УДК 621.391.7

Ю.Є. ЯРЕМЧУК, канд. техн. наук

СПЕЦІАЛІЗОВАНІ ПРОЦЕСОРИ РЕАЛІЗАЦІЇ АВТЕНТИФІКАЦІЇ УЧАСНИКІВ ВЗАЄМОДІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Вступ

Проблема автентифікації учасників взаємодії займає важливе місце в криптографічних системах. Такі відомі методи, як Фейге – Фіата - Шаміра, Гіллоу - Куіскуотера та Шнорра [1 – 3], що забезпечують вирішення даної проблеми, базуються на операції піднесення до степеня, яка вимагає виконання досить складних обчислень, а це, в свою чергу, впливає на швидкість роботи методу при його практичній реалізації.

В роботі [4] представлено метод автентифікації учасників взаємодії, який базується на рекурентних V_k^+ та U_k -послідовностях. У порівнянні з відомими методами цей метод має простішу процедуру завдання параметрів та приблизно вдвічі меншу складність обчислень. Крім того, у представленому методі, окрім передавання параметрів, безпосередньо під час автентифікації необхідно виконувати два етапи передавання інформації, замість трьох як у відомих методах.

Оскільки в криптографічних методах, що використовують технологію відкритого ключа, виконуються досить складні обчислення над числами великої розрядності (1024–4096 двійкових розрядів), це вимагає великого часу і тому програмна реалізація не завжди є прийнятною. Підвищення швидкості криптографічних перетворень може бути досягнуто за рахунок апаратної реалізації методів. Тому в роботі [5] розглянуто можливість побудови спеціалізованих процесорів реалізації автентифікації учасників взаємодії на основі рекурентних V_k^+ та U_k -послідовностей.

В роботі [6] запропоновано метод автентифікації учасників взаємодії на основі математичного апарату тільки рекурентних V_k^+-послідовностей, який, у порівнянні з методом представленим у роботі [4], забезпечив підвищення стійкості процесу автентифікації за рахунок отримання коду автентифікації у вигляді елементу послідовності, обчисленого за мультиплікативним, а не адитивним способом зміни індексу.

При цьому актуальною залишається розробка спеціалізованих процесорів реалізації запропонованого в роботі [6] методу автентифікації учасників взаємодії з метою підвищення швидкості виконання процесу автентифікації.

Постановка задач досліджень

Розробити принципи побудови спеціалізованих процесорів реалізації методу автентифікації учасників взаємодії на основі рекурентних V_k^+-послідовностей, що представлений в роботі [6]. Дослідити запропоновані процесори щодо швидкості їх роботи і порівняти з відповідними процесорами, що реалізують відомі методи-аналоги.

Розробка принципів побудови спеціалізованих процесорів реалізації автентифікації учасників взаємодії

Для реалізації представленого в [6] методу автентифікації учасників взаємодії 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, що представлено в роботі [7].

Для реалізації обчислень претендентом згідно представленого методу пропонується процесор, схему якого наведено на рис. 1.

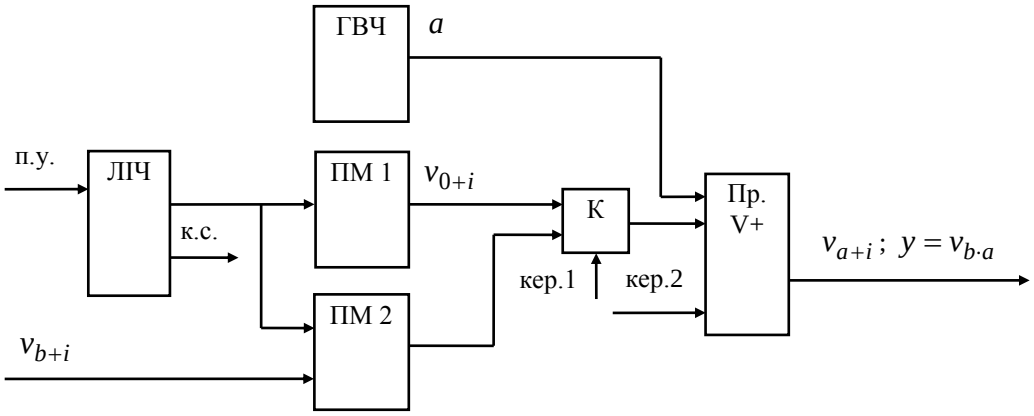

Рис. 1. Структурна схема процесора виконання обчислень претендентом для доведення своєї автентичності

Процесор містить генератор випадкових чисел ГВЧ; пристрій обчислення елементів V_k^+ - послідовностей Пр.V+; 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 претендентом елементів $v_{b+i,k}$, $i = \overline{-(k-1),0}$, що отримуються від перевіряльника; комутатор К; лічильник ЛІЧ.

Доведення претендентом своєї автентичності здійснюється таким чином.

Генератор ГВЧ генерує випадкове число a, яке разом з даними, що знаходяться в блоці пам'яті ПМ 1, подаються 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 $v_{a+i,k}$, $i = \overline{-(k-1),0}$, які як відкритий ключ передаються перевіряльнику.

Потім з блоку пам'яті ПМ 2 на вхід пристрою Пр.V+ подаються елементи $v_{b+i,k}$, $i = \overline{-(k-1),0}$, прийняті від перевіряльника, після чого пристрій Пр.V+ здійснює обчислення за модулем p елементу $v_{b\cdot a,k}$, що отримується на виході процесора як результат коду автентичності y, який передається перевіряльнику.

Неважко помітити, що процесор реалізації обчислень перевіряльником має бути в основному аналогічним тому, що і для претендента. Відмінність полягає лише в тому, що перевіряльнику необхідно перевірити обчислене значення y' як результат $v_{a\cdot b,k}$ за модулем p з отриманим значенням y від претендента шляхом віднімання і пересвідченням того, що отриманий результат буде нулем. Для цього до процесору перевірки автентичності слід ввести додатковий блок пам'яті ПМ 3 для зберігання прийнятого від претендента значення $y = v_{b\cdot a,k} \bmod p$, а також ввести пристрій віднімач ВДЧ для перевірки цього значення з обчисленим значенням $y' = v_{a\cdot b,k} \bmod p$.

Також слід зазначити, що обчислення перевіряльником за модулем p елементів $v_{b+i,k}$, $i = \overline{-(k-1),0}$, буде здійснюватись щоразу при кожному сеансі автентифікації претендента, в той час як відкритий ключ $v_{a+i,k}$, $i = \overline{-(k-1),0}$, буде обчислюватись за модулем p претендентом лише один раз перед великою серією таких сеансів.

Враховуючи сказане, процесор для реалізації обчислень перевіряльником згідно представленого методу буде мати вигляд, схему якого наведено на рис. 2.

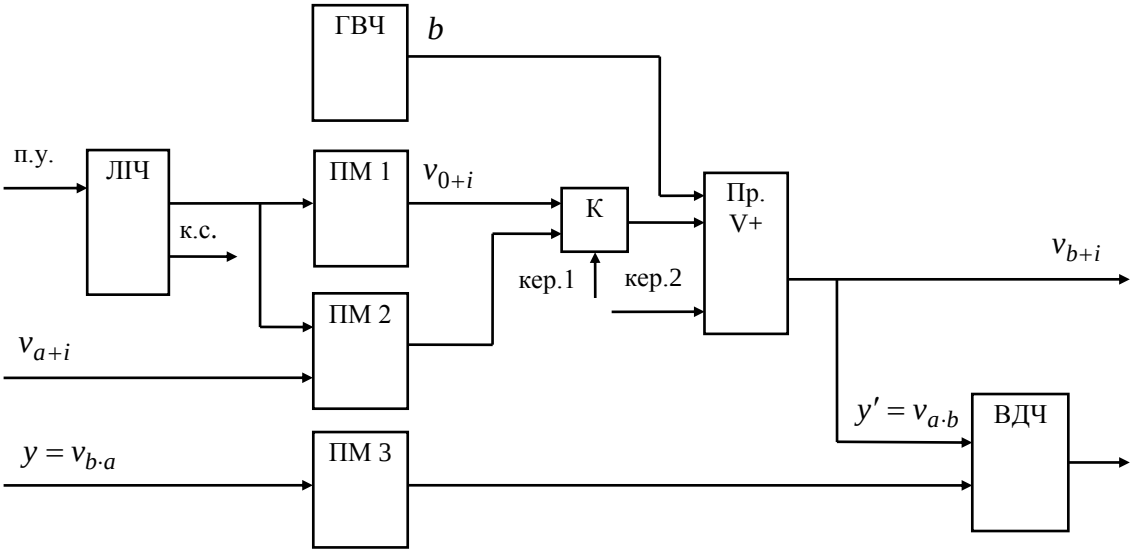

Рис. 2. Структурна схема процесора виконання обчислень перевіряльником для перевірки автентичності претендента

Після отримання перевіряльником коду автентичності y від претендента процесор перевірки автентичності обчислить елемент $y' = v_{a \cdot b,k} \bmod p$ та перевірить його із значенням $y = v_{b \cdot a,k} \bmod p$, що знаходиться в блоці памяті ПМ 3, за допомогою пристрою віднімача ВДЧ. 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.

В [5] встановлено, що час обчислення за модулем елементів V_k^+-послідовності дорівнює:

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

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 як претендентом, так і перевіряльником, на процесорах, що представлені відповідно на рис. 1 та 2, буде дорівнювати

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

Проведемо тепер порівняння часу роботи розроблених процесорів реалізації автентифікації учасників 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. В [5] показано, що час виконання піднесення до степеня за модулем відповідним пристроєм

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

Використовуючи пристрій піднесення до степеня за модулем для побудови спеціалізованого процесору доведення або перевірки автентифікації учасників взаємодії за відомим методом Шнорра, отримаємо час виконання операцій на цьому процесорі

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

Аналіз отриманих оцінок показує, що час доведення автентичності в цілому з боку претендента так і час перевірки з боку перевіряльника на процесорах, що реалізують відомий метод Шнорра, є меншим, ніж на процесорах, що реалізують представлений метод відповідно кожною стороною на основі рекурентних V_k^+ - та U_k -послідовностей, причому майже у три рази, навіть для $k=2$. Однак, по-перше, розроблені процесори реалізують метод, який є більш криптографічно стійким, ніж відомі методи. По-друге, розробка представленого процесору 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 елементу V_k^+ -послідовності відбувається лише один раз перед шифруванням всього повідомлення, на відміну від відомих аналогів, коли це здійснити неможливо.

Якщо порівнювати час роботи розроблених процесорів автентифікації учасників взаємодії за методом на основі V_k^+ -послідовностей з відповідними спеціалізованими процесорами, що реалізують метод на основі рекурентних V_k^+ та U_k -послідовностей [5], то розроблені процесори мають також меншу, майже у два рази, швидкість роботи, однак при цьому вони реалізують автентифікацію на значно вищому рівні криптографічної стійкості.

Висновки

Таким чином, розроблено спеціалізовані процесори, що реалізують метод автентифікації учасників взаємодії на основі математичного апарату рекурентних V_k^+ -послідовностей.

Аналіз часу роботи розроблених процесорів показав, що час автентифікації учасників взаємодії на процесорах, які реалізують відомі методі, що 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 їх застосування в криптографічних системах, що використовують математичний апарат рекурентних послідовностей.

Список літератури: 1. *Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.* Handbook of Applied Cryptography. – CRC Press, 2001. – 816 p. 2. *Петров, А.А.* Компьютерная безопасность. Криптографические методы защиты. – М. : ДМК, 2000. – 448 с. 3. *Романец, Ю.В., Тимофеева, П.А., Шаньгин, В.Ф.* Защита информации в компьютерных системах и сетях. – М. : Радио и связь, 2001. – 376 с. 4. *Яремчук, Ю.Є.* Метод автентифікації сторін взаємодії на основі рекурентних послідовностей // Сучасний захист інформації. – 2013. - №1. – С. 4–10. 5. *Яремчук, Ю.Є.* Спеціалізовані процесори для здійснення автентифікації сторін взаємодії на основі рекурентних послідовностей // Захист інформації. – Т. 15, №1, 2013. – С. 56–62. 6. *Яремчук, Ю.Є.* Можливість автентифікації сторін взаємодії на основі рекурентних послідовностей // Захист інформації. – 2013. - Т. 15, №4. – С. 76–81. 7. *Яремчук, Ю.Є.* Пристрій обчислення елементів рекурентних послідовностей // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2012. - №3(174), Ч. 2. – С. 212–218.

Вінницький національний технічний університет *Надійшла до редколегії 11.10.2013*