2. *Сапожников Н.Е.* К вопросу о выполнении операции сложения над вероятностно преобразованными сигналами / Н.Е. Сапожников // Сб. Всесоюзной школы-семинара "Передача, обработка и отображение информации". – Теберда - Харьков, 1991. − С. 25 - 28.

3. *Сапожников Н.Е.* Сравнительная оценка эффективности дискретных форм представления информации / Н.Е. Сапожников // Зб. наук. пр. СНУЯЕтаП. – Севастополь: СНУЯЭиП, 2000. – Вып. 1. – С. 64 – 70.

4. *Сапожников Н.Е.* Оценка точности и быстродействия при вероятностной форме представления информации / Н.Е. Сапожников, Д.В. Моисеев, Ю.Ю. Столярчук // Зб. наук. пр. СНУЯЕтаП. – Севастополь: СНУЯЭиП, 2011. – Вып. 3 (39). − С. 134 - 140.

5. *Сапожников Н.Е.* Вероятностные вычислительные модели // Н.Е. Сапожников, Д.В. Моисеев, А.Г. Шокин, Ю.А. Барановский // Зб. наук. пр. СНУЯЕтаП. – Севастополь: СНУЯЭиП, 2013. – Вип. 1 (45). − С. 210 - 215.

6. *Сапожников Н.Е.* Выполнение параллельных вычислений при вероятностном представлении информации / Н.Е. Сапожников, Д.В. Моисеев, П.С. Бейнер, Н.В. Бейнер // Technology audiT and producTion reserves. − Харьков, 2013. - № 3/1 (11). − С. 9 – 12.

7. *Угрюмов Е.П.* Цифровая схемотехника: учеб. пособие для вузов / Е.П. Угрюмов. – 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2004. – 800 с.

8. Пат. 103342 Україна, МПК (2013.01) H03M 1/00. Імовірнісний перелельний сумато р / Сапожніков М.Є. (UA), Моісєєв Д.В. (UA), Редько О.С. (UA), Пахомова А.А. (UA); заявитель и патентообладатель Севастопольський національний університет ядерної енергії та промисловості. − № a2001106863; заяв. 31.05.11, опубл. 10.10.2013, Бюл. № 19.

Надійшла до редакції 27.11.2013 р.

УДК 621.391.7

СПЕЦІАЛІЗОВАНІ ПРОЦЕСОРИ РЕАЛІЗАЦІЇ ВІДКРИТОГО РОЗПОДІЛУ СЕКРЕТНИХ КЛЮЧІВ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Ю.Є. Яремчик, к.т.н., доц.

Центр інформаційних технологій і захисту інформації
Вінницького національного технічного університету

В роботі представлено принципи побудови спеціалізованих процесорів відкритого розподілу секретних ключів на основі V_k^+–рекурентних послідовностей. У порівнянні з відомими аналогами розроблені процесори хоч і є менш швидкими, але забезпечують більший рівень криптографічної стійкості підчас розподілу.

Вступ

Вирішення проблеми керування ключами є на сьогодні однією з важливих задач криптографії. Ключ - секретна інформація, що використовується криптографічним алгоритмом при шифруванні/дешифруванні повідомлень, обчисленні коду автентичності, генеруванні та перевірці цифрового підпису. При використанні одного й того ж алгори-

тму результат шифрування залежить від ключа. Для сучасних алгоритмів сильної криптографії втрата ключа приводить до практичної неможливості розшифрувати інформацію. Згідно з принципом Керхгоффа, надійність криптографічної системи повинна визначатися секретністю ключів, але не секретністю використовуваних алгоритмів або їх особливостей.

Найбільш гостро проблема розподілу ключів стає в симетричних криптосистемах [1], коли перед початком роботи систем виникає необхідність здійснювати попереднє передавання секретного ключа обом сторонам. Вперше можливість розподілу секретних ключів відкритим каналом зв'язку була запропонована Діффі та Хеллманом [2]. Даний метод базується на операції піднесенні до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість його роботи при практичній реалізації.

В роботі [3] представлено метод розподілу секретних ключів відкритим каналом, який базується на рекурентних V_k^+ та U_k –послідовностей. У порівнянні з відомим методом розподілу ключів Діффі-Хеллмана запропонований метод забезпечує для кожного користувача майже вдвічі меншу складність обчислень. Крім того, запропонований метод має простішу процедуру завдання параметрів.

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 [4] розглянуто можливість побудови спеціалізованих процесорів для розподілу секретних ключів на основі рекурентних V_k^+ та U_k –послідовностей.

В роботі [5] запропоновано метод відкритого розподілу секретних ключів на основі математичного апарату тільки рекурентних V_k^+ –послідовностей, який, у порівнянні з методом представленим у роботі [3], забезпечив підвищення стійкості розподілу ключів за рахунок отримання спільного ключа на завершальному етапі розподілу у вигляді елементу послідовності, обчисленого за мультиплікативним, а не адитивним способом зміни індексу.

При цьому актуальним залишається розробка спеціалізованих процесорів реалізації запропонованого в роботі [5] методу відкритого розподілу секретних ключів з метою підвищення швидкості виконання розподілу.

Розробка принципів побудови спеціалізованих процесорів реалізації відкритого розподілу секретних ключів

Для реалізації представленого в [5] методу відкритого розподілу секретних ключів 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 [6].

Не важко помітити, що згідно представленого методу Користувач A та Користувач B виконують однакові операції. Тому реалізацію відкритого розподілу секретних ключів як з боку одного користувача, так і другого, пропонується здійснювати на процесорі, схема якого наведена на рисунки.

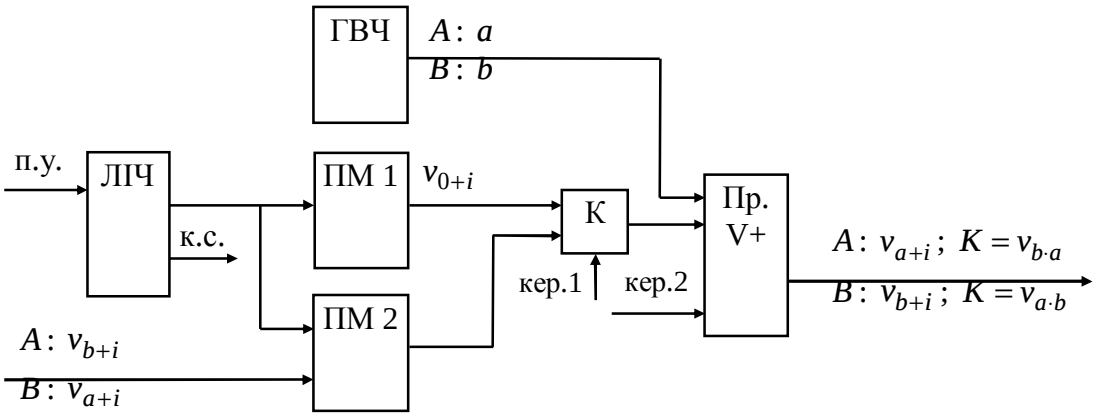

Рис. Структурна схема процесора для розподілу секретних ключів на основі V_k^+–послідовностей

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 Користувачем A елементів $v_{b+i,k}$, $i = \overline{-(k-1),0}$, та елементів $v_{a+i,k}$, $i = \overline{-(k-1),0}$ Користувачем B; комутатор К; лічильник ЛІЧ.

Робота процесора як з боку Користувача A, так і з боку Користувача B буде аналогічною. Розглянемо роботу процесора з боку Користувача A, яка буде відбуватись 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 передаються Користувачу B.

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 Користувача B, після чого пристрій Пр.V+ здійснює обчислення за модулем p елементу $v_{b\cdot a,k}$ як результат секретного ключа K, що отримується на виході процесора.

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

В [4] встановлено, що час обчислення за модулем елементів V_k^+–послідовності дорівнює

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

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.

Враховуючи це, час обчислень кожним з користувачів на процесорі, що представлений на рисунки, буде дорівнювати

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

Проведемо тепер порівняння розроблених процесорів для розподілу секретних ключів з відповідними спеціалізованими процесорами, що реалізують відомий метод.

За основу порівняння візьмемо аналог – відомий метод Діффі-Хеллмана. Основною операцією, що виконується в методі Діффі-Хеллмана, є піднесення до степеня за модулем. В [4] показано, що час виконання піднесення до степеня за модулем відповідним пристроєм буде дорівнювати

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

Використовуючи пристрій піднесення до степеня за модулем для побудови спеціалізованого процесору розподілу секретних ключів за відомим методом Діффі-Хеллмана, отримаємо час виконання операцій на цьому процесорі:

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

Аналіз отриманих оцінок показує, що час розподілу секретних ключів на процесорах, що реалізують відомий метод Діффі-Хеллмана, є меншим, ніж на процесорах, що реалізують представлений метод на основі рекурентних V_k^+–послідовностей, причому навіть для $k=2$ майже у 3 рази. Однак, по-перше, розроблені процесори реалізують метод, який є більш криптографічно стійким, ніж відомий метод. 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 не можливо.

Якщо порівнювати час роботи розроблених процесорів відкритого розподілу секретних ключів за методом на основі V_k^+–послідовностей з відповідними спеціалізованими процесорами, що реалізують метод на основі рекурентних V_k^+ та U_k–послідовностей [4], то розроблені процесори мають також меншу, майже у два рази, швидкість роботи, однак при цьому вони реалізують розподіл ключів на значно вищому рівні криптографічної стійкості.

Висновки

Таким чином, розроблено спеціалізовані процесори, що реалізують метод відкритого розподілу секретних ключів на основі математичного апарату рекурентних V_k^+–послідовностей.

Аналіз часу роботи розроблених процесорів показав, що час розподілу секретних ключів на процесорах, що реалізують відомий метод Діффі-Хеллмана, є меншим, ніж на розроблених процесорах, однак розроблені процесори забезпечують більший рівень криптографічної стійкості процесу розподілу, а також надають більші можливості щодо їх застосування в криптографічних системах, що використовують математичний апарат рекурентних послідовностей.

СПЕЦИАЛИЗИРОВАННЫЕ ПРОЦЕССОРЫ РЕАЛИЗАЦИИ ОТКРЫТОГО РАСПРЕДЕЛЕНИЯ СЕКРЕТНЫХ КЛЮЧЕЙ НА ОСНОВЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Ю.Е. Яремчук

В работе представлены принципы построения специализированных процессоров открытого распределения секретных ключей 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 распределения.

SPECIALIZED PROCESSORS REALIZATION PUBLIC DISTRIBUTION of SECRET KEYS BASED on RECURRENT SEQUENCES

I. Iaremchuk

The paper presents principles of specialized processors for public distribution of secret keys based on the V_k^+ recurrent sequences. Compared with the known analogues developed processors although less speed, but provide a higher level of cryptographic reliability during distribution.

Список використаних джерел

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

2. *Diffie W.* New directions in cryptography / W. Diffie, M.E. Hellman // IEEE Transactions on Information Theory. – 1976. - № 22. – P. 644 – 654.

3. *Яремчук Ю.Є.* Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем / Ю.Є. Яремчук // Захист інформації. - 2012. – № 4. – С. 120 – 127.

4. *Яремчук Ю.Є.* Спеціалізовані процесори для розподілу секретних ключів на основі рекурентних послідовностей / Ю.Є. Яремчук // Вісник Вінницького політехнічного інституту. - 2013. – С. 123 – 127.

5. *Яремчук Ю.Є.* Метод відкритого розподілу секретних ключів на основі рекурентних послідовностей / Ю.Є. Яремчук // Інформаційна безпека. - 2013. – № 2. – С. 177 – 183.

6. *Яремчук Ю.Є.* Пристрій обчислення елементів рекурентних послідовностей / Ю.Є. Яремчук // Вісник Східноукраїнського націон. ун-ту ім. В. Даля. − Ч. 2. – 2012. - № 3 (174). – С. 212 – 218.

Надійшла до редакції 17.12.2013 р.