УДК 621.391.7

**Ю. Є. Яремчук**
Вінницький національний технічний університет
вул. Хмельницьке шосе, 95, 21021 Вінниця, Україна

# Спеціалізовані процесори реалізації автентифікації суб'єктів (об'єктів) взаємодії на основі рекурентних послідовностей

*Представлено принципи побудови спеціалізованих процесорів реалізації автентифікації суб'єктів (об'єктів) взаємодії на основі рекурентних* $V_k$ *-послідовностей. Порівняно з відомими аналогами розроблені процесори хоч і є менш швидкими, але забезпечують більший рівень криптографічної стійкості під час автентифікації, а також надають більші можливості їхнього застосування у системах, що використовують математичний апарат рекурентних послідовностей.*

***Ключові слова:*** *спеціалізовані процесори, захист інформації, криптографія, автентифікація сторін взаємодії, рекурентні послідовності.*

## Вступ

Задача забезпечення цілісності на сьогодні є не менш актуальною, ніж забезпечення конфіденційності. Її вирішення здійснюється за допомогою криптографічних методів автентифікації та цифрового підписування [1, 2]. Відомі методи Шнорра, Фейге-Фіата-Шаміра та Гіллоу-Куіскуотера [1], що забезпечують вирішення проблеми автентифікації суб'єктів (об'єктів) взаємодії, базуються на операції піднесення до степеня над числами великої розрядності, яка вимагає виконання досить складних обчислень, що, в свою чергу, впливає на швидкість роботи методу при його практичній реалізації.

У роботі [3] представлено метод автентифікації суб'єктів (об'єктів) взаємодії на основі математичного апарату рекурентних $V_k$ -послідовностей, в якому відбувається заміна піднесення до степеня обчисленням елемента рекурентної послідовності з певним індексом. Порівняно з відомими методами цей метод є більш стійким і має значно простішу процедуру завдання параметрів.

Оскільки в асиметричних криптографічних методах обчислення виконуються над числами великої розрядності (1024–4096 розрядів), що вимагає великого часу, то програмна реалізація не завжди є прийнятною. Підвищення швидкості криптографічних перетворень може бути досягнуто за рахунок апаратної реалізації методів.

***Метою роботи*** є розробка спеціалізованих процесорів реалізації запропонованого в роботі [3] методу автентифікації суб'єктів (об'єктів) взаємодії, що забезпечує підвищення рівня криптографічної стійкості.

## Постановка задач досліджень

У рамках представленої статті постає задача розробки принципів побудови спеціалізованих процесорів реалізації методу автентифікації суб'єктів (об'єктів) взаємодії на основі рекурентних $V_k$-послідовностей, що представлений у роботі [3], а також дослідження запропонованих процесорів щодо швидкості їхньої роботи і порівняння з відповідними процесорами, що реалізують відомі методи-аналоги.

## Розробка принципів побудови спеціалізованих процесорів реалізації автентифікації суб'єктів (об'єктів) взаємодії на основі $V_k$-послідовностей

Для реалізації представленого в [3] методу автентифікації суб'єктів (об'єктів) взаємодії перш за все необхідно реалізувати обчислення за модулем $p$ елементів $v_{n+i,k}$, $i=\overline{-(k-1),k-1}$, та $v_{-n+i,k}$, $i=\overline{-k,k-2}$, елементів $v_{n\cdot m+i,k}$, $i=\overline{-1,k-2}$, та $v_{-n\cdot m+i,k}$, $i=\overline{-(k-1),0}$, а також елементів $v_{n+m+i,k}$, $i=\overline{-1,k-2}$, та елемента $v_{-n+m,k}$. Ці обчислення пропонується здійснювати на одному пристрої обчислення елементів $V_k$-послідовності. Як варіант, ці обчислення можуть бути реалізовані на пристрої, що представлено в роботі [4].

Для реалізації обчислень претендентом згідно представленого в [3] методу автентифікації пропонується процесор, схему якого наведено на рис. 1.

Процесор містить: генератор випадкових чисел ГВЧ; пристрій обчислення елементів $V_k$-послідовностей Пр.V; блоки пам'яті ПМ 1 та ПМ 2, призначені відповідно для зберігання значень $a$ і $b$; блоки пам'яті ПМ 3 та ПМ 5, призначені для зберігання відповідно елементів $v_{0+i,k}$, $i=\overline{-(k-1),0}$, та $v_{b+i,k}$, $i=\overline{-(k-1),0}$; блок пам'яті ПМ 4, призначений для зберігання елементів $v_{c+i,k}$, $i=\overline{-(k-1),0}$, що отримуються від перевіряльника; комутатори К 1 і К 2; лічильник ЛІЧ.

Доведення претендентом своєї автентичності здійснюється таким чином.

Генератор ГВЧ за сигналом керування «кер.1» генерує випадкове число $a$, яке за сигналом запису «кер.2» записується в блок пам'яті ПМ 1, а звідти разом з даними, що знаходяться в блоці пам'яті ПМ 3, подаються на відповідні входи пристрою Пр.V. Далі пристрій Пр.V обчислює за модулем $p$ елементи $v_{-a+i,k}$, $i=\overline{-k,-1}$, які як відкритий ключ передаються перевіряльнику.

Лічильник ЛІЧ забезпечує послідовний перебір усіх елементів $v_{0+i,k}$, $i=\overline{-(k-1),0}$, що знаходяться у блоці пам'яті ПМ 3, та подання їх на пристрій Пр.V. Початкова установка лічильника ЛІЧ здійснюється за допомогою сигналу

«п.у.», що надходить від пристрою керування, після чого лічильник видає адресу першого елемента блоку пам'яті ПМ 3. По завершенні роботи лічильника ЛІЧ на пристрій керування подається сигнал кінця роботи «кер.4».

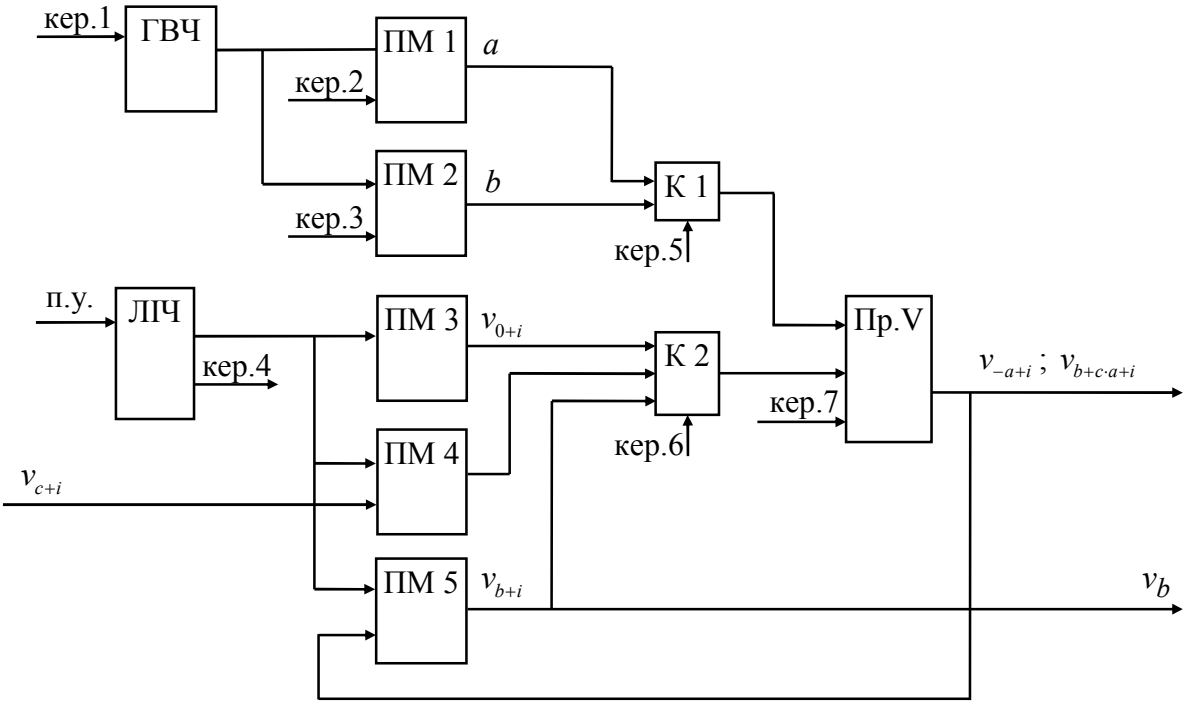


Рис. 1. Структурна схема процесора виконання обчислень претендентом для доведення своєї автентичності

Коли претендент безпосередньо хоче довести свою автентичність, генератор ГВЧ за сигналом керування «кер.1» генерує випадкове число $b$, яке за сигналом запису «кер.3» записується у блок пам'яті ПМ 2, а звідти разом з даними, що знаходяться у блоці пам'яті ПМ 3, подаються на відповідні входи пристрою Пр.V, після чого пристрій Пр.V обчислює за модулем $p$ елементи $v_{b+i,k}$, $i=\overline{-(k-1),0}$, які після обчислень записуються у блок пам'яті ПМ 5.

Після отримання від перевіряльника значень елементів $v_{c+i,k}$, $i=\overline{-(k-1),0}$, вони записуються в блок пам'яті ПМ 4, після чого разом зі значенням $a$, яке знаходиться в блоці пам'яті ПМ 1, подаються на відповідні входи пристрою Пр.V. Результатом обчислень пристрою Пр.V над цими значеннями будуть елементи $v_{c\cdot a+i,k}$, $i=\overline{-1,k-2}$, які зберігатимуться у відповідному блоці пам'яті пристрою Пр.V з тим, щоб продовжити обчислення за модулем $p$ елементів $v_{b+c\cdot a+i,k}$, $i=\overline{-1,k-2}$, використовуючи при цьому елементи $v_{b+i,k}$, $i=\overline{-(k-1),0}$, що подаються на пристрій Пр.V з блоку пам'яті ПМ 5. Отримані за модулем $p$ значення елементів $v_{b+c\cdot a+i,k}$, $i=\overline{-1,k-2}$, з пристрою Пр.V разом із значенням $v_{b,k}$ з блоку пам'яті ПМ 5 передаються перевіряльнику.

Для реалізації обчислень перевіряльником згідно представленого в [3] методу пропонується процесор, схему якого наведено на рис. 2.

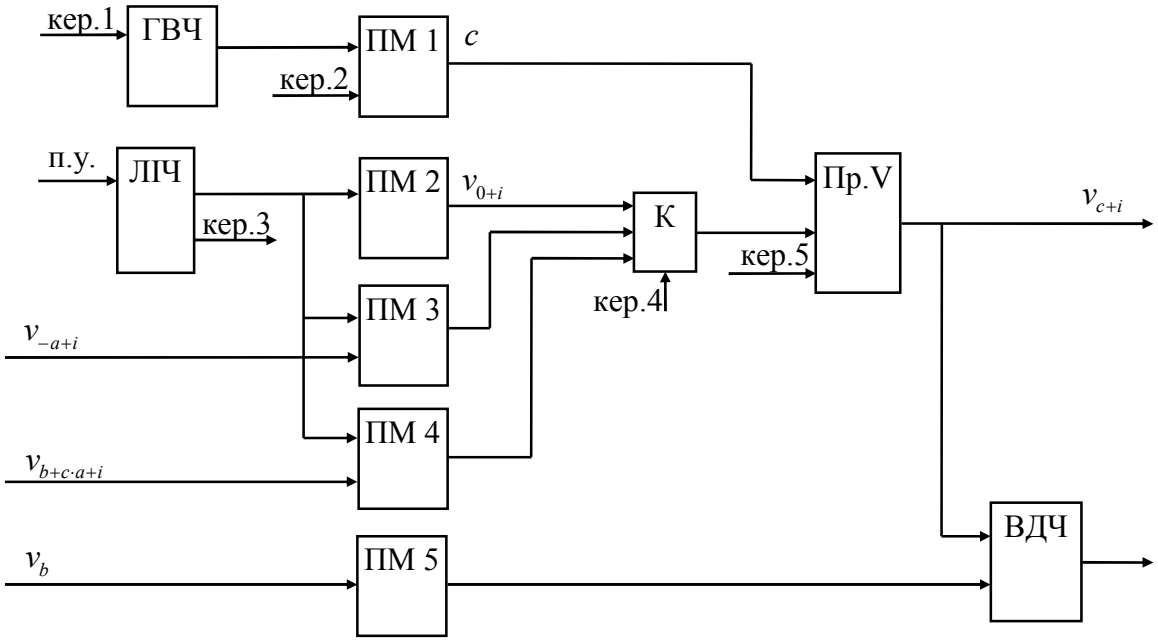


Рис. 2. Структурна схема процесора виконання обчислень перевіряльником для перевірки автентичності претендента

Процесор містить генератор випадкових чисел ГВЧ; пристрій обчислення елементів $V_k$-послідовностей Пр.V; блок пам'яті ПМ 1, призначений для зберігання значення $c$; блок пам'яті ПМ 2, призначений для зберігання елементів $v_{0+i,k}$, $i=\overline{-(k-1),0}$; блоки пам'яті ПМ 3, ПМ 4 та ПМ 5, що призначені для зберігання відповідно елементів $v_{-a+i,k}$, $i=\overline{-k,-1}$, $v_{b+c\cdot a+i,k}$, $i=\overline{-1,k-2}$, та $v_{b,k}$, що отримуються від перевіряльника; віднімач ВДЧ; комутатор К; лічильник ЛІЧ.

Коли претендент повідомляє перевіряльника про бажання щодо перевірки своєї автентичності, перевіряльник здійснює перевірку автентичності претендента наступним чином.

Генератор ГВЧ за сигналом керування «кер.1» генерує випадкове число $c$, яке за сигналом запису «кер.2» записується в блок пам'яті ПМ 1, а звідти разом з елементами $v_{0+i,k}$, $i=\overline{-(k-1),0}$, що знаходяться в блоці пам'яті ПМ 2, подаються на відповідні входи пристрою Пр.V, після чого пристрій Пр.V обчислює за модулем $p$ елементи $v_{c+i,k}$, $i=\overline{-(k-1),0}$, які передаються претенденту.

Потім на входи пристрою Пр.V подаються отримані раніше від претендента елементи відкритого ключа $v_{-a+i,k}$, $i=\overline{-k,-1}$, що зберігаються у блоці пам'яті ПМ 3, а також значення $c$ з блоку пам'яті ПМ 1. Далі пристрій Пр.V обчислює за модулем $p$ елементи $v_{-a\cdot c+i,k}$, $i=\overline{-(k-1),0}$, і зберігає їх у своєму блоці пам'яті. Піс-

ля цього на вхід пристрою Пр.V з блоку пам'яті ПМ 4 надходять отримані від претендента елементи $v_{b+c\cdot a+i,k}$, $i=\overline{-1,k-2}$, і пристрій Пр.V здійснює обчислення за модулем $p$ елемента $v_{-a\cdot c+(b+c\cdot a),k}$.

На завершення, за допомогою пристрою віднімача ВДЧ отриманий елемент $v_{-a\cdot c+(b+c\cdot a),k}$ порівнюється із значенням елемента $v_{b,k}$, який був отриманий від претендента і зберігається у блоці пам'яті ПМ 5. Якщо на виході віднімача ВДЧ буде нуль, то автентичність претендента буде вважатись підтвердженою.

Проведемо тепер дослідження часу роботи розроблених процесорів та порівняємо їх з часом роботи процесорів, що реалізують відомі аналоги.

У [5] встановлено, що час обчислення за модулем елементів $V_k$-послідовності дорівнює:

$$T_V = Hq\cdot\left(k^2+k\right)\cdot T_{мн.Монт.}, \tag{1}$$

де $H$ — кількість машинних одиниць інформації для зберігання великого числа; $q$ — кількість розрядів машинної одиниці інформації; $T_{мн.Монт.}$ — час множення за модулем за методом Монтгомері.

Враховуючи це, час обчислень претендентом на процесорі, що представлений на рис. 1, буде дорівнювати:

$$T_{прет.} = 3Hq\cdot\left(k^2+k\right)\cdot T_{мн.Монт.}, \tag{2}$$

а час обчислень перевіряльника на процесорі, що представлений на рис. 2, буде дорівнювати:

$$T_{перев.} = 2Hq\cdot\left(k^2+k\right)\cdot T_{мн.Монт.}. \tag{3}$$

Проведемо тепер порівняння часу роботи розроблених процесорів реалізації автентифікації суб'єктів (об'єктів) взаємодії з відповідними спеціалізованими процесорами, що реалізують відомі методи.

За основу порівняння візьмемо аналог — відомий метод автентифікації Шнорра. Основною операцією, що виконується в методі Шнорра, є піднесення до степеня за модулем. У [5] показано, що час виконання піднесення до степеня за модулем відповідним пристроєм буде дорівнювати:

$$T_{ПДС\,\mathrm{mod}} = 2\left(Hq+1\right)\cdot T_{мн.Монт}. \tag{4}$$

Використовуючи пристрій піднесення до степеня за модулем для побудови спеціалізованого процесора доведення або перевірки автентичності суб'єктів (об'єктів) взаємодії за відомим методом Шнорра, отримаємо час виконання операцій на цьому процесорі:

$$T_{Шнорра} = 4\left(Hq+1\right)\cdot T_{мн.Монт.}. \tag{5}$$

Аналіз отриманих оцінок показує, що як час доведення автентичності з боку претендента, так і час перевірки з боку перевіряльника на процесорах, що реалізують відомий метод Шнорра, є меншим, ніж відповідними процесорами, що реалізують представлений в [3] метод на основі $V_k$-послідовностей, причому майже у 4 рази, навіть для $k = 2$. Однак, по-перше, розроблені процесори реалізують метод, який є більш криптографічно стійким, ніж відомі методи. По-друге, розробка представленого процесора обумовлена необхідністю використання в криптографічних системах разом з іншими спеціалізованими процесорами, що вирішують різні криптографічні задачі на єдиному математичному апараті рекурентних $V_k$-послідовностей, де переваги в часі роботи можуть бути суттєвими, особливо в тих випадках, коли криптографічні перетворення відбуваються над блоками відкритого або зашифрованого повідомлення $M_j$, $j = \overline{1,Q}$, і обчислення елемента $V_k$-послідовності відбувається лише один раз перед шифруванням всього повідомлення, на відміну від відомих аналогів, коли це здійснити неможливо.

## Висновки

Розроблено спеціалізовані процесори реалізації методу автентифікації суб'єктів (об'єктів) взаємодії на основі рекурентних $V_k$-послідовностей, причому як з боку претендента, що доводить свою автентичність, так і з боку перевіряльника, який цю автентичність перевіряє. Аналіз часу роботи розроблених процесорів показав, що час автентифікації суб'єктів (об'єктів) взаємодії на процесорах, що реалізують відомі методи і базуються на операції піднесення до степеня, є меншим, ніж на розроблених процесорах. Однак, розроблені процесори забезпечують більший рівень криптографічної стійкості процесу автентифікації, а також надають більші можливості щодо їхнього застосування в криптографічних системах, що використовують математичний апарат рекурентних послідовностей.

1. *Menezes A.J.* Handbook of Applied Cryptography / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. — CRC Press, 2001. — 816 p.

2. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. — М.: Триумф, 2002. — 816 с.

3. *Яремчук Ю.Є.* Методи автентифікації на основі рекурентних послідовностей / Ю.Є. Яремчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2013. — Вип. 1(25). — С. 39–49.

4. *Яремчук Ю.Є.* Пристрій обчислення елементів рекурентних послідовностей. Ч. 2. / Ю.Є. Яремчук // Вісник Східноукраїнського національного університету імені Володимира Даля. — 2012. — № 3(174). — С. 212–218.

5. *Яремчук Ю.Є.* Спеціалізовані процесори для здійснення автентифікації сторін взаємодії на основі рекурентних послідовностей / Ю.Є. Яремчук // Захист інформації. — 2013. — Т. 15, № 1. — С. 56–62.

Надійшла до редакції 05.03.2014