УДК 621.391.7

Ю.Є. ЯРЕМЧУК, канд. техн. наук

СПЕЦІАЛІЗОВАНІ ПРОЦЕСОРИ ШИФРУВАННЯ ІНФОРМАЦІЇ БЕЗ ПОПЕРЕДНЬОГО РОЗПОДІЛУ КЛЮЧІВ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Вступ

Проблема розподілу ключів займає важливе місце в криптографічних системах. В симетричних криптосистемах [1, 2] ця проблема є більш гострою і полягає в необхідності обміну секретними ключами перед безпосереднім шифруванням інформації, причому таким чином, щоб ключ обміну став відомий лише учасникам обміну. В асиметричних системах [1-4] ця проблема по суті виключається, оскільки розповсюдженню підлягає лише відкритий ключ, який є доступним будь-кому, хто бажає послати повідомлення адресату, але і в цьому випадку сама необхідність попереднього передавання ключів залишається.

Під час реалізації криптографічних систем виникають випадки, коли необхідно здійснювати шифрування інформації без попереднього розповсюдження ключів [1, 2]. В таких випадках застосовують протоколи шифрування без попереднього розподілу ключів. Вперше такий протокол був запропонований Шаміром [5] і має назву трьохетапний протокол Шаміра. В протоколі передавач і приймач виконують обчислення над даними по два рази на кожному боці, здійснюючи при цьому три передавання даних: два від передавача до приймача і одне від приймача до передавача. З точки зору обчислювальної складності метод є недостатньо ефективним, оскільки крім необхідності виконання трьохетапної процедури передавання, ще й необхідно під час обчислень здійснювати піднесення до степеня над числами великої розрядності.

Виходячи з цього, актуальним є побудова методів шифрування без попереднього розподілу ключів на основі таких математичних апаратів, які б могли забезпечувати спрощення обчислень. В цьому зв'язку певний інтерес викликає апарат на основі рекурентних послідовностей [6], який дозволяє за певних умов спрощувати обчислення в криптографічних застосуваннях, що базуються на його основі.

Особливість методів, що використовують технологію відкритого ключа, полягає в тому, що в них необхідно виконувати обчислення над числами великої розрядності (1024–4096 двійкових розрядів), тому програмна реалізація алгоритмів шифрування вимагає великого часу і для деяких застосувань є непридатною. Потрібна в цих випадках швидкість шифрування може бути досягнута за рахунок апаратної реалізації методу шифрування. Тому розглядається можливість побудови спеціалізованих процесорів шифрування та дешифрування інформації без попереднього розподілу ключів на основі рекурентних послідовностей.

Постановка задач досліджень

Розглянути математичний апарат рекурентних послідовностей з точки зору побудови швидкісних методів шифрування інформації без попереднього розподілу ключів та розробити принципи побудови спеціалізованих процесорів на їх основі. Дослідити запропоновані процесори щодо швидкості їх роботи і порівняти з відповідними процесорами, що реалізують відомі методи-аналоги.

Шифрування інформації без попереднього розподілу ключів на основі рекурентних послідовностей

Рекурентні послідовності в загальному вигляді породжуються співвідношенням [6]

$$u_n = a_1 \cdot u_{n-1} + a_2 \cdot u_{n-2} + \ldots + a_k \cdot u_{n-k},$$

де a_1, a_2, . . . , a_k – коефіцієнти, k – порядок послідовності, виходячи з початкових елементів u_0, u_1, . . . , u_k.

Назвемо послідовність чисел, що обчислюються за формулою

$$v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k} \tag{1}$$

для початкових значень $v_{0,k} = 1$, $v_{1,k} = g_2$ для $k = 2$; $v_{0,k} = v_{1,k} = ... = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$; де g_1, g_k – цілі числа; n і k – цілі додатні – V_k^+–послідовністю.

Формула (1) дозволяє отримувати значення для зростаючих n, починаючи з $n = 0$. Можлива і зворотна процедура, коли елементи послідовності обчислюються для спадних n, починаючи з деякого значення $n = l$. Обчислення елементів такої послідовності буде здійснюватись таким чином

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}. \tag{2}$$

Обчислення за формулою (2) може продовжуватись і для $n < 0$, тобто існує два виду послідовностей. Перший вид послідовностей формується для n – додатних за формулою (1). Другий вид послідовностей формується для n – від'ємних за формулою (2).

Назвемо V_k^-–послідовністю послідовність чисел, що обчислюються за формулою (2) для n – від'ємних при початкових значеннях $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$ для $k = 2$; $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = ... = v_{-k,k} = 0$ для $k > 2$.

Тоді послідовність чисел, яка складається з V_k^+–послідовності та V_k^-–послідовності назвемо V_k – послідовністю.

V_k – послідовність є окремим випадком більш узагальненої послідовності, оскільки значення більшості початкових елементів нульові. Якщо дозволити, щоб ці початкові елементи приймали будь-які значення, то отримаємо такий варіант узагальненої послідовності.

Назвемо послідовність чисел, що обчислюються за формулою

$$u_{n,k} = g_k u_{n-1,k} + g_1 u_{n-k,k} \tag{3}$$

для початкових значень $u_{0,k} = g_1$, $u_{1,k} = g_2$, $u_{2,k} = g_3$, ... $u_{k-1,k} = g_k$; де g_1, g_2, g_3, ... , g_k - цілі числа; n і k – цілі додатні числа – U_k –послідовністю.

Для будь-яких цілих додатних n, m та k отримано таку аналітичну залежність

$$u_{n+m,k} = v_{m+(k-2),k} \cdot u_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot u_{n-k+i,k}. \tag{4}$$

Для будь-яких цілих додатних n та k, таких що $n \geq k$, отримано залежність, яка дозволяє обчислювати елементи U_k –послідовності тільки на основі елементів V_k^+ – послідовності

$$u_{n,k} = g_k \cdot v_{n-1,k} + g_1 \cdot \sum_{i=1}^{k-1} g_i \cdot v_{n-i-1,k}. \tag{5}$$

Виходячи з формули (3) вираз для обчислення елементів $u_{n,k}$ для спадних n, починаючи з деякого $n = l$, має такий вигляд

$$u_{n,k} = \frac{u_{n+k,k} - g_k u_{n+k-1,k}}{g_1}. \qquad (6)$$

Для будь-яких цілих додатних n і m, таких що $1 \le m < n$ та будь-якого цілого додатного k отримано таку залежність

$$u_{n-m,k} = v_{-m+(k-2),k} \cdot u_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} \cdot u_{n-k+i,k} \cdot \qquad (7)$$

Ідея методу шифрування інформації без попереднього розподілу ключів базується на послідовному використанні спочатку аналітичної залежності (4) обчислення елементу $u_{n+m,k}$, а потім залежності (7) обчислення елементу $u_{n-m,k}$. Таким чином, якщо порівнювати з відомим методом Шаміра, здійснюється заміна модулярного піднесення до степеня обчисленням за модулем елементу U_k –послідовності з певним індексом.

Загальна процедура шифрування даних без попереднього розподілу ключів згідно методу, що пропонується, представлена на рис.1.

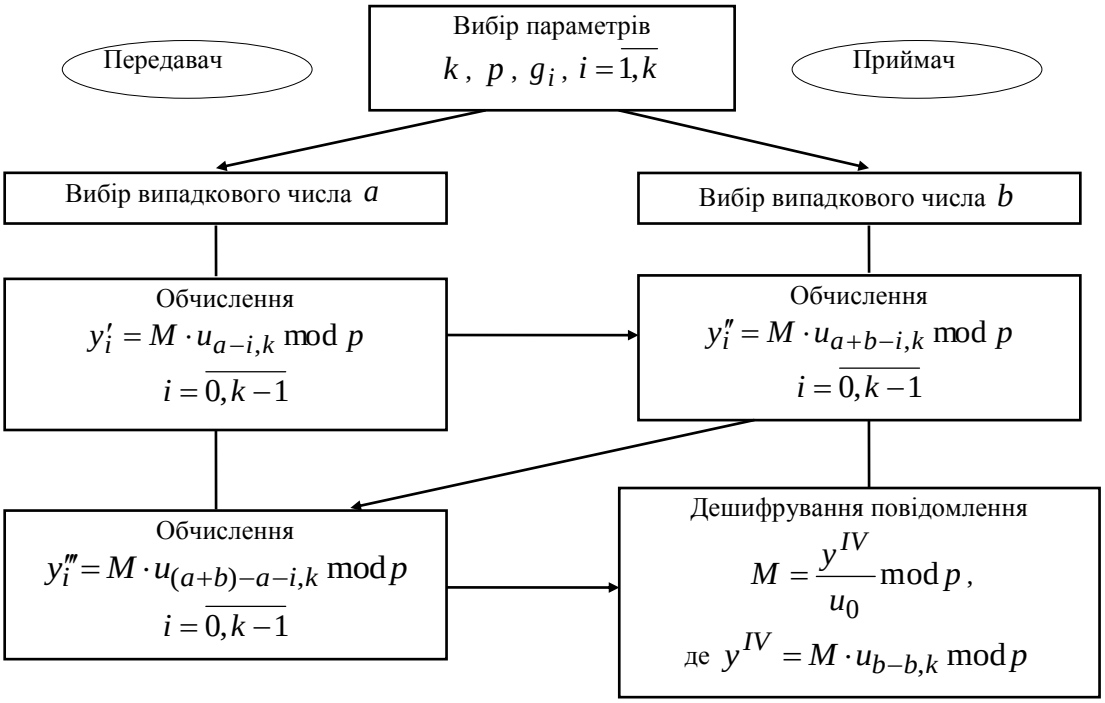

Рис. 1. Процедура шифрування даних без попереднього розподілу ключів на основі елементів U_k -послідовності

Згідно із запропонованим методом шифрування основні обчислення виконуються згідно залежностей (4) і (7). Для обчислення елементів $u_{n+m-i,k}$, $i = \overline{0,k-1}$ згідно залежності (4) потрібні елементи $v_{m+i,k}$, $i = \overline{-k,k-2}$ та елементи $u_{n-i,k}$, $i = \overline{0,k-1}$, а для обчислення елементів $u_{n-m-i,k}$, $i = \overline{0,k-1}$ згідно залежності (7) потрібні елементи $v_{-m+i,k}$, $i = \overline{-k,k-2}$ та елементи $u_{n-i,k}$, $i = \overline{0,k-1}$. Обчислення елементів $u_{n-i,k}$, $i = \overline{0,k-1}$ здійснюється Передавачем за формулою (5). При цьому потрібно мати елементи $v_{n+i,k}$, $i = \overline{-2k+1,-1}$.

Звідси виходить, що всього для обчислення елементу $u_{n+m,k}$ згідно залежності (4) та елементу $u_{n-i,k}$, $i = \overline{0,k-1}$ за формулою (5) потрібно мати елементи $v_{n+i,k}$, $i = \overline{-2k+1,k-2}$, V_k -послідовності. Частину елементів цього набору для $i = \overline{-(k-1),k-2}$ отримаємо за алго-

ритмом прискореного обчислення елементів V_k^+ –послідовності, який може бути реалізований на основі відомого бінарного методу піднесення до степеня [7, 1]. Іншу частину, для $i = \overline{-2k+1,-k}$, отримаємо за формулою (2), використовуючи дані отримані в цьому алгоритмі. В результаті невизначеним залишається лише обчислення елементів $v_{-m+i,k}$, $i = \overline{-k,k-2}$, що використовуються в залежності (7), і які можуть бути обчислені за алгоритмом прискореного обчислення елементів $v_{n,k}$ для від'ємних значень n на основі того самого бінарного методу піднесення до степеня.

Проведено дослідження теоретичної криптостійкості та складності обчислень за даним методом, а також порівняння з відомим методом Шаміра. Показано, що розглянутий метод має не менший рівень криптостійкості, ніж відомий метод, але при цьому значно меншу складність обчислень у порівнянні з відомим.

Розробка принципів побудови спеціалізованих процесорів шифрування інформації без попереднього розподілу ключів

В розглянутому методі основними є обчислення за модулем V_k та U_k – послідовностей, а саме елементів $v_{n+i,k}$, $i = \overline{-2k+1,k-2}$, для додатних значень n, $v_{n+i,k}$, $i = \overline{-k,k-2}$, для від'ємних n, а також елементів $u_{n-i,k}$, $u_{n+m-i,k}$, $u_{n-m-i,k}$ для $i = \overline{0,k-1}$. Всі ці обчислення пропонується здійснювати на одному пристрої обчислення елементів V_k та U_k – послідовностей, роботу якого організуємо в п'яти режимах. В першому режимі будемо здійснювати обчислення елементів $v_{n+i,k}$, $i = \overline{-2k+1,k-2}$, для додатних значень n. Другий режим роботи пристрою буде забезпечувати обчислення елементів $v_{n+i,k}$, $i = \overline{-k,k-2}$, для від'ємних значень n. Третій, четвертий та п'ятий режими роботи пристрою будуть забезпечувати відповідно обчислення елементів $u_{n-i,k}$, $u_{n+m-i,k}$, $u_{n-m-i,k}$ для $i = \overline{0,k-1}$ згідно формули (5) та залежностей (4) і (7).

Визначено, що час обчислення елементів V_k – послідовності в першому і другому режимах дорівнює

$$T_{\mathrm{V}} = Hq \cdot (k^2 + k) \cdot T_{\text{мн.Монт.}},$$

де H – кількість машинних одиниць інформації для зберігання великого числа,
q – кількість розрядів машинної одиниці інформації,
$T_{\text{мн.Монт.}}$ – час множення за модулем за методом Монтгомері, а час обчислення елементів U_k – послідовності в третьому, четвертому і п'ятому режимах; $T_{\mathrm{U}} = (k^2 + k) \cdot T_{\text{мн.Монт.}}$

Для реалізації шифрування інформації без попереднього розподілу ключів згідно представленого методу пропонується процесор, схему якого наведено на рис. 2.

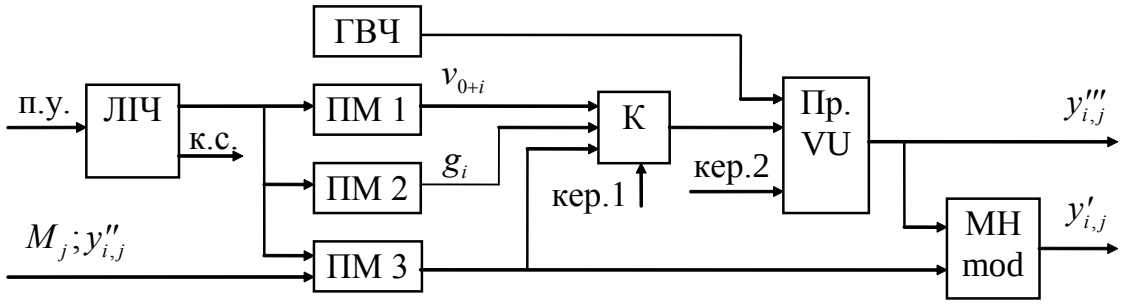

Рис. 2. Структурна схема процесора шифрування без попереднього розподілу ключів (варіант 1)

Процесор містить генератор випадкових чисел ГВЧ; пристрій обчислення елементів V_k та U_k – послідовностей Пр.VU; блок множення за модулем МН mod; блоки пам'яті ПМ 1 та ПМ 2, призначені для зберігання відповідно елементів $v_{0+i,k}$, $i=\overline{-(k-1),0}$, та коефіцієнтів рекурентного співвідношення g_i, $i=\overline{1,k}$; блок пам'яті ПМ 3, призначений для зберігання кодового блоку відкритого повідомлення M_j, а також елементів $y''_{i,j}$, $i=\overline{0,k-1}$, що отримуються від Приймача під час шифрування інформації; комутатор К; лічильник ЛІЧ.

Шифрування інформації здійснюється таким чином.

Генератор ГВЧ формує випадкове число a, яке разом з даними, що знаходяться в блоці пам'яті ПМ 1 подаються на відповідні входи пристрою ПР.VU. Цей пристрій, здійснюючи свою роботу в першому та другому режимах, обчислює відповідно елементи $v_{a+i,k}$, $i=\overline{-2k+1,k-2}$, для додатних значень n та елементи $v_{a+i,k}$, $i=\overline{-k,k-2}$, для від'ємних n та зберігає обчислені елементи у своєму блоці пам'яті протягом всього процесу шифрування – дешифрування одного блоку інформації.

Далі на пристрій Пр.VU надходять дані з блоку пам'яті ПМ 2 і він, здійснюючи свою роботу в третьому режимі, обчислює елементи $u_{a-i,k}$, $i=\overline{0,k-1}$. Отримані дані разом з кодовим блоком відкритого повідомлення M_j, що знаходиться в ПМ 3, послідовно поступають на блок множення МН mod, а з нього результат множення за модулем – $y'_{i,j}$, $i=\overline{0,k-1}$, передається Приймачу.

Після цього в блок пам'яті ПМ 3 записуються дані $y''_{i,j}$, $i=\overline{0,k-1}$, а звідти вони подаються на пристрій Пр.VU, який, здійснюючи свою роботу в п'ятому режимі, обчислює $y'''_{i,j}$, $i=\overline{0,k-1}$. Після передачі отриманих даних Приймачу завершується шифрування одного блоку інформації.

Зазначимо, що процесор шифрування може бути побудований таким чином, що замість блоку множення за модулем МН mod буде використовуватись аналогічний пристрій, що застосовується в пристрої Пр.VU.

Враховуючи це, для реалізації процесору шифрування інформації згідно представленого методу необхідно 4 суматора, один пристрій множення та пам'ять ємністю $(H+2)\cdot\left[2\cdot(Hq+1)\cdot(2k-1)+10\cdot(k+1)\right]+4$ машинних одиниць інформації. Час шифрування на цьому процесорі буде дорівнювати

$$T_{\text{ш}}=(Q+2Hq)\cdot(k^2+k)\cdot T_{\text{мн.Монт.}},$$

де Q – кількість кодових блоків відкритого повідомлення M.

Для реалізації дешифрування згідно представленого методу пропонується процесор, структурна схема якого представлена на рис. 3.

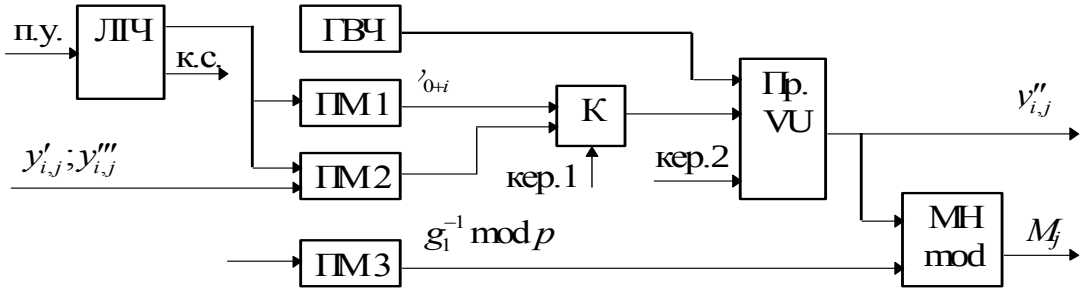

Рис. 3. Структурна схема процесора дешифрування без попереднього розподілу ключів (варіант 1)

Процесор містить генератор випадкових чисел ГВЧ; пристрій обчислення елементів V_k та U_k - послідовностей Пр.VU; блок множення за модулем МН mod; блок пам'яті ПМ 1, призначений для зберігання елементів $v_{0+i,k}$, $i=\overline{-(k-1),0}$; блок пам'яті ПМ 2, призначений для зберігання даних $y'_{i,j}$ та $y'''_{i,j}$, $i=\overline{0,k-1}$, що поступають на відповідних етапах дешифрування інформації від Передавача; блок пам'яті ПМ 3, що використовується для зберігання значення $g_1^{-1} \bmod p$; комутатор К; лічильник ЛІЧ.

Дешифрування інформації здійснюється таким чином.

Генератор ГВЧ формує випадкове число b, яке разом з даними, що знаходяться в блоці пам'яті ПМ 1 поступають на пристрій ПР.VU, який, під час своєї роботи в першому режимі, обчислює елементи $v_{b+i,k}$, $i=\overline{-2k+1,k-2}$, та зберігає їх в своєму блоці пам'яті протягом всього етапу дешифрування одного блоку інформації.

Далі дані $y'_{i,j}$, $i=\overline{0,k-1}$, що приймаються від Передавача, записуються в блок пам'яті ПМ 2, а звідти поступають на пристрій Пр.VU, який, здійснюючи свою роботу в четвертому режимі, обчислює елементи $y''_{i,j}$, $i=\overline{0,k-1}$, і отримані дані передаються до Передавача.

Потім дані $y'''_{i,j}$, $i=\overline{0,k-1}$, що надходять від Передавача, записуються в блок пам'яті ПМ 2, а звідти подаються на пристрій Пр.VU. Останній, здійснюючи свою роботу в п'ятому режимі, обчислює значення y^{IV}, яке разом зі значенням $g_1^{-1} \bmod p$, що знаходиться в блоці пам'яті ПМ 3, поступає на пристрій множення МН mod. Після виконання пристроєм МН mod операції множення за модулем, отримується кодовий блок відкритого повідомлення M_j.

Слід зазначити, що пристрій дешифрування інформації може бути побудований таким чином, щоб остання операція множення за модулем виконувалась відповідним пристроєм, що використовується в пристрої Пр.VU.

З урахуванням цього, для реалізації процесора дешифрування інформації згідно представленого методу необхідно чотири суматора, один пристрій множення та пам'ять ємністю $(H+2)\cdot\left[2\cdot(Hq+1)\cdot(2k-1)+9k+11)\right]+4$ машинних одиниць інформації. Час дешифрування на цьому процесорі буде дорівнювати

$$T_{\text{дш}} = [Q(k+1)+Hqk]\cdot(k+1)\cdot T_{\text{мн.Монт.}}.$$

Аналіз представленого методу шифрування без попереднього розподілу ключів показує, що обчислення $y'_{i,j}$ та $y'''_{i,j-1}$ для $i=\overline{0,k-1}$ при шифруванні інформації, а також $y''_{i,j}$ та M_{j-1} для $i=\overline{0,k-1}$ при дешифруванні можна виконувати водночас.

Це дозволяє при шифруванні (дешифруванні) використовувати два пристрої Пр.VU для побудови процесорів конвеєрного типу.

Структурна схема процесора для шифрування наведена на рис. 4.

Процесор для шифрування, на відміну від того, що наведений на рис. 2, містить два пристрої для обчислення елементів V_k та U_k – послідовностей Пр.VU 1 та Пр.VU 2.

Робота процесорів також аналогічна. Відмінність полягає в тому, що шифрування інформації відбувається водночас для двох кодових блоків відкритого повідомлення M_j та M_{j-1}. При цьому обчислення $y'_{i,j}$, $i=\overline{0,k-1}$, здійснюється за допомогою пристроїв Пр.VU1 та МН mod, а обчислення $y'''_{i,j-1}$, $i=\overline{0,k-1}$, – за допомогою пристрою Пр.VU 2.

Також зазначимо, що після обчислення пристроєм Пр.VU 1 елементів V_k – послідовності, вони з блоку пам'яті ПМ 4 цього пристрою переписуються в такий же блок пам'яті пристрою Пр.VU 2.

Для реалізації процесору, схема якого наведена на рис. 4, необхідно 8 суматорів, два пристрої множення та пам'ять ємністю $(H+2)\cdot\left[4\cdot(Hq+1)\cdot(2k-1)+17k+20)\right]+8$ машинних одиниць інформації.

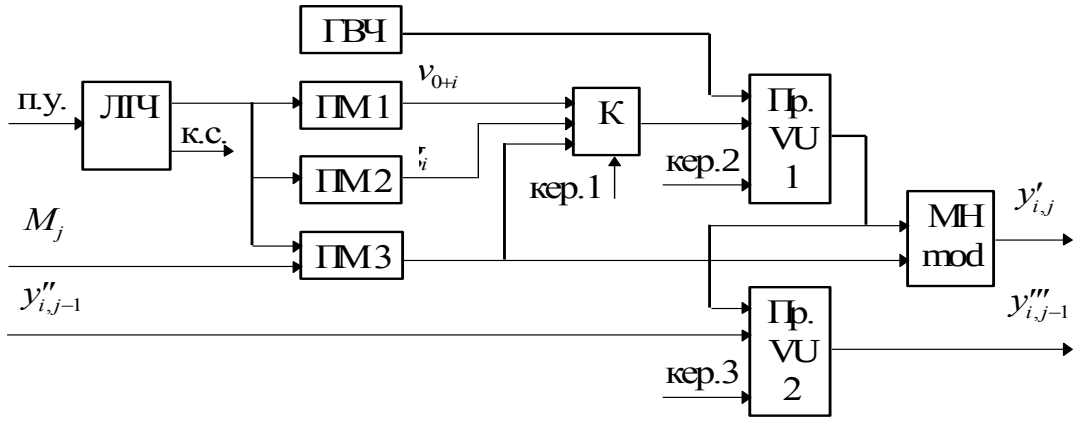

Рис. 4. Структурна схема процесора шифрування без попереднього розподілу ключів (варіант 2)

Час шифрування кожної частини відкритого повідомлення M_j буде вдвічі швидше, ніж на процесорі, що представлений на рис. 2, тобто

$$T'_{\text{ш}} = [(Q/2)+2Hq)]\cdot(k^2+k)\cdot T_{\text{мн.Монт.}}.$$

Для дешифрування інформації пропонується процесор, структурна схема якого наведена на рис. 5.

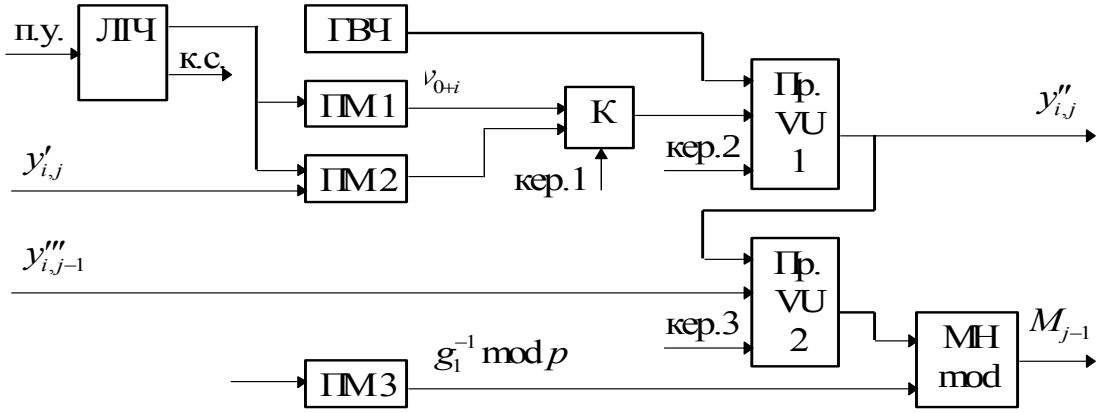

Рис. 5. Структурна схема процесора дешифрування без попереднього розподілу ключів (варіант 2)

Цей процесор аналогічний процесору, схема якого наведена на рис. 3. Відмінність полягає у використанні двох пристроїв обчислення елементів V_k та U_k - послідовностей, замість одного, а також в тому, що одночасно відбуваються обчислення $y''_{i,j}$, $i=\overline{0,k-1}$, за допомогою пристрою Пр.VU1 та дешифрування M_{j-1} за допомогою пристроїв Пр.VU2 та МНmod.

Слід також зазначити, що після отримання пристроєм Пр.VU 1 елементів $v_{n+i,k}$, $i=\overline{-k,k-2}$, вони записуються в блок пам'яті ПМ 4 пристрою Пр.VU 2 з такого ж блоку пам'яті пристрою Пр.VU 1.

Для реалізації процесора, структурна схема якого наведена на рис. 5, потрібно 8 суматорів, два пристрої множення та пам'ять ємністю $(H+2)\cdot\left[4\cdot(Hq+1)\cdot(2k-1)+16k+21)\right]+8$ машинних одиниць інформації. Час дешифрування кожного кодового блоку на цьому процесорі буде вдвічі швидше, ніж на процесорі, що представлений на рис. 3, тобто

$$T'_{\text{дш}} = [(Q/2)(k+1) + Hqk] \cdot (k+1) \cdot T_{\text{мн.Монт.}}.$$

Аналіз роботи розглянутих процесорів показує, що за допомогою пристрою Пр.VU 2 (рис. 5) обчислюється один елемент U_k – послідовності, в той час, як за допомогою інших пристроїв Пр.VU 1, Пр.VU 2 (рис. 4) та Пр.VU 1 (рис. 5) обчислюється k елементів U_k – послідовності.

Тобто при дешифруванні пристрій Пр.VU 2 завантажений менше, але, незважаючи на це, шифрування – дешифрування буде виконуватись вдвічі швидше, ніж в процесорах, схеми яких наведені на рис. 2, 3.

Проведемо порівняння розроблених процесорів для шифрування–дешифрування інформації зі спеціалізованими процесорами, що реалізують відомі методи.

Основна операція, що виконується у відомому методі Шаміра, – піднесення до степеня за модулем – може здійснюватись за методом Монтгомері [1], який має меншу складність обчислень, ніж відомий бінарний метод [1, 7]. Метод піднесення до степеня за Монтгомері оснований на множенні за методом Монтгомері,що дозволяє використати пристрій множення за Монтгомері для реалізації пристрою піднесення до степеня за Монтгомері.

Виходячи з цього, маємо пристрій піднесення до степеня за Монтгомері, який потребує для своєї реалізації, на рівні машинних одиниць інформації, $10(H+2)+3$ регістрів пам'яті, три суматори та один пристрій множення. Час виконання піднесення до степеня за модулем на цьому пристрої дорівнює

$$T_{\text{ПДСmod}} = 2(Hq+1) \cdot T_{\text{мн.Монт.}}.$$

Використовуючи пристрій піднесення до степеня за модулем, маємо процесор для шифрування (дешифрування) за відомим методом Шаміра. Кожен з цих процесорів потребує для своєї реалізації три суматори, один пристрій множення та пам'ять ємністю $13(H+2)+3$ машинних одиниць інформації.

Шифрування інформації на процесорі для шифрування (дешифрування) інформації за відомим методом Шаміра має однаковий час з дешифруванням:

$$T_{\text{Щ, ш}} = T_{\text{Щ, дш}} = 4Q(Hq+1) \cdot T_{\text{мн.Монт.}}.$$

Аналіз апаратурних витрат процесорів для шифрування–дешифрування за відомим та процесорів для шифрування–дешифрування згідно запропонованого методу Шаміра показує, що перші потребують менших апаратурних витрат, ніж останні.

Для порівняння часу роботи процесорів за відомими та запропонованими методами введемо відносну оцінку. В результаті маємо

$$\delta = \frac{8Q(Hq+1)}{Q(2k^2+3k+1)+3Hq(k^2+k)}.$$

Значення δ для різних значень Hq, Q та k наведені в таблиці:

k	Q	Hq	δ	k	Q	Hq	δ
2	100	1024	41.1399	3	100	1024	20.6737
		2048	42.7276			2048	21.4196
		4096	43.5689			4096	21.8134
	1000	1024	245.2740		1000	1024	126.4184
		2048	316.0574			2048	161.1356
		4096	369.3986			4096	186.8047

Аналіз відносних оцінок, наведених в таблиці, показує, що час шифрування – дешифрування на процесорах, що реалізують запропонований метод менше для будь-якого k, ніж на процесорах, що реалізують відомий метод Шаміра, причому більш ніж у 10 разів для $Q = 100$ і більш ніж у 10^2 разів для $Q = 1000$.

Висновки

Розглянуто математичний апарат рекурентних V_k – та U_k – послідовностей та їх аналітичних залежностей. На основі цього апарату представлено метод шифрування інформації без попереднього розподілу ключів, суть якого полягає в заміні піднесення до степеня обчисленням певного елементу U_k –послідовності.

Представлений метод шифрування дозволяє виконувати певні обчислення як послідовно, так і паралельно. Тому його апаратна реалізація може здійснюватись або у вигляді процесора з одним пристроєм для обчислення елементів V_k та U_k – послідовностей, або процесора конвеєрного типу з двома пристроями для обчислення елементів V_k та U_k – послідовностей. Перший варіант вимагає менше апаратурних витрат, ніж другий варіант, але наявність двох рівнів конвеєру забезпечує останньому продуктивність вдвічі більшу, ніж для першого варіанту.

Процесори, що реалізують запропонований метод, потребують більше апаратурних витрат, ніж процесори, що реалізують відомий метод Шаміра, але забезпечують більш ніж у k разів для будь-якого порядку послідовності k менший час шифрування – дешифрування.

Список літератури: 1. *Menezes A.J., van Oorschot P.C., Vanstone S.A.* Handbook of Applied Cryptography. – CRC Press, 2001. – 816 p. 2. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М. : Триумф, 2002. – 816 с. 3. *Молдовян Н.А., Молдовян А.А.* Введение в криптосистемы с открытым ключом. – Спб. : БХВ-Петербург, 2005. – 288 с. 4. *Саломаа А.* Криптография с открытым ключом. – М. : Мир, 1995. – 318 с. 5. *Месси Д.Л.* Введение в современную криптологию // ТИИЭР. – Т.76. – 1988. – №5. – С. 24 – 42. 6. *Маркушевич А.И.* Возвратные последовательности. – М. : Наука, 1975. – 48 с. 7. *Кнут Д.* Искусство программирования для ЭВМ. – Т.2. Получисленные алгоритмы. – М. : Вильямс, 2004. – 832 с.

Вінницький національний технічний університет

Поступила в редколлегию 15.10.2013