УКРАЇНА

(19) UA (11) 54025 (13) U

(51) МПК (2009)
H04L 9/06

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

# ОПИС
## ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під відповідальність власника патенту

## (54) СПОСІБ ШИФРУВАННЯ ДАНИХ НА ОСНОВІ ТРЬОХ НЕСУМІСНИХ ГРУП ОПЕРАЦІЙ



**(21)** u201004698
**(22)** 20.04.2010
**(24)** 25.10.2010
**(46)** 25.10.2010, Бюл.№ 20, 2010 р.
**(72)** ЛУЖЕЦЬКИЙ ВОЛОДИМИР АНДРІЙОВИЧ, ДМИТРИШИН ОЛЕКСАНДР ВАСИЛЬОВИЧ, БАРИШЕВ ЮРІЙ ВОЛОДИМИРОВИЧ
**(73)** ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

**(57)** Спосіб шифрування даних на основі трьох несумісних груп операцій, який полягає в тому, що послідовність двійкових символів відкритого тексту розбивають на n-бітні блоки, кожний з яких послідовно розміщують в накопичувачі даних, при цьому дані $r_{i-1}$ з виходу накопичувача даних і дані відповідного підключа $K_i$ з виходу накопичувача секретного ключа кожного циклу надходять на вхід функції перетворення $f(r_{i-1}, K_i)$, яка є множенням значення даних $r_{i-1}$ на першу складову підключа зашифрування $A_i$ за модулем $m_i$, який є другою складовою підключа $K_i$, функцію $f(r_{i-1}, K_i)$ реалізують за допомогою пристрою множення за модулем, який **відрізняється** тим, що зашифрування даних виконують L циклів, перша та друга складові підключа $K_i (i = 1, 2, ..., L)$ містять по два коефіцієнти $A_i = A'_i A''_i$ і $m_i = m'_i \| m''_i, m''_i = 2^n - m'_i$, $A'_i = \gamma(m'_i), A''_i = \gamma(m''_i)$, які із секретними підключами $B_i$ та $C_i$ генерують на пристрої розширення ключів з початкового секретного ключа $k_0$ і заносять в накопичувач секретного ключа, підключ $B_i$ і вхідний блок даних $r_{i-1}$ подають на входи пристрою додавання за модулем $2^n$, який реалізує функцію $g(r_{i-1}, B_i) = r_{i-1}, B_i$, отриманий результат та складові підключа $K_i$ подають на входи пристрою, що реалізує функцію $f(g(r_{i-1}, B_i), K_i) = g(r_{i-1}, B_i) \cdot A'_i \bmod m'_i$, якщо $g(r_{i-1}, B_i) < m'_i$ або $f(g(r_{i-1}, B_i), K_i) = (g(r_{i-1}, B_i) - m'_i \cdot A''_i \bmod m'' + m'_i$, якщо $g(r_{i-1}, B_i) \geq m'_i$, перетворений блок даних і підключ $C_i$ надходять на входи суматора за модулем 2, який реалізує функцію $v(f(g(r_{i-1}, B_i), K_i), B_i) = f(g(r_{i-1}, B_i), K_i) \oplus B_i$, а при розшифруванні, яке проводять в оберненому порядку по відношенню до зашифрування, на пристрої розширення ключів генерують секретні підключі $B'_i = 2^n - B_i$, $C'_i = C_i$ і складові підключа $K'_i, m'_i, m''_i$, $A'_i = \gamma^{-1}(m'_i), A''_i = \gamma^{-1}(m''_i)$, які заносять в накопичувач секретного ключа і подають в зворотному порядку, в кожному циклі блок даних $r_{i-1}$ і відповідний підключ $C'_i$ з виходу накопичувача секретного ключа подають на входи суматор за модулем 2, що реалізує функцію $v(r_{i-1}, C'_i) = r_{i-1} \oplus C'_i$, перетворений блок даних і відповідні складові підключа $K'_i$ з виходу накопичувача секретного ключа подають на входи пристрою, який реалізує функцію $f(v(r_{i-1}, C'_i), K_i) = v(r_{i-1}, C'_i) \cdot A''_i \bmod m'_i$, якщо $v(r_{i-1}, C'_i) < m'_i$ або $f(v(r_{i-1}, C'_i), K_i) = (v(r_{i-1}, C'_i) - m'_i) \cdot A''_i \bmod m'' + m'_i$, якщо $v(r_{i-1}, C'_i) \geq m'_i$, отриманий результат і відповідний підключ $B'_i$ з виходу накопичувача секретного ключа подають на входи пристрою додавання за модулем $2^n$, що реалізує функцію $g(f(v(r_{i-1}, C'_i), K'_i), B'_i) = f(v(r_{i-1}, C'_i), K'_i) + B'_i)$.



(19) UA (11) 54025 (13) U

Корисна модель відноситься до галузі криптографічного захисту інформації і може бути використана в засобах шифрування та у системах передачі конфіденційної інформації.

Відомий спосіб шифрування даних для систем обробки в ЕОМ, який полягає в тому, що послідовність двійкових символів відкритого тексту розбивають на n бітні блоки, кожний з котрих розбивають у свою чергу на правий $R_0$ та лівий $L_0$ півблоки по n/2 біти, які розміщують у відповідних накопичувачах, зашифрування котрих включає в себе 1 циклів, при цьому дані правого півблока $R_{i-1}$ використовують для обчислення різниці за модулем m зі значенням лівого півблока $L_{i-1}$ і цю різницю заносять у накопичувач правого півблока наступного циклу так, що $R_i=R_{i-1}-L_{i-1}(modm)$, вихідні дані циклової функції заносять у накопичувач лівого півблока, тобто $L_i=f(R_{i-1}K_i)$, при цьому як циклову функцію перетворення використовують модульне множення значення $R_{i-1}$ накопичувача $N_{i-1}$ правого півблока на ключ зашифрування $K_i\equiv(K_i)^E(modm)$, так що у накопичувач $N_i$ лівого півблока наступного циклу заносять число $L_i\equiv R_{i-1}\cdot(K_i)^E$ (modm), тобто $f(R_{i-1}, K_i) \equiv R_{i-1}\cdot(K_i)^E$ (modm), а при розшифруванні, яке проводиться в оберненому порядку по відношенню до зашифрування, у кожному циклі в основному режимі значення $L_{j-1}$ накопичувача $N_{i-1}$ лівого півблока подають на вхід циклової функції перетворення $g(L_{i-1}, K_{I+j+1})$, при цьому як циклову функцію перетворення використовують модульне множення значення $L_{j-1}$ накопичувача $N_{i-1}$ лівого півблока на ключ розшифрування $K_i\equiv(K_{I-j+1})^{-E}(modm)$, так що у накопичувач $N_i$ правого півблока наступного циклу заноситься число $R_j \equiv L_{j-1}\cdot K''_j(modm)$, тобто $R_j \equiv f'(L_{j-1},K_{I-j+1}) \equiv L_{j-1}\cdot(K_{I-j+1})^{-E}(modm)$, а значення накопичувана правого півблока $R_{j-i}$ сумують за модулем m зі значенням виходу циклової функції перетворення $g(L_{j-1}, K_{i-j-1})$ і результат заносять в накопичувач $N_i$ лівого півблока наступного циклу, тобто $L_j = R_{j-1}+g(L_{j-1}, K_{I-j+1})(modm)$, а в режимі використання лазівки обчислюють піднесення значення $L_{j-1}$ накопичувача $N_{j-1}$ лівого півблока до степеня D за модулем m, тобто обчислюють $X_{j-1} = (L_{j-1})^D(modm)$, і потім з отриманого числа обчислюють корінь степеня D за модулем m, і в накопичувач $N_i$ правого півблока заносять число $R_j = \sqrt[D]{X_{j-1}}$, тобто циклова функція перетворення має вигляд $h(L_{j-1}, L(m))= \sqrt[D]{X_{j-1}}(\mathrm{mod}\, m)$, а значення накопичувача правого півблока $R_{j-1}$ сумують за модулем m зі значенням виходу тепер вже циклової функції перетворення $h(L_{j-1},L(m))$, і результат заносять в накопичувач $N_i$ лівого півблока наступного циклу, тобто $L_j =R_{j-1}+h(L_{i-1},L(m))(modm)$, де m=pq - модуль перетворення, котрий є добутком двох простих чисел p і q, L(m) - узагальнена функція Ейлера числа m, показники степенів E і D пов'язані умовою $ED\equiv0(modL(m))$ (Патент України № 50199, МПК H04L9/06, Бюл. №10, 2002р.).

Недоліками аналогу є недостатня швидкодія роботи шифру, за рахунок великої обчислювальної складності отримання ключа зашифрування циклових функції та збільшення зашифрованого блоку даних на два біти порівняно із блоком відкритого тексту, що збільшує складність реалізації способу.

Найбільш близьким за сукупністю ознак до запропонованого є спосіб шифрування даних для систем обробки в ЕОМ, який полягає в тому, що послідовність двійкових символів відкритого тексту розбивають на n-бітні блоки, кожний з яких послідовно розміщують в накопичувачі, надалі накопичувачі даних, зашифрування яких складається з чотирьох циклів, при цьому дані $r_{i-1}$ з виходу (i-1)-го накопичувача тексту, надалі накопичувача даних, і дані відповідного підключа $K_i$ з виходу i-го накопичувана секретного ключа кожного циклу надходять на вхід циклової функції, надалі функції, перетворення $f(r_{i-1}, K_i)$, яка є множенням значення даних $r_{i-1}$ на першу складову підключа зашифрування $A_i$ за модулем $m_i$, який є другою складовою підключа $K_i$, які розміщують в і-му накопичувачі секретного ключа, а функцію $f(r_{i-1}, K_i) \equiv r_{i-1}\cdot A_i \bmod m_i$ реалізують за допомогою блока множення за модулем, надалі пристрій множення за модулем, на вхід якого додатково подають значення модуля $m_i$ з виходу і-го накопичувача секретного ключа, а при розшифруванні, яке проводять в оберненому порядку по відношенню до зашифрування, у кожному циклі, дані $r_{i-1}$ з виходу (i-1)-го накопичувача і дані відповідного підключа $K_{5-i}$ з виходу (5-i)-го накопичувача секретного ключа подають на вхід функції перетворення $f(r_{i-1}, K_{5-i})=r_{i-1}\cdot A^{-1}_{5-i} \bmod m_{5-i}$, яка є множенням значення $r_{i-1}$ з (i-l)-го накопичувача даних на першу складову підключа розшифрування за модулем, який є другою складовою підключа розшифрування, які подають з (5-i)-го накопичувача секретного ключа і реалізують за допомогою пристрою множення за модулем (Патент України № 38795, МПК H04L9/06, Бюл. №2, 2009р.).

Недоліками способу-прототипу є те, що значення кожного наступного модуля $m_i$, яке подається на вхід функції перетворення $f(r_{i-1}, K_i)$ залежить від значення попереднього модуля, що зменшує криптографічну стійкість шифру та збільшення зашифрованого блоку даних на один біт порівняно із блоком відкритого тексту, що збільшує складність реалізації способу.

В основу корисної моделі поставлена задача створення способу шифрування даних на основі трьох несумісних груп операцій, в якому за рахунок використання незалежних значень модулів ті та введення двох додаткових несумісних груп операцій досягається можливість підвищення криптографічної стійкості шифру і за рахунок використання значень модулів ті тієї ж розрядності, що і блоки відкритих текстів досягається можливість усунення надлишковості зашифрованих блоків даних, що призводить до зменшення складності реалізації способу.

Поставлена задача вирішується тим, що в спосіб шифрування даних на основі трьох несумісних груп операцій, який полягає в тому, що послідовність двійкових символів відкритого тексту розбивають на n-бітні блоки, кожний з яких послідовно розміщують в накопичувані даних, при цьому дані

$r_{i-1}$ з виходу накопичувана даних, і дані відповідного підключа $K_i$ з виходу накопичувача секретного ключа кожного циклу надходять на вхід функції перетворення $f(r_{i-1}, K_i)$, яка є множенням значення даних $r_{i-1}$ на першу складову підключа зашифрування $A_i$ за модулем $m_i$, який є другою складовою підключа $K_i$, функцію $f(r_{i-1}, K_i)$ реалізують за допомогою пристрою множення за модулем, зашифрування даних виконують L циклів, перша та друга складові підключа $K_i$ (i=1, 2, ..., L) містять по два коефіцієнти $A_i = A_i' \| A_i''$ і $m_i = m_i' \| m_i'', m_i'' = 2^n - m_i'$, $A_i' = \gamma(m_i'), A_i'' = \gamma(m_i'')$, які із секретними підключами $B_i$ та $C_i$ генерують на пристрої розширення ключів з початкового секретного ключа $k_0$ і заносять в накопичувач секретного ключа, підключ $B_i$ і вхідний блок даних $r_{i-1}$ подають на входи пристрою додавання за модулем $2^n$, який реалізує функцію $g(r_{i-1}, B_i) = r_{i-1} + B_i$, отриманий результат та складові підключа $K_i$ подають на входи пристрою, що реалізує функцію $f(g(r_{i-1}, Bi), K_i) = g(r_{i-1}, B_i) \cdot A'_i \bmod m'_i$, якщо $g(r_{i-1}, B_i < m'_i$ або $f(g(r_{i-1}, B_i), K_i) = (g(r_{i-1}, B_i) - m'_i) \cdot A''_i \bmod m''_i + m'_i$, якщо $g(r_{i-1}, B_i) \geq m'_i$, перетворений блок даних і підключ $C_i$ надходять на входи суматора за модулем 2, який реалізує функцію $v(f(g(r_{i-1}, B_i), K_i), B_i) = f(g(r_{i-1}, B_i), K_i) \oplus B_i$, а при розшифруванні, яке проводять в оберненому порядку по відношенню до зашифрування, на пристрої розширення ключів генерують секретні підключі $B'_i = 2^n - B_i$, $C'_i = C_i$ і складові підключа $K'_i$: $m'_i$, $m''_i$, $A_i' = \gamma^{-1}(m_i'), A_i'' = \gamma^{-1}(m_i'')$, які заносять в накопичувач секретного ключа і подають в зворотному порядку, в кожному циклі блок даних $r_{i-1}$ і відповідний підключ $C'_i$ з виходу накопичувача секретного ключа подають на входи суматор за модулем 2, що реалізує функцію $v(r_{i-1}, C'_i) = r_{i-1} \oplus C'_i$, перетворений блок даних і відповідні складові підключа $K'_i$ з виходу накопичувача секретного ключа подають на входи пристрою, який реалізує функцію $f(v(r_{i-1}, C'_i), K'_i) = v(r_{i-1}, C'_i) \cdot A'_i \bmod m'_i$, якщо $v(r_{i-1}, C'_i) < m'_i$ або $f(v(r_{i-1}, C'_i), K'_i = (v(r_{i-1}, C'_i) - m'_i) \cdot A''_i \bmod m''_i + m'_i$, якщо $v(r_{i-1}, C'_i) \geq m'_i$, отриманий результат і відповідний підключ $B'_i$ з виходу накопичувача секретного ключа подають на входи пристрою додавання за модулем $2^n$, що реалізує функцію $g(f(v(r_{i-1}, C'_i), K'_i), B'_i) = f(v(r_{i-1}, C_i), K'_i) + B'_i$.

На Фіг.1 зображена схема пристрою, який виконує зашифрування блоку даних; на Фіг.2 - схема пристрою, що виконує розшифрування зашифрованого блоку даних; на Фіг.3 - схема пристрою, який реалізує функцію $f(r_{i-1}, K_i)$.

Пристрій, що зображений на Фіг.1 містить пристрій розширення ключів 1, вхід якого з'єднано з першим входом даного пристрою, виходи пристрою розширення ключів 1 з'єднано з входами накопичувача секретного ключа 2, перший, другий, третій та четвертий виходи якого з'єднано з першим, другим, третім та четвертим входами пристрою 3, який реалізує функцію $f(r_{i-1}, K_i)$, накопичувач даних 4, вихід якого з'єднано з першим входом першого блока комутації 5, вихід якого з'єднано з першим входом першого пристрою додавання за модулем $2^n$ 6, п'ятий вихід накопичувача секретного ключа 2 з'єднано з входом другого блока комутації 7, перший вихід якого з'єднано з другим входом першого пристрою додавання за модулем $2^n$ 6, вихід якого з'єднано з п'ятим входом пристрою 3, вихід якого з'єднано з першим входом суматора за модулем 2 8, вихід якого є виходом даного пристрою і з'єднано з другим входом першого блока комутації 5, другий вихід другого блока комутації 7 з'єднано з другим входом суматора за модулем 2 8, вхід накопичувача даних 4 з'єднано з другим входом даного пристрою.

Пристрій, що зображений на Фіг.2 містить пристрій розширення ключів 1, вхід якого з'єднано з першим входом даного пристрою, виходи пристрою розширення ключів 1 з'єднано з входами накопичувача секретного ключа 2, перший, другий, третій та четвертий виходи якого з'єднано з першим, другим, третім та четвертим входами пристрою 3, який реалізує функцію $f(r_{i-1}, K_i)$, накопичувач даних 4, вхід якого з'єднано з другим входом даного пристрою, вихід накопичувача даних 4 з'єднано з першим входом першого блока комутації 5, вихід якого з'єднано з першим входом суматора за модулем 2 8, вихід якого з'єднано з п'ятим входом пристрою 3, вихід якого з'єднано з першим входом першого пристрою додавання за модулем $2^n$ 6, вихід якого є виходом даного пристрою і з'єднано з другим входом першого блока комутації 5, п'ятий вихід накопичувача секретного ключа 2 з'єднано з входом другого блока комутації 7, перший вихід якого з'єднано з другим входом першого пристрою додавання за модулем $2^n$ 6, другий вихід другого блока комутації 7 з'єднано з другим входом суматора за модулем 2 8.

Пристрій, що зображений на Фіг.3 містить пристрій порівняння 9, перший та другий вхід якого з'єднано з першим та другим входом даного пристрою, вихід пристрою порівняння 9 з'єднано з першим входом третього блока комутації 10, першим входом четвертого блока комутації 11, першим входом п'ятого блока комутації 12 та першим входом шостого блока комутації 13, другі входи третього блоку комутації 10 і шостого блоку комутації 13 з'єднано з другим входом даного пристрою, вихід третього блоку комутації 10 з'єднано з першим входом пристрою віднімання за модулем $2^n$ 14, другий вхід якого з'єднано з першим входом даного пристрою, вихід пристрою віднімання за модулем $2^n$ 14 з'єднано з першим входом пристрою множення за модулем 15, другий та третій входи якого з'єднано з виходами четвертого 11 та п'ятого 12 блоків комутації відповідно, другий та третій входи четвертого блоку комутації 11 з'єднано з другим та третім входами даного пристрою відповідно, другий та третій входи п'ятого блоку комутації 12 з'єднано з четвертим та п'ятим входами даного пристрою відповідно, вихід регістру 17 з'єднано з третіми входами третього блоку комутації 10 та шостого блоку комутації 13, вихід пристрою множення за модулем 15 з'єднано з першим входом другого пристрою додавання за модулем $2^n$ 16, другий вхід якого з'єднано з виходом шостого блоку комутації 13, вихід другого пристрою додавання за модулем $2^n$ 16 з'єднано з виходом даного пристрою.

Спосіб шифрування даних на основі трьох несумісних груп операцій здійснюють таким чином. Під час зашифрування блоку даних, на пристрій розширення ключів 1 (див. Фіг.1) надсилають початковий секретний ключ $k_0$ з якого для кожного циклу генерують $B_i$, $C_i$ і $d_i$, якщо $d_i \le 2^{n-2}$, то обчислюють $m'_i=d_i+2^{n-1}$ та використовують такі константи a=-1, b=-2, c=-4, якщо $d_i \le 3\cdot 2^{n-2}$, то $m'_i=d_i-2^{n-1}$ та використовують такі константи a=-1, b=-2, c=-4, в протилежному випадку $m'_i=d_i$ та використовують такі константи a=1, b=2, c=4, обчислюють $m''_i=2^n-m'_i$. Значення множників $A'_i=\gamma(m'_i)$ та $A''_i=\gamma(m''_i)$ розраховують на пристрої розширення ключів згідно такої функції

$$\gamma(m'_i)=\begin{cases}(m'_i+a)>>1, \text{ якщо } m'_{i0}=1,\\ (m'_i+b)>>, \text{ якщо } m'_{i0}=0, \text{ і } m'_{i1}=0,\\ (m'_i+c)>>1, \text{ якщо } m'_{i0}=0, \text{ і } m'_{i1}=1,\end{cases}$$

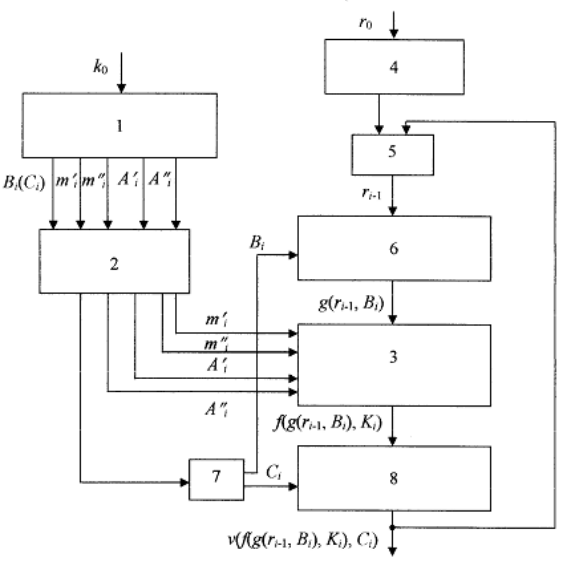
де $m'_{i0}$ - значення 0-го біта $m'_i$, $m'_{i1}$ - значення 1-го біта $m'_i$, $\gamma(m''_i)$ розраховують так само. Отримані складові підключа $K_i$ та підключі $B_i$ і $C_i$ надходять в накопичувач секретного ключа 2 з якого підключ $B_i$ через другий блок комутації 7 та вхідний блок даних $r_{i-1}$ через перший блок комутації 5 надходять на перший пристрій додавання за модулем $2^n$ 6, отриманий результат та складові підключа $K_i$ надходять на пристрій 3, який реалізує функцію $f(g(r_{i-1}, B_i), K_i)$, перетворений блок даних та підключ $C_i$ з виходу накопичувача секретного ключа 2 через другий блок комутації 7 надходять на суматор за модулем 2 8, отриманий результат $r_i=v(f(g(r_{i-1}, B_i), K_i), C_i)$ надсилають на перший блок комутації 5. Вище описані дії виконують L циклів, після завершення яких зашифрований блок даних подається на вихід пристрою зашифрування з виходу суматора за модулем 2 8.

Розшифрування зашифрованого блоку даних виконують в оберненому порядку по відношенню до зашифрування. На пристрій розширення ключів 1 (див. Фіг.2) надсилають початковий секретний ключ $k_0$ з якого для кожного циклу генерують $B_i$, $C_i$ і $d_i$ з якого, за тим же принципом, що і під час зашифрування, обчислюють значення $m'_i$ і $m''_i$ та обирають константи a, b і c. Значення множників $A'_i=\gamma^{-1}(m'_i)$, та $A''_i=\gamma^{-1}(m''_i)$ розраховують на пристрої розширення ключів згідно такої функції

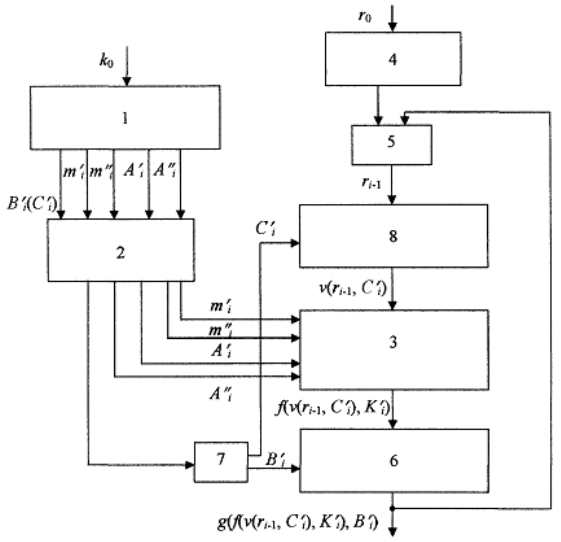
$$\gamma^{-1}(m'_i)=\begin{cases}2, \text{якщо } a=1 \text{ і } m'_{i0}=1,\\ m'_i-2, \text{якщо } a=-1 \text{ і } m'_{i0}=1,\\ (m'_i+b)>>1, \text{якщо } m'_{i0}=0 \text{ і } m'_{i1}=0,\\ (m'_i+4)>>1, \text{якщо } c=4, m'_{i0}=m'_{i2}=0 \text{ і } m'_{i1}=1,\\ (m'_i+\gamma(m'_i))>>1, \text{якщо } c=4, m'_{i0}=0 \text{ і } m'_{i1}=m'_{i2}=1,\\ (m'_i-\gamma(m'_i))>>1-1, \text{якщо } c=-4, m'_{i0}=0 \text{ і } m'_{i1}=m'_{i2}=1,\\ (m'_i+\gamma(m'_i))>>1+1, \text{якщо } c=-4, m'_{i0}=0 \text{ і } m'_{i2}=m'_{12}=1,\end{cases}$$

де $m'_{i0}, m'_{i1}, m'_{i2}$ - значення 0-го, 1-го та 2-го бітів відповідно, $\gamma^{-1}(m'_i)$ розраховують так само. Розраховані складові підключа $K'_i$ та підключі $B'_i=2^n-B_i$ і $C'_i=C_i$, в оберненому порядку, надходять в накопичувач секретного ключа 2, з якого підключ $C'_i$ через другий блок комутації 7 та вхідний блок даних $r_{i-1}$ через перший блок комутації 5 надходить на суматор за модулем 2 8, з виходу якого перетворений блок даних і складові підключа $K'_i$ надходять на пристрій 3, який реалізує функцію $f(v(r_{i-1}, C'_i), K'_i)$, отриманий результат з виходу пристрою 3 та підключ $B'_i$ з виходу накопичувача секретного ключа 2 через другий блок комутації 7 надходять на перший пристрій додавання за модулем $2^n$ 6, з виходу якого отримують перетворений блок даних $r_i=g(f(v(r_{i-1}, C'_i), K'_i), B'_i)$, який надсилають на перший блок комутації 7. Вище описані дії виконують L циклів, після завершення яких розшифрований блок даних подають на вихід пристрою розшифрування з виходу прілого пристрою додавання за модулем $2^n$ 6.

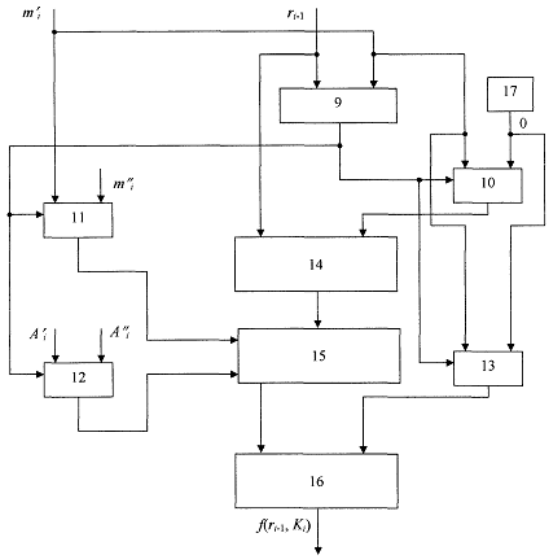
В регістр 17, пристрою, що реалізує функцію $f(r_{i-1}, K_i)$ (див. Фіг.3), заносять 0, на входи пристрою порівняння 9 подають вхідний блок даних $r_{i-1}$, який шифруватимуть та модуль $m'_i$, якщо $r_{i-1} < m'_i$, то на перші (керуючі) входи блоків комутації 10, 11, 12 і 13 подають логічну одиницю, тоді на перший вхід пристрою віднімання за модулем $2^n$ 14 з третього блока комутації 10 подають 0, на другий та третій входи пристрою множення за модулем 15 з виходу блоків комутації 11 і 12 подають значення $m'_i$ та $A'_i$ відповідно, на другий вхід другого пристрою додавання за модулем $2^n$ 16 надсилають 0, з виходу шостого блока комутації 13, якщо $r_{i-1} \ge m'_i$, то на перші входи блоків комутації 10, 11, 12 і 13 подають логічний нуль, тоді на перший вхід пристрою віднімання за модулем $2^n$ 14 з третього блока комутації 10 надсилають $m'_i$, на другий та третій входи пристрою множення за модулем 15 з виходу блоків комутації 11 і 12 подають значення $m''_i$ та $A''_i$ відповідно, на другий вхід другого пристрою додавання за модулем $2^n$ 16 надсилають $r_{i-1}$ з виходу шостого блока комутації 13. Вхідний блок даних $r_{i-1}$ надходить на пристрій віднімання за модулем $2^n$ 14, на якому від $r_{i-1}$ віднімають значення, яке надходить з третього блоку комутації 10, отриманий результат з виходу пристрою віднімання за модулем $2^n$ 14 надходить на пристрій множення за модулем 15, результат множення надходить на другий пристрій додавання за модулем $2^n$ 16, де його додають із значенням, яке надходить з шостого блоку комутації 13. Перетворений блок даних надходить на вихід пристрою, який реалізує функцію $f(r_{i-1}, K_i)$.




Фіг. 1




Фіг. 2




Фіг. 3

Комп'ютерна верстка Л. Купенко Підписне Тираж 26 прим.

Міністерство освіти і науки України
Державний департамент інтелектуальної власності, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

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