УКРАЇНА

(19) UA (11) 53494 (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 ДВОХ НЕСУМІСНИХ ГРУП ОПЕРАЦІЙ

(21) u201003864
(22) 06.04.2010
(24) 11.10.2010
(46) 11.10.2010, Бюл.№ 19, 2010 р.
(72) ЛУЖЕЦЬКИЙ ВОЛОДИМИР АНДРІЙОВИЧ, ДМИТРИШИН ОЛЕКСАНДР ВАСИЛЬОВИЧ
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

(57) Спосіб шифрування даних на основі двох 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 секретним підключем B_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 $f(g(r_{i-1}, B_i), K_i)=(g(r_{i-1}, B_i)-m'_i)\cdot A''_i \bmod m''_i+m'_i$, якщо $g(r_{i-1}, B_i)\geq m'_i$, а при розшифруванні, яке проводять в оберненому порядку по відношенню до зашифрування, на пристрої розширення ключів генерують складові підключа K'_i: m'_i, m''_i, $A'_i=\gamma^{-1}(m'_i)$, $A''_i=\gamma^{-1}(m''_i)$ і $B'_i=2^n-B_i$, які заносять в накопичувач секретного ключа і подають в зворотному порядку, в кожному циклі блок даних r_{i-1} і відповідні складові підключа K'_i з виходу накопичувача секретного ключа подають на входи пристрою, який реалізує функцію $f(r_{i-1}, K'_i)=r_{i-1}\cdot A'_i \bmod m'_i$, якщо $r_{i-1}<m'_i$, або $f(r_{i-1}, K'_i)=(r_{i-1}-m'_i)\cdot A''_i \bmod m''_i+m'_i$, якщо $r_{i-1}\geq m'_i$, отриманий результат і відповідний підключ B'_i з виходу накопичувача секретного ключа подають на входи пристрою додавання за модулем 2^n, що реалізує фунфункцію $g(f(r_{i-1}, K'_i), B'_i)=f(r_{i-1}, K'_i)+B'_i$.

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 п 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 $R_i=R_{i-1}-L_{i-1}$,(mod m), 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 $K_i'\equiv(K_i)^E$(mod m), так що у накопичувач N_i лівого півблока наступного циклу заносять число $L_i\equiv R_{i-1}\cdot(K_i)^H$(mod m), тобто $f(R_{i-1},K_i)\equiv R_{i-1}\cdot(K_i)^E$(mod m), а при розшифруванні, яке проводиться в оберненому порядку по відношенню до зашифрування, у кожному циклі в основному режимі значення L_{j-l} накопичувача N_{j-1} лівого півблока подають на вхід циклової функції перетворення $g(L_{i-1},K_{l-j+1})$, при цьому як циклову функцію перетворення використовують модульне множення значення L_{j-1} накопичувача N_{i-1} лівого півблока на ключ розшифрування $K_j''\equiv(K_{l-j+l})^{-E}$(mod m), так що у накопичувач N_i правого півблока наступного циклу заноситься число $R_j\equiv L_{j-1}\cdot K_j''$(mod m), тобто $R_j\equiv f'(L_{j-1},K_{l-j+1})\equiv L_{j-1}\cdot(K_{l-j+l})^{-E}$(mod m), а значення накопичувача правого півблока R_{i-1} сумують за модулем m зі значенням виходу циклової функції перетворення $g(L_{j-1},K_{l-j+l})$ і результат заносять в накопичувач N_i лівого півблока наступного циклу, тобто $L_j=R_{j-1}+g(L_{j-1},(K_{l-j+l})$(mod m), а в режимі вико-

(19) UA (11) 53494 (13) U

ристання лазівки обчислюють піднесення значення L_{j-1} накопичувача N_{j-1} лівого півблока до степеня D за модулем m, тобто обчислюють $X_{j-1}=(L_{j-1})^D(\mathrm{mod}\ m)$, і потім з отриманого числа обчислюють корінь степеня D за модулем m, і в накопичувач N_j 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 $L_i=R_{j-1}+h(L_{j-1},L(m))(\mathrm{mod}\ m)$, 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 $ED\equiv 0(\mathrm{mod}\ L(m))$ (Патент України № 50199, МПК H04L9/06, Бюл. № 10, 2002 р.).

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 накопичувача 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 накопичувані секретного ключа, а функцію $f(r_{i-1}, K_i)\equiv r_{i-1}\cdot A_i \mod m_i$ 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 $f(r_{i-1},K_{5-i})\equiv r_{i-1}\cdot A_{5-i}^{-1}\mathrm{mod}m_{5-i}$, яка є множенням значення r_{i-1} з (i-1)-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, 2009 р.).

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 двох несумісних груп операцій, в якому за рахунок використання незалежних значень модулів m_i та введення додаткової арифметичної операції досягається можливість підвищення криптографічної стійкості шифру і за рахунок використання значень модулів m_i 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 двох 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 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 секретним підключем B_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 $f(g(r_{i-1}, B_i), K_i)=g(r_{i-1}, B_i)\cdot A'_i \mod m'_i$, якщо $g(r_{i-1}, B_i)<m'_i$ або $f(g(r_{i-1}, B_i), K_i)=g(r_{i-1}, B_i)-m'_i)\cdot A''_i \mod m''_i+m'_i$, якщо $g(r_{i-1}, B_i)\geq m'_i$, а при розшифруванні, яке проводять в оберненому порядку по відношенню до зашифрування, на пристрої розширення ключів генерують складові підключа K'_i: m'_i, m''_i, $A'_i=\gamma^{-1}(m'_i)$, $A''_i=\gamma^{-1}(m''_i)$ і $B'_i=2^n-B_i$, які заносять в накопичувач секретного ключа і подають в зворотному порядку, в кожному циклі блок даних r_{i-1} і відповідні складові підключа K'_i з виходу накопичувача секретного ключа подають на входи пристрою, який реалізує функцію $f(r_{i-1}, K'_i)=r_{i-1}\cdot A'_i \mod m'_i$, якщо $r_{i-1}<m'_i$ або $f(r_{i-1}, K'_i)=(r_{i-1}-m'_i)\cdot A''_i \mod m''_i+m'_i$, якщо $r_{i-1}\geq m'_i$, отриманий результат і відповідний підключ B'_i з виходу накопичувача секретного ключа подають на входи пристрою додавання за модулем 2^n, що реалізує функцію $g(f(r_{i-1}, K'_i), B'_i)=f(r_{i-1}, K'_i)+B'_i$.

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

Пристрій, що зображений на фіг. 1 містить пристрій порівняння 1, перший та другий вхід якого з'єднано з першим та другим входом даного при-

строю, вихід пристрою порівняння 1 з'єднано з першим входом першого блока комутації 2, першим входом другого блока комутації 3, першим входом третього блока комутації 4 та першим входом четвертого блока комутації 5, другі входи першого блоку комутації 2 і четвертого блоку комутації 5 з'єднано з другим входом даного пристрою, вихід блоку комутації 2 з'єднано з першим входом пристрою віднімання за модулем 2^n 6, другий вхід якого з'єднано з першим входом даного пристрою, вихід пристрою віднімання за модулем 2^n 6 з'єднано з першим входом пристрою множення за модулем 7, другий та третій входи якого з'єднано з виходами другого 3 та третього 4 блоків комутації відповідно, другий та третій входи другого блоку комутації 3 з'єднано з другим та третім входами даного пристрою відповідно, другий та третій входи третього блоку комутації 4 з'єднано з четвертим та п'ятим входами даного пристрою відповідно, вихід регістру 8 з'єднано з третіми входами першого блоку комутації 2 та четвертого блоку комутації 5, вихід пристрою множення за модулем 7 з'єднано з першим входом пристрою додавання за модулем 2^n 9, другий вхід якого з'єднано з виходом четвертого блоку комутації 5, вихід пристрою додавання за модулем 2^n 9 з'єднано з виходом даного пристрою.

Пристрій, що зображений на фіг. 2 містить накопичувач даних 13, вихід якого з'єднано з першим входом блока комутації 14, вихід якого з'єднано з першим входом пристрою додавання за модулем 2^n 15, пристрій розширення ключів 10, вхід якого з'єднано з першим входом даного пристрою, виходи пристрою розширення ключів 10 з'єднано з входами накопичувача секретного ключа 11, перший, другий, третій та четвертий виходи якого з'єднано з першим, другим, третім та четвертим входами пристрою 12, який реалізує функцію $f(r_{i-1}, K_i)$, п'ятий вихід накопичувача секретного ключа 11 з'єднано з другим входом пристрою додавання за модулем 2^n 15, вихід якого з'єднано з п'ятим входом пристрою 12, вихід якого є виходом даного пристрою і з'єднано з другим входом блока комутації 14, вхід накопичувана даних 13 з'єднано з другим входом даного пристрою.

Пристрій, що зображений на фіг. 3 містить пристрій розширення ключів 10, вхід якого з'єднано з першим входом даного пристрою, виходи пристрою розширення ключів 10 з'єднано з входами накопичувача секретного ключа 11, перший, другий, третій та четвертий виходи якого з'єднано з першим, другим, третім та четвертим входами пристрою 12, який реалізує функцію $f(r_{i-1}, K_i)$, накопичувач даних 13, вхід якого з'єднано з другим входом даного пристрою, вихід накопичувача даних 13 з'єднано з першим входом блока комутації 14, вихід якого з'єднано з п'ятим входом пристрою 12, вихід якого з'єднано з першим входом пристрою додавання за модулем 2^n 15, вихід якого є виходом даного пристрою і з'єднано з другим входом блока комутації 14, другий вхід пристрою додавання за модулем 2^n 15 з'єднано з п'ятим виходом накопичувача секретного ключа 11.

Спосіб шифрування даних на основі двох несумісних груп операцій здійснюють таким чином. В регістр 8, пристрою, що реалізує функцію $f(r_{i-1}, K_i)$ (див. фіг. 1), заносять 0, на входи пристрою порівняння 1 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 2, 3, 4 і 5 подають логічну одиницю, тоді на перший вхід пристрою віднімання 6 з блока комутації 2 подають 0, на другий та третій входи пристрою множення за модулем 7 з виходу блоків комутації 3 і 4 подають значення m'_i та A'_i відповідно, на другий вхід пристрою додавання 9 надсилають 0 з виходу четвертого блока комутації 5, якщо $r_{i-1}\geq m'_i$, то на перші входи блоків комутації 2, 3, 4 і 5 подають логічний нуль, тоді на перший вхід пристрою віднімання за модулем 2^n 6 з блока комутації 2 надсилають m'_i, на другий та третій входи пристрою множення за модулем 7 з виходу блоків комутації 3 і 4 подають значення m''_i та A''_i відповідно, на другий вхід пристрою додавання 9 надсилають m'_i з виходу четвертого блока комутації 5. Вхідний блок даних r_{i-1} надходить на пристрій віднімання за модулем 2^n 6, на якому від r_{i-1} віднімають значення, яке надходить з першого блоку комутації 2, отриманий результат з виходу пристрою віднімання 6 надходить на пристрій множення за модулем 7, результат множення надходить на пристрій додавання за модулем 2^n 9, де його додають із значенням, яке надходить з четвертого блоку комутації 5. Перетворений блок даних надходить на вихід пристрою, який реалізує функцію $f(r_{i-1}, K_i)$.

Зашифрування блоку даних виконують таким чином. На пристрій розширення ключів 10 (див. фіг. 2) надсилають початковий секретний ключ k_0 з якого для кожного циклу генерують B_i і d_i, якщо $d_i\leq 2^{n-2}$, то обчислюють $m'_i=d_i+2^{n-1}$ та використовують такі константи a=-1, b=-2, c=-4, якщо $d_i\leq 3\cdot 2^{n-2}$, 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

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

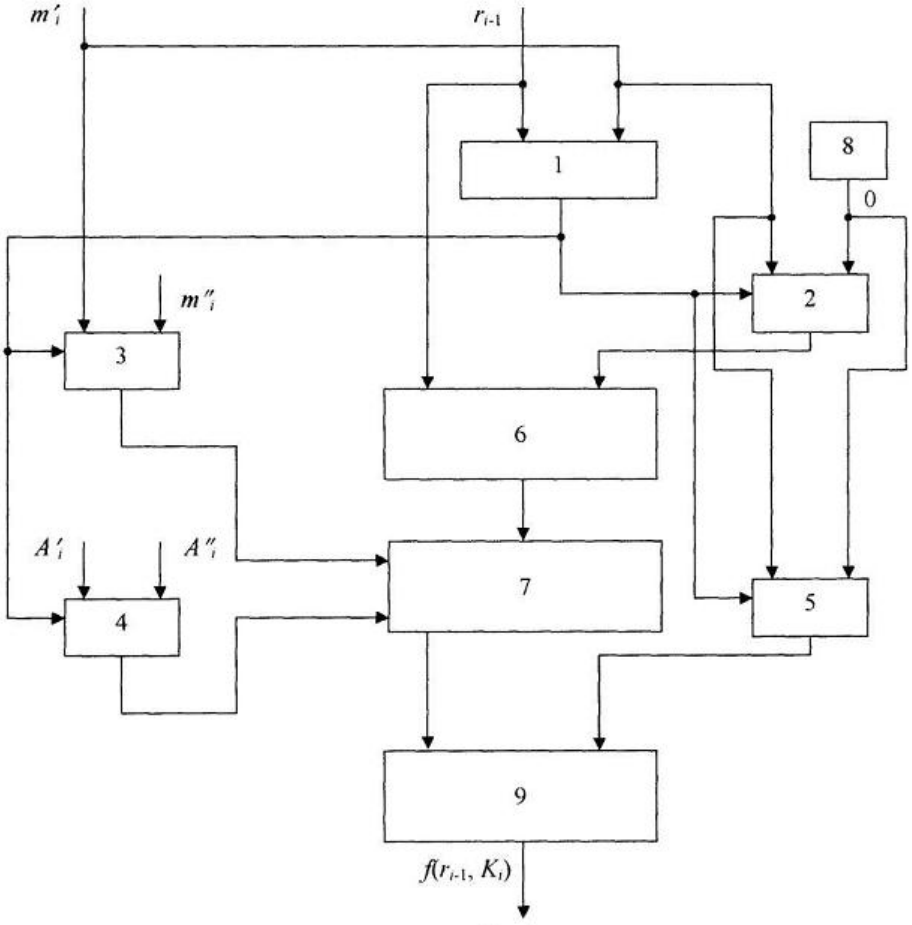
де m_{i0} - значення 0-го біта m'_i, m'_{i1} - значення 1-го біта m'_i, $\gamma(m''_i)$ розраховують так само. Отримані складові підключа K_i та B_i надходять в накопичувач секретного ключа 11 з якого підключ B_i та вхідний блок даних r_{i-1} через блок комутації 14 надходять на пристрій додавання за модулем 2^n 15, отриманий результат та складові підключа K_i надходять на пристрій 12, який реалізує функцію $f(g(r_{i-1}, B_i), K_i)$. Вище описані дії виконують L циклів, після завершення яких зашифрований блок даних подається на вихід пристрою зашифрування з виходу пристрою 12.

Розшифрування зашифрованого блоку даних виконують в оберненому порядку по відношенню до за шифрування. На пристрій розширення ключів 10 (див. фіг. 3) надсилають початковий секретний ключ k_0 з якого для кожного циклу генерують B_i та d_i з якого, за тим же принципом, що і під час зашифрування, обчислюють значення m'_i і m''_i та

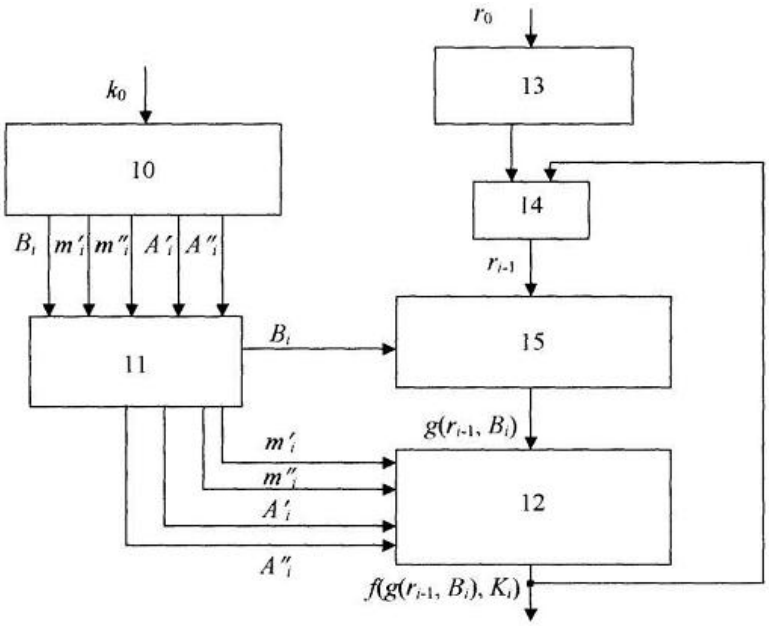
обирають константи a, b і c. Значення множників $A'_i=\gamma^{-1}(m'_i)$ та $A''_i=\gamma^{-1}(m''_i)$ розраховують на пристрої розширення ключів згідно такої функції

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

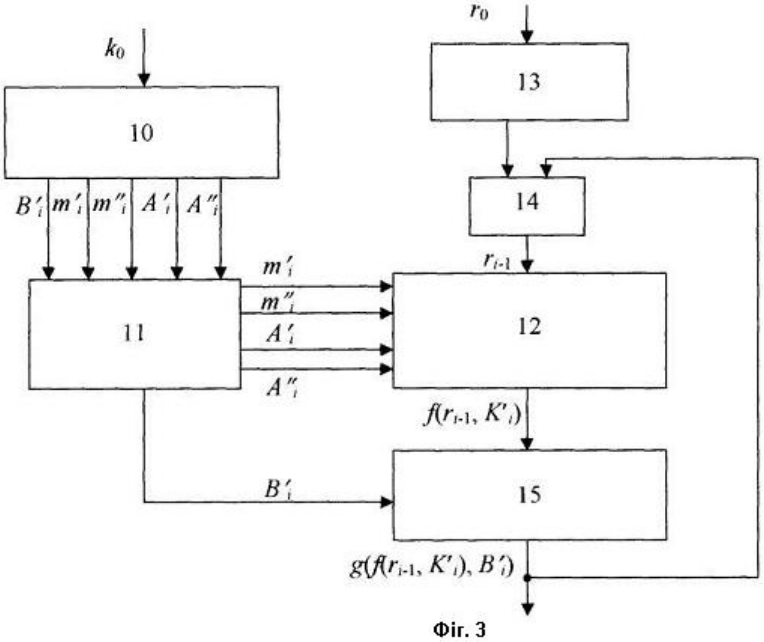
де m'_{i0}, m'_{i1}, m'_{i2} - значення 0-го, 1-го та 2-го бітів відповідно, $\gamma^{-1}(m''_i)$ розраховують так само. Отримані складові підключа K'_i та $B'_i=2^n-B_i$, в обраному порядку, надходять в накопичувач секретного ключа 11 з якого складові підключа K'_i та вхідний блок даних r_{i-1} через блок комутації 14 надходить на пристрій 12, який реалізує функцію $f(r_{i-1}, K'_i)$, отриманий результат та підключ B'_i надходять на пристрій додавання за модулем 2^n 15, з виходу пристрою додавання за модулем 2^n отримують перетворений блок даних $r_i=g(f(r_{i-1}, K'_i), B'_i)$, який через блок комутації 14 надходить на пристрій 12. Вище описані дії виконують L циклів, після завершення яких розшифрований блок даних подають на вихід пристрою розшифрування з виходу пристрою додавання за модулем 2^n 15.



Фіг. 1



Фіг. 2



Фіг. 3

Комп'ютерна верстка В. Мацело 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