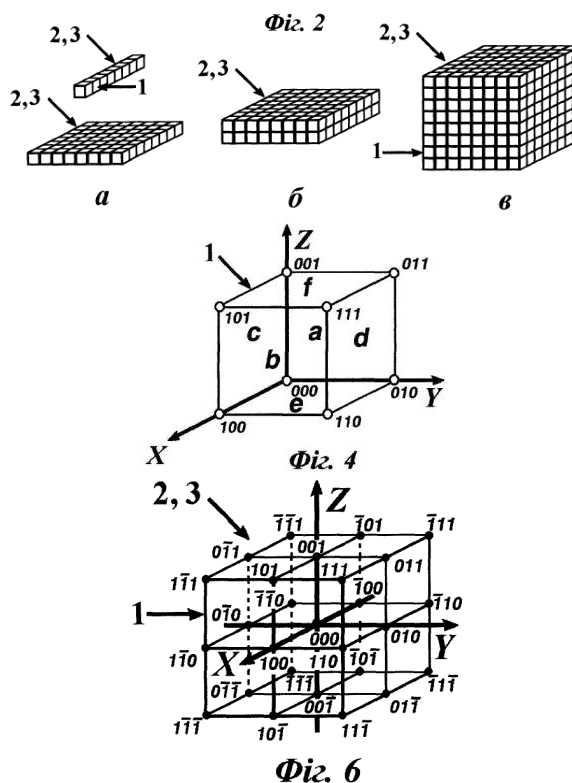
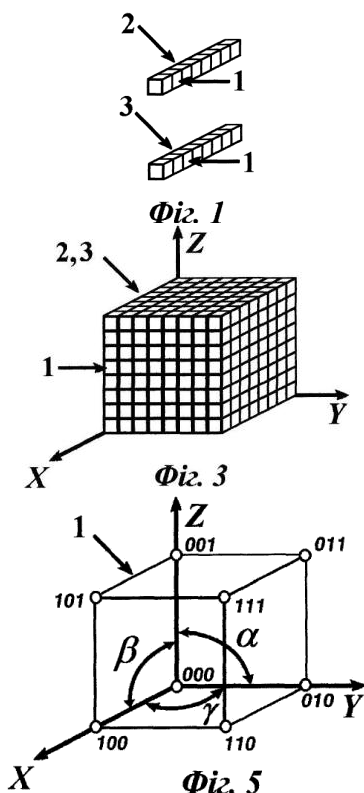
Після завершення всіх процедур, передбачених у змінному блоці керуючої пам'яті 28, перетворена інформація зчитується (як і в проміжних етапах) з оперативних запам'ятовуючих пристроїв 48 та 49 і записується в регістри 18 та 19. Далі, операційний пристрій 22 через буферний регістр 58,

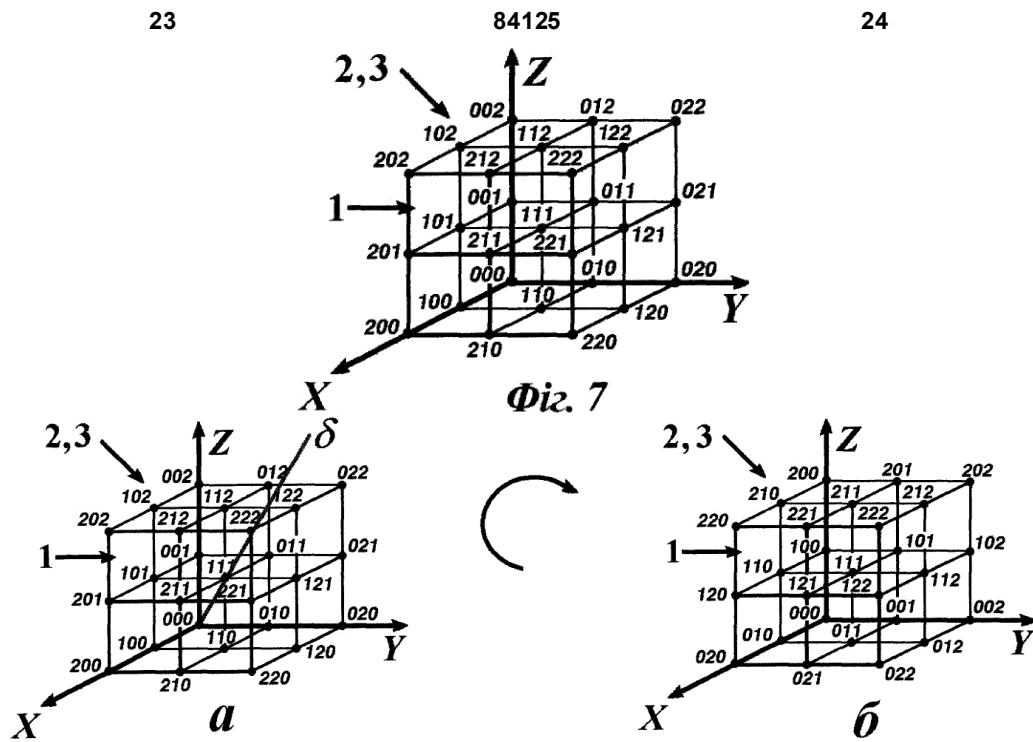
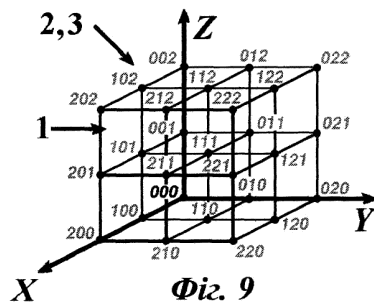
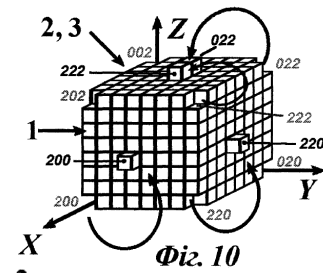
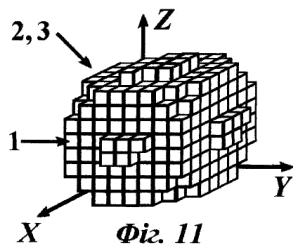
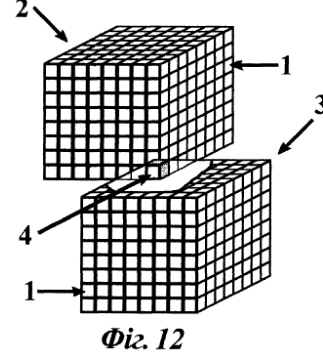
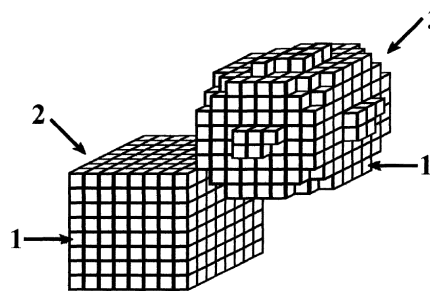
через вхід 63 регістра завдання і результату 8, - записує кінцевий результат у зазначений регістр 8 під впливом керуючих сигналів, що надходять на його керуючий вхід запису 51 від сьомого виходу 50 регістра сигнальних ознак 32. На завершальній стадії обнулюються регістри 18 і 19 (було описано вище), формувач адреси 38 формує неіснуючу адресу для змінного блоку керуючої пам'яті 28. Операційний пристрій 22 встановлюється в режим очікування.

Відновлення перетвореної інформації у вихідну виконується цим же пристроєм, але після заміни змінного блоку керуючої пам'яті 28. Тому що всі процедури необхідно виконувати в зворотній послідовності.

Таким чином, у порівнянні з прототипом, запропоновані спосіб перетворення інформації та пристрій для його здійснення дозволяють із високою швидкістю опрацювання перетворити вихідну інформацію до транспортування, а несанкціоноване розкриття було б неможливим навіть при наявності ключа.

Використання даного винаходу відкидає можливість існуючі методи перетворення інформації замінити на більш досконалі.



**Fig. 8****Fig. 9****Fig. 10****Fig. 11****Fig. 12****Fig. 13**

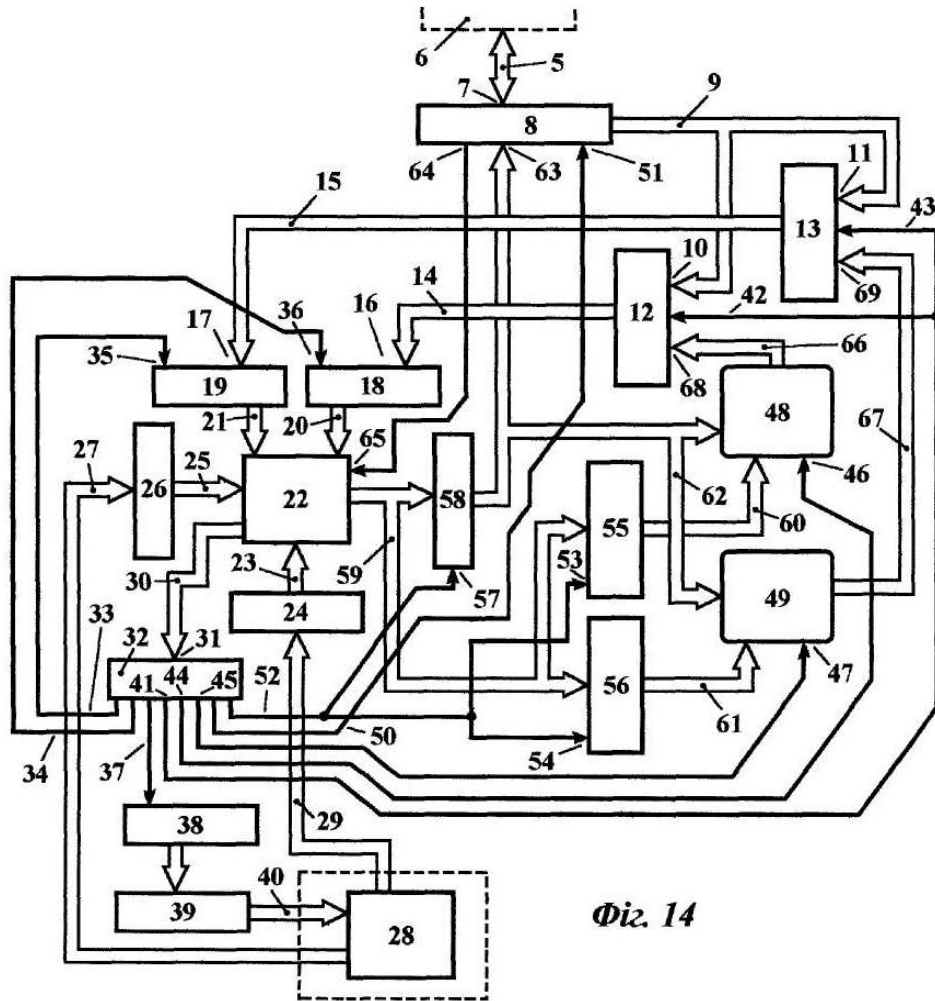


Fig. 14