УДК 621.391.7

Ю.Є. ЯРЕМЧУК, канд. техн. наук

СПЕЦІАЛІЗОВАНІ ПРОЦЕСОРИ РЕАЛІЗАЦІЇ ЦИФРОВОГО ПІДПИСУВАННЯ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Вступ

Цифрові підписи мають широке застосування в галузі інформаційної безпеки, включаючи автентифікацію, цілісність даних і безвідмовність [1]. В загальному випадку цифровий підпис являє собою деяке число специфічної структури, яке допускає перевірку за допомогою відкритого ключа того факту, що воно було вироблено для деякого повідомлення з використанням секретного ключа.

Цифрове підписування передбачає два етапи: формування та перевіряння цифрового підпису, що реалізується за певним протоколом [1]. Серед існуючих протоколів цифрового підписування найбільшого поширення отримали ті, що реалізують рандомізовані схеми з додаванням повідомлення, зокрема це методи Шнорра, Ель-Гамаля, DSA [1 – 3]. Ці методи 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. Актуальним також залишається питання підвищення криптографічної стійкості методів цифрового підписування.

В роботі [4] представлено метод цифрового підписування на основі математичного апарату рекурентних V_k –послідовностей, в якому відбувається заміна піднесення до степеня обчисленням елементу рекурентної послідовності з певним індексом. У порівнянні з відомими методами цей метод є більш стійким, має значно простішу процедуру завдання параметрів, а також забезпечує спрощення обчислень процедури перевірки цифрового підпису.

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

Мета роботи - розробка спеціалізованих процесорів реалізації запропонованого в роботі [4] методу цифрового підписування з метою підвищення швидкості виконання процедур формування та перевіряння підпису.

Постановка задач досліджень

Розробити принципи побудови спеціалізованих процесорів реалізації методу цифрового підписування на основі рекурентних V_k –послідовностей, що представлений в роботі [4]. Дослідити запропоновані процесори щодо швидкості їх роботи і порівняти з відповідними процесорами, що реалізують відомі методи-аналоги.

Розробка принципів побудови спеціалізованих процесорів реалізації цифрового підписування на основі V_k –послідовностей

Для реалізації представленого в [4] методу цифрового підписування 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 $v_{-n\cdot m+i,k}$, $i = \overline{-(k-1), 0}$, а також елементу $v_{-n+m,k}$. 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 [5].

Для реалізації підписантом формування цифрового підпису згідно представленого в [4] методу цифрового підписування пропонується процесор, схему якого наведено на рис. 1.

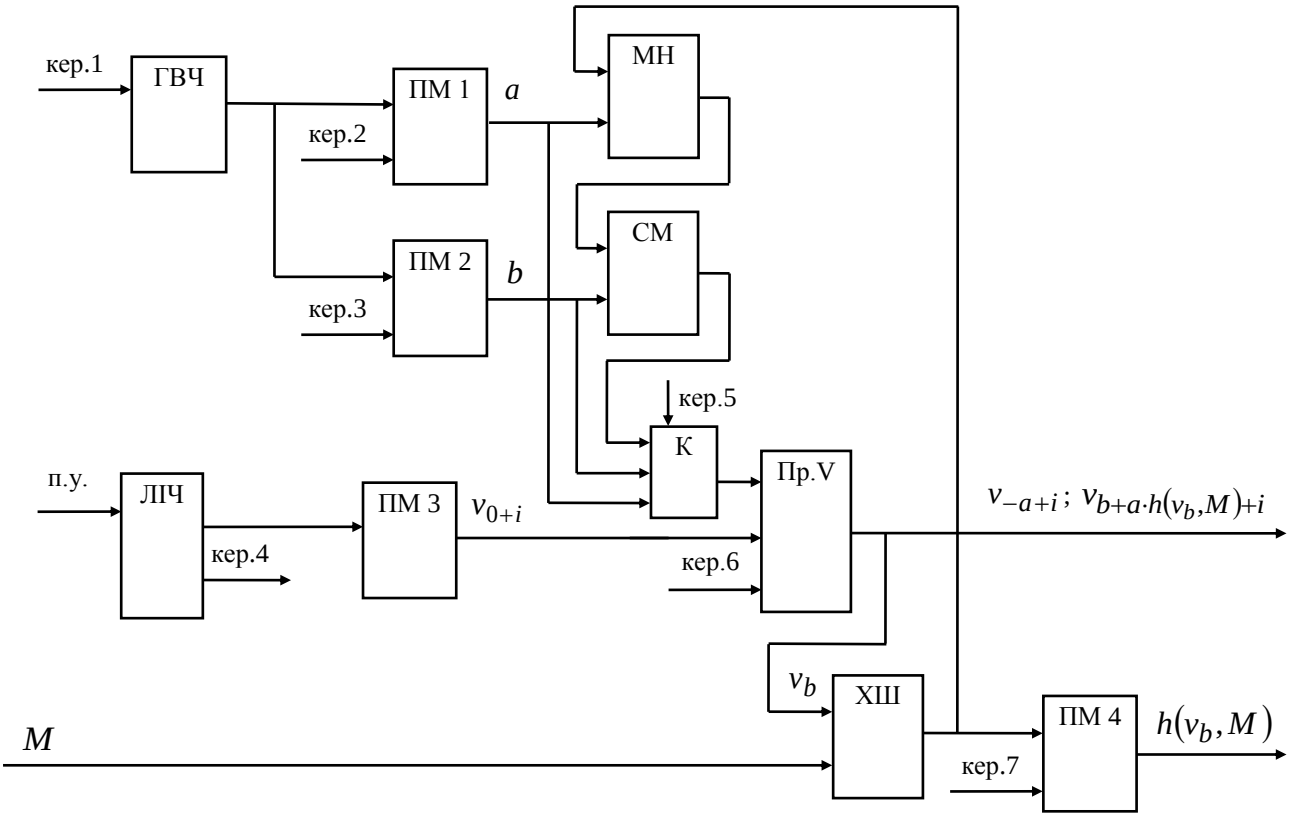

Рис. 1. Структурна схема процесора формування цифрового підпису

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; блок пам'яті ПМ 3, призначений для зберігання елементів $v_{0+i,k}$, $i=\overline{-(k-1),0}$; блок пам'яті ПМ 4, призначений для зберігання хеш-значення $h(v_b,M)$; суматор СМ; пристрій множення МН; пристрій хешування ХШ; комутатор К; лічильник ЛІЧ.

Формування підписантом цифрового підпису здійснюється таким чином.

Генератор ГВЧ за сигналом керування «кер.1» генерує випадкове число a, яке за сигналом запису «кер.2» записується у 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 елементу блоку пам'яті ПМ 3. По завершенні роботи лічильника ЛІЧ на пристрій керування подається сигнал кінця роботи «кер.4».

Безпосередньо під час формування підписантом цифрового підпису, 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 цього пристрій Пр.V у відповідному режимі за сигналом керування «кер.6» обчислює за модулем p елемент $v_{b,k}$, який разом із відкритим повідомленням M подається на пристрій хешування ХШ і той

обчислює хеш-значення $h(v_b \bmod p, M)$, яке записується у блок пам'яті ПМ 4. В цей же час отримане значення $h(v_b \bmod p, M)$ з пристрою хешування ХШ разом із значенням a, що зберігається у блоці пам'яті ПМ 1, подаються на пристрій множення МН, на якому обчислюється значення $a \cdot h(v_b \bmod p, M)$ і результат подається разом із значенням b, що зберігається у блоці пам'яті ПМ 2, на суматор СМ, який обчислює значення $b + a \cdot h(v_b \bmod p, M)$. Це значення разом з елементами $v_{0+i,k}$, $i = \overline{-(k-1),0}$, що знаходяться у блоці пам'яті ПМ 3, подаються на відповідні входи пристрою Пр.V і той у відповідному режимі за сигналом керування «кер.6» обчислює за модулем p елементи $v_{b+a\cdot h(v_b \bmod p,M)+i,k}$, $i = \overline{-1,k-2}$, які разом із раніше обчисленим хеш-значенням $h(v_b \bmod p, M)$, що зберігається у блоці пам'яті ПМ 4, передаються перевіряльнику.

Для реалізації обчислень перевіряльником згідно представленого в [4] методу цифрового підписування пропонується процесор, схему якого наведено на рис. 2.

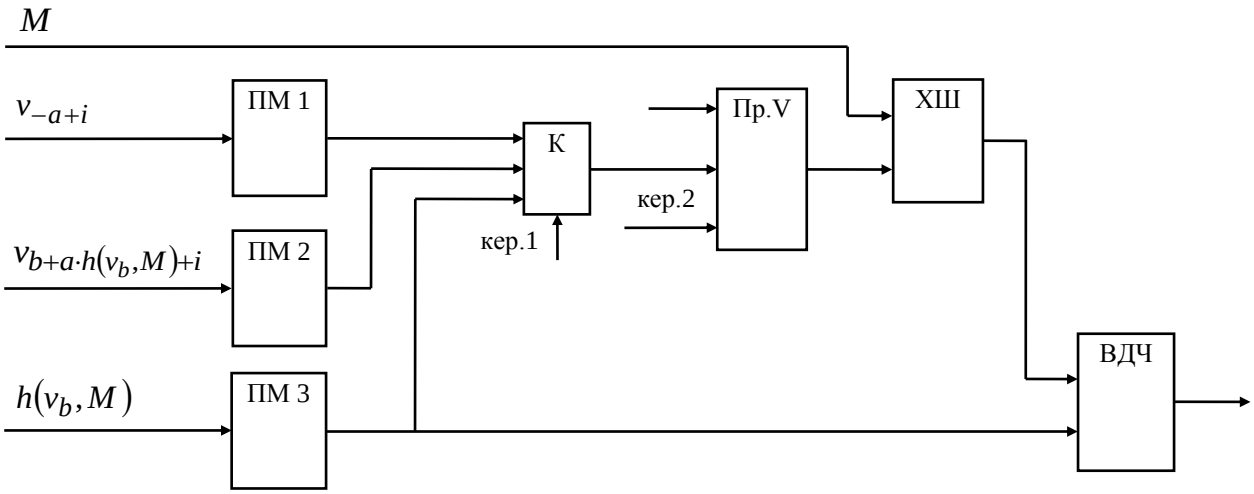

Рис. 2. Структурна схема процесора перевіряння цифрового підпису

Процесор містить пристрій обчислення елементів V_k – послідовностей Пр.V; блоки пам'яті ПМ 1, ПМ 2 та ПМ 3, що призначені для зберігання відповідно елементів $v_{-a+i,k}$, $i = \overline{-k,-1}$, елементів $v_{b+a\cdot h(v_b \bmod p,M)+i,k}$, $i = \overline{-1,k-2}$, та хеш-значення $h(v_b \bmod p, M)$, що отримуються від підписанта; пристрій хешування ХШ; віднімач ВДЧ; комутатор К.

Перевіряльник здійснює перевірку отриманого від підписанта цифрового підпису таким чином.

Спочатку на вхід пристрою Пр.V подаються отримані раніше від підписанта елементи відкритого ключа $v_{-a+i,k}$, $i = \overline{-k,-1}$, що зберігаються у блоці пам'яті ПМ 1, а також значення $h(v_b \bmod p, M)$ з блоку пам'яті ПМ 3. Далі пристрій Пр.V у відповідному режимі за сигналом керування «кер.2» обчислює за модулем p елементи $v_{-a\cdot h(v_b \bmod p,M)+i,k}$, $i = \overline{-(k-1),0}$, і зберігає їх у своєму блоці пам'яті. Після цього на вхід пристрою Пр.V з блоку пам'яті ПМ 2 надходять елементи $v_{b+a\cdot h(v_b \bmod p,M)+i,k}$, $i = \overline{-1,k-2}$, і пристрій Пр.V здійснює обчислення за модулем p елементу $v_{-a\cdot h(v_b \bmod p,M)+(b+a\cdot h(v_b \bmod p,M)),k}$. Потім отриманий елемент з виходу пристрою Пр.V разом з відкритим повідомленням M подається на пристрій хешування ХШ, який здійснює обчислення хеш-значення.

На завершення, за допомогою пристрою віднімача ВДЧ отримане на виході пристрою хешування ХШ значення порівнюється із значенням елементу $h(v_b \bmod p, M)$, що отримано від підписанта і зберігається у блоці пам'яті ПМ 3. Якщо на виході віднімача ВДЧ буде нуль, то підпис приймається, інакше – відкидається.

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

В [6] встановлено, що час обчислення за модулем елементів V_k-послідовності з великим значенням індексу

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

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.

Оскільки в сучасних криптосистемах оперують з числами великої розрядності, тобто Hq буде приймати значення порядка 1024–4096 розрядів, то при оцінюванні часу виконання процедур цифрового підписування на розроблених процесорах оцінками інших обчислень, окрім обчислень елементу V_k-послідовності за прискореними алгоритмами, можна знехтувати.

Враховуючи це, час обчислень формування підпису підписантом на процесорі, що представлений на рис. 1,

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

а час обчислень перевіряння підпису на процесорі, що представлений на рис. 2,

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

Проведемо тепер порівняння часу роботи розроблених процесорів реалізації цифрового підписування з відповідними спеціалізованими процесорами, що реалізують відомі методи.

За основу порівняння візьмемо аналог – відомий метод цифрового підписування Шнорра. Основною операцією, що виконується в методі Шнорра, є піднесення до степеня за модулем. В [6] показано, що час виконання піднесення до степеня за модулем відповідним пристроєм буде дорівнювати

$$T_{ПДС \bmod} = 2(Hq + 1) \cdot T_{мн.Монт.}. \tag{4}$$

Використовуючи пристрій піднесення до степеня за модулем для побудови спеціалізованого процесору формування або перевіряння цифрового підпису за відомим методом Шнорра, отримаємо час виконання операцій на цьому процесорі:

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

Аналіз отриманих оцінок показує, що час формування цифрового підпису підписантом на процесорі, що реалізує відомий метод Шнорра, є меншим, ніж на відповідному процесорі, що реалізує представлений в [4] метод на основі V_k – послідовностей, причому для $k = 2$ у чотири рази. Однак при цьому час перевірки цифрового підпису з боку перевіряльника на розробленому процесорі за рівних умов ($k = 1$) є меншим, ніж на відповідному процесорі, що реалізує відомий метод Шнорра.

Також слід зазначити, що, по-перше, розроблені процесори реалізують метод, який є більш криптографічно стійким, ніж відомі методи. По-друге, розробка представлених процесорів 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.

Висновки

Розроблено спеціалізовані процесори реалізації методу цифрового підписування на основі рекурентних V_k-послідовностей, причому як формування цифрового підпису з боку підписанта, так перевірки підпису з боку перевіряльника.

Аналіз часу роботи розроблених процесорів показав, що в цілому час цифрового підписування на процесорах, що реалізують відомі методи і базуються на операції піднесення до степеня, є меншим, ніж на розроблених процесорах. Однак за рівних умов час роботи процесору перевірки підпису, що базується на математичному апараті V_k-послідовностей, є меншим, ніж на відповідному процесорі, що реалізує відомий метод-аналог. Окрім того, розроблені процесори забезпечують більший рівень криптографічної стійкості цифрового підписування, 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. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М. : Триумф, 2002. – 816 с. 3. *Молдавян, Н.А.* Теоретический минимум и алгоритмы цифровой подписи. – СПб. : БХВ-Петербург, 2010. – 304 с. 4. *Яремчук, Ю.Є.* Метод цифрового підписування на основі рекурентних послідовностей // Інформаційна безпека. –2013. – №1. – С. 165–175. 5. *Яремчук, Ю.Є.* Пристрій обчислення елементів рекурентних послідовностей // Вісник Східноукраїнського нац. ун-ту імені Володимира Даля. – 2012. - №3(174), Ч. 2. – С. 212–218. 6. *Яремчук, Ю.Є.* Спеціалізовані процесори для здійснення автентифікації сторін взаємодії на основі рекурентних послідовностей // Захист інформації. – 2013. – Т. 15, №1. – С. 56–62.

Вінницький національний технічний університет *Надійшла до редколегії 14.01.2014*