УДК 621.391.7

**Ю.Є.Яремчук,**
кандидат технічних наук, доцент

# СПЕЦІАЛІЗОВАНІ ПРОЦЕСОРИ РЕАЛІЗАЦІЇ ШИФРУВАННЯ З ВІДКРИТИМ КЛЮЧЕМ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

*У роботі представлено принципи побудови спеціалізованих процесорів для шифрування з відкритим ключем на основі $V_k^+$ – рекурентних послідовностей. Порівняно з відомими аналогами, розроблені процесори хоча й є менш швидкими, але забезпечують вищий рівень криптографічної стійкості під час шифрування.*

***Ключові слова**: спеціалізовані процесори, захист інформації, криптографія, шифрування з відкритим ключем, рекурентні послідовності.*

*В работе представлены принципы построения специализированных процессоров для шифрования с открытым ключом на основе $V_k^+$ – рекуррентных последовательностей. По сравнению с известными аналогами, разработанные процессоры хоть и являются менее быстрыми, но обеспечивают больший уровень криптографической стойкости во время шифрования.*

***Ключевые слова**: специализированные процессоры, защита информации, криптография, шифрование с открытым ключом, рекуррентные последовательности.*

*Paper presents principles of specialized processors for encryption with the public key based on the $V_k^+$ recurrent sequences. Compared with the known analogues the developed processors although are less speed, but provide a higher level of cryptographic reliability during encryption.*

***Keywords:** specialized processors, information security, cryptography, encryption with the public key, recurrent sequences.*

Задача забезпечення конфіденційності інформація є історично першою й залишається на сьогодні однією з ключових задач криптографії. Вирішення цієї задачі здійснюється методами шифрування [1–3], серед яких найбільшого поширення отримали методи шифрування з відкритим ключем [3], оскільки в них виключається необхідність фізичного розподілу ключів секретним каналом або наявності третьої сторони для реалізації цього.

Найбільш відомими методами шифрування з відкритим ключем є метод, що реалізує відомий стандарт RSA [4], а також метод Ель-Гамаля [5]. В роботі [6] представлено метод шифрування з відкритим ключем на основі рекурентних $V_k^+$ та $U_k$ -послідовностей, який, порівняно з відомими аналогами, забезпечує за певних умов меншу складність обчислень, має простішу процедуру завдання параметрів і дозволяє встановлювати необхідний рівень криптографічної стійкості залежно від порядку послідовності $k$.

Оскільки в криптографічних методах, що використовують технологію відкритого ключа, виконуються досить складні обчислення над числами великої розрядності (1024–4096 двійкових розрядів), це потребує багато часу і тому програмна реалізація не завжди є прийнятною. Підвищення швидкості криптографічних перетворень може бути досягнуто за рахунок апаратної реалізації методів. Тому в роботі [7] розглянуто можливість побудови спеціалізованих процесорів шифрування з відкритим ключем на основі рекурентних $V_k^+$ та $U_k$-послідовностей.

В роботі [8] запропоновано метод шифрування з відкритим ключем на основі математичного апарату тільки рекурентних $V_k^+$-послідовностей, який, порівняно з методом, представленим у роботі [6], забезпечив підвищення стійкості шифрування за рахунок того, що під час шифрування відкрите повідомлення поєднується з елементом рекурентної послідовності, обчисленим за мультиплікативним, а не адитивним способом зміни індексу.

При цьому актуальною залишається розробка спеціалізованих процесорів реалізації запропонованого в роботі [8] методу шифрування з відкритим ключем з метою підвищення швидкості виконання шифрування/дешифрування.

## Розробка принципів побудови спеціалізованих процесорів для шифрування з відкритим ключем

Для реалізації представленого в [8] методу шифрування з відкритим ключем перш за все необхідно реалізувати обчислення за модулем $p$ елементів $v_{n+i,k}$, $i = \overline{-(k-1), k-2}$, а також елементу $v_{m \cdot n,k}$. Ці обчислення пропонується здійснювати на одному пристрої обчислення елементів $V_k^+$ – послідовності. Одним з варіантів реалізації такого пристрою може бути пристрій, представлений в роботі [9].

Для реалізації шифрування (дешифрування) з відкритим ключем передавачем (приймачем) за представленим у [8] методом пропонується схема процесору, що наведена на рис. 1.

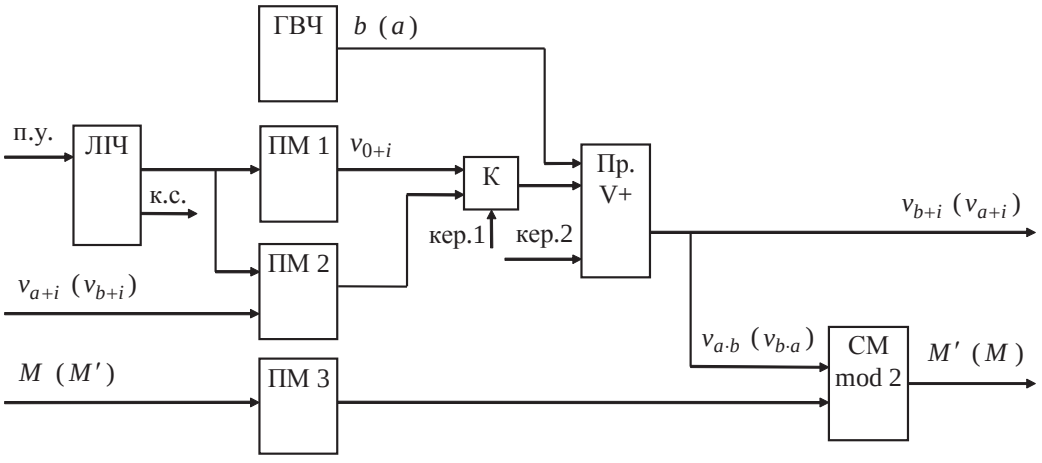


Рис. 1. Структурна схема процесора шифрування (дешифрування) з відкритим ключем на основі $V_k^+$-послідовностей

Процесор містить генератор випадкових чисел ГВЧ; пристрій обчислення елементів $V_k^+$ – послідовностей Пр. V+; суматор за модулем 2 СМ mod 2; 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 при шифруванні передавачем елементів відкритого ключа $v_{a+i,k}$, $i=\overline{-(k-1),0}$, та елементів $v_{b+i,k}$, $i=\overline{-(k-1),0}$, при дешифруванні приймачем; блок пам'яті ПМ 3, призначений для зберігання блоку відкритого повідомлення $M$ або зашифрованого повідомлення $M'$, відповідно, при його шифруванні або дешифруванні; комутатор К; лічильник ЛІЧ.

Робота процесора як із боку передавача, так і з боку приймача буде аналогічною. Розглянемо роботу процесора з боку передавача, яка буде відбуватись таким чином.

Генератор ГВЧ генерує випадкове число $b$, яке разом з даними, що знаходяться в блоці пам'яті ПМ 1, подається на відповідні входи пристрою Пр. V+.

Далі на вхід пристрою Пр.V+ подаються дані з блоку пам'яті ПМ 2, після чого цей пристрій обчислює за модулем $p$ елементи $v_{b+i,k}$, $i=\overline{-(k-1),0}$, які передаються приймачу.

Потім з блоку пам'яті ПМ 2 на вхід пристрою Пр. V+ подаються елементи $v_{a+i,k}$, $i=\overline{-(k-1),0}$, прийняті від приймача, після чого пристрій Пр. V+ здійснює обчислення за модулем $p$ елемента $v_{a\cdot b,k}$, який разом із блоком відкритого повідомлення $M$ надходить на вхід суматора за модулем 2 СМ mod 2, після чого він обчислює результат роботи всього процесора шифрування – зашифроване повідомлення $M'$, що передається приймачу.

Проведемо тепер дослідження часу роботи розробленого процесору та порівняємо його з часом роботи процесора, що реалізує відомий аналог.

У [7] встановлено, що час обчислення за модулем елементів $V_k^+$-послідовності дорівнює:

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

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, а також те, що відкритий ключ $v_{a+i,k}$, $i=\overline{-(k-1),0}$, приймач або центр довіри обчислює на попередньому етапі шифрування лише один раз, так само й обчислення передавачем елементів $v_{b+i,k}$, $i=\overline{-(k-1),0}$, на основі сеансового ключа $b$ здійснюється фактично один раз перед початком сеансу шифрування всього повідомлення $M$, то час обчислень передавачем або приймачем на процесорі, що представлений на рис. 1, буде головним чином дорівнювати часу обчислення елементу $v_{m\cdot n,k}$, тобто

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

Проведемо тепер порівняння розроблених процесорів реалізації шифрування з відкритим ключем з відповідними спеціалізованими процесорами, що реалізують відомі методи.

За основу порівняння візьмемо аналог – відомий метод Ель-Гамаля. Основною операцією, що виконується в методі Ель-Гамаля, є піднесення до ступеня за модулем. В [7] показано, що час виконання піднесення до ступеня за модулем відповідним пристроєм буде дорівнювати:

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

Використовуючи пристрій піднесення до ступеня за модулем для побудови спеціалізованого процесора шифрування (дешифрування) з відкритим ключем за відомим методом Ель-Гамаля, отримаємо час виконання операцій на цьому процесорі:

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

Аналіз отриманих оцінок показує, що час шифрування на процесорах, що реалізують відомий метод Ель-Гамаля, є меншим, ніж на процесорах, що реалізують представлений метод на основі рекурентних $V_k^+$ – послідовностей, причому навіть для $k=2$ майже у 2 рази. Однак, по-перше, розроблені процесори реалізують метод, який є більш криптографічно стійким, ніж відомий метод. По-друге, розробка представленого процесора обумовлена необхідністю використання в криптографічних системах разом з іншими спеціалізованими процесорами, які вирішують різні криптографічні задачі на єдиному математичному апараті рекурентних $V_k^+$ – послідовностей, що дає додаткові переваги методу під час практичної реалізації.

Якщо порівнювати час роботи розроблених процесорів шифрування з відкритим ключем за методом на основі $V_k^+$ – послідовностей з відповідними спеціалізованими процесорами, що реалізують метод на основі рекурентних $V_k^+$ та $U_k$ – послідовностей [7], то розроблені процесори мають також меншу, майже у два рази, швидкість роботи, однак при цьому вони реалізують шифрування інформації на значно вищому рівні криптографічної стійкості.

**Висновки**

Таким чином, розроблено спеціалізовані процесори, що реалізують метод шифрування інформації з відкритим ключем на основі математичного апарату рекурентних $V_k^+$ послідовностей.

Аналіз часу роботи розроблених процесорів показав, що час шифрування інформації на процесорах, що реалізують відомий метод Ель-Гамаля, є меншим, ніж на розроблених процесорах, однак розроблені процесори забезпечують вищий рівень криптографічної стійкості шифрування, а також надають більші можливості щодо їх застосування в криптографічних системах, які використовують математичний апарат рекурентних послідовностей.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

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 / Б. Шнайер. – М. : Триумф, 2002. – 816 с.

3. *Молдовян Н.А.* Введение в криптосистемы с открытым ключом / Н.А. Молдовян., А.А. Молдовян. – Спб. : БХВ-Петербург, 2005. – 288 с.

4. *Rivest R.L., Shamir A., and Adleman L.M.* A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. – 1978. – Volume 21, Issue 2. – P. 120–126.

5. *ElGamal T.* A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Intern. Symp. Informat. Theory. – 1985. – V.IT–31 № 4. – P. 469–472.

6. *Яремчук Ю.Є.* Метод асиметричного шифрування інформації на основі рекурентних послідовностей / Ю.Є. Яремчук // Сучасна спеціальна техніка. –2012. – № 4/ – С. 79–87.

7. *Яремчук Ю.Є.* Спеціалізовані процесори асиметричного шифрування інформації на основі рекурентних послідовностей / Ю.Є. Яремчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 2(24), 2012. – С. 53–58.

8. *Яремчук Ю.Є.* Метод шифрування інформації з відкритим ключем на основі рекурентних послідовностей / Ю.Є. Яремчук // Інформаційна безпека. –2013. – № 3. – С. 41–46.

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

Отримано 2.10.2013.