УДК 621.391.7

Ю. Є. Яремчук, канд. техн. наук, доц.

СПЕЦІАЛІЗОВАНІ ПРОЦЕСОРИ ДЛЯ РОЗПОДІЛУ СЕКРЕТНИХ КЛЮЧІВ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Викладено принципи побудови спеціалізованих процесорів для розподілу секретних ключів відкритим каналом зв'язку на основі рекурентних послідовностей. Проведено оцінювання часу роботи розроблених процесорів. Порівняння швидкості роботи розроблених процесорів з відомими аналогами показало, що за певних умов вони можуть забезпечувати значно меншу складність обчислень для кожного користувача.

Вступ

Задача забезпечення конфіденційності інформації може бути розв'язана лише за умови вирішення проблеми керування ключами [1]. Розподіл ключів є однією з фундаментальних задач криптографії. Найгостріше проблема розподілу ключів стає в симетричних криптосистемах, де перед початком роботи необхідно здійснювати передавання секретного ключа обом сторонам.

Вперше можливість розподілу секретних ключів відкритим каналом зв'язку була запропонована Діффі та Хеллманом [2]. Криптостійкість методу Діффі–Хеллмана базується на складності обчислення дискретних логарифмів, що на сьогодні відноситься до важкорозв'язуваних задач. Однак при цьому проблема дискретного логарифмування досліджується доволі активно, тому пошук надійних методів розподілу ключів залишається актуальним.

В роботі [3] запропоновано метод LUCDIF, який є аналогом методу Діффі–Хеллмана і використовує в своїй основі рекурентні послідовності Люка за модулем простого числа p замість модулярного піднесення до степеня. Пізніше в роботі [4] було показано, що функції Люка, які є аналогом проблеми дискретного логарифмування, послаблюють проблему дискретного логарифмування, а сам метод не володіє якимось суттєвими перевагами в порівнянні з оригінальним методом.

В роботі [5] показано можливість побудови протоколу Діффі–Хеллмана на основі технології еліптичних кривих. Математичний апарат еліптичних кривих дає можливість для забезпечення високої обчислювальної складності криптографічних перетворень на еліптичних кривих використовувати у порівнянні з відомим методом менші довжини ключів та загальносистемних параметрів, що, в свою чергу, приводить до підвищення швидкодії та зменшення апаратних витрат. Незважаючи на це, слід відмітити наявність значної кількості атак на криптографічні схеми, що базуються на еліптичних кривих, більшість з яких розглянуто в [6].

В роботі [7] викладено 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 за певних умов дозволяє спрощувати обчислення і має простішу процедуру задання параметрів. Крім того, він є стійкішим, а також дозволяє встановлювати необхідну криптостійкість залежно від порядку послідовності k .

Особливість криптографічних методів полягає в тому, що в них необхідно виконувати обчислення над числами великої розрядності (1024—4096 двійкових розрядів), що вимагає затрат часу, і тому програмна реалізація не завжди є прийнятною. Підвищення швидкості криптографічних перетворень може бути досягнуто за рахунок їх апаратної реалізації. Тому розглядається можливість побудови спеціалізованих процесорів для розподілу секретних ключів на основі рекурентних V_k^+- та U_k-послідовностей.

Розподіл секретних ключів на основі рекурентних послідовностей

V_k^+-послідовністю [7] називається послідовність чисел, що обчислюються за формулою

$$v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k} \qquad (1)$$

для початкових значень $v_{0,k}=1$, $v_{1,k}=g_2$ для $k=2$;

$v_{0,k}=v_{1,k}=...=v_{k-3,k}=0$; $v_{k-2,k}=1$; $v_{k-1,k}=g_k$ для $k>2$,

де g_1, g_k — цілі числа; n і k — цілі додатні числа.

Формула (1) дозволяє отримувати значення для зростаючих n, починаючи з $n=0$. Можлива і зворотна процедура, коли елементи послідовності обчислюються для спадних n, починаючи з деякого значення $n=l$. Обчислення елементів такої послідовності буде здійснюватись таким чином:

$$v_{n,k}=\frac{v_{n+k,k}-g_k v_{n+k-1,k}}{g_1}. \tag{2}$$

U_k-послідовністю [7] називається послідовність чисел, що обчислюються за формулою

$$u_{n,k}=g_k u_{n-1,k}+g_1 u_{n-k,k} \tag{3}$$

для початкових значень $u_{0,k}=g_1$, $u_{1,k}=g_2$, $u_{2,k}=g_3$, ... $u_{k-1,k}=g_k$,

де g_1, g_2, g_3, ..., g_k — цілі числа; n і k — цілі додатні числа.

Для будь-яких цілих додатних n, m та k отримано таку залежність:

$$u_{n+m,k}=v_{m+(k-2),k}\cdot u_{n,k}+g_1\cdot\sum_{i=1}^{k-1}v_{m+(k-2)-i,k}\cdot u_{n-k+i,k}\,. \tag{4}$$

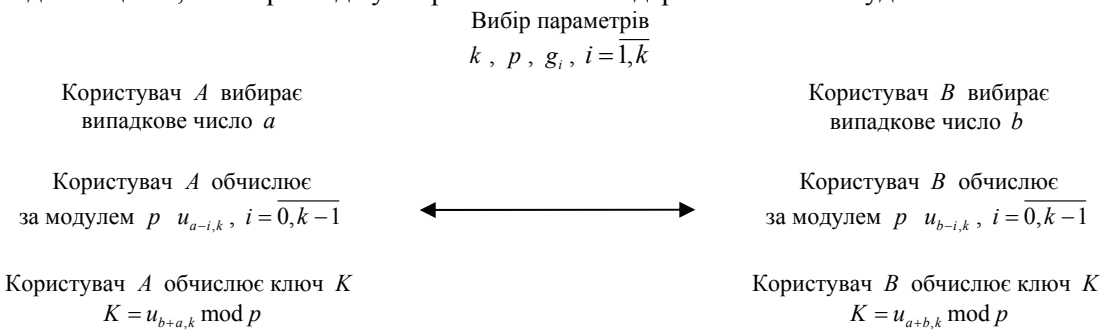
Для будь-яких цілих додатних n та k, таких що $n\geq k$, отримано залежність, яка дозволяє обчислювати елементи U_k-послідовності тільки на основі елементів V_k^+-послідовності:

$$u_{n,k}=g_k v_{n-1,k}+g_1\sum_{i=1}^{k-1}g_i\cdot v_{n-i-1,k}. \tag{5}$$

Метод розподілу секретних ключів [7] базується на властивості (4), яка дозволяє обчислити елемент $u_{n+m,k}$, використовуючи елементи V_k^+- та U_k-послідовностей, причому можна зробити це двома шляхами: або використовуючи елементи $v_{m+i,k}$, $i=\overline{-1,k-2}$, та $u_{n-i,k}$, $i=\overline{0,k-1}$, або використовуючи елементи $v_{n+i,k}$, $i=\overline{-1,k-2}$, та $u_{m-i,k}$, $i=\overline{0,k-1}$.

Тоді, якщо один користувач для будь-якого вибраного ним випадкового числа a обчислить $u_{a-i,k}$, $i=\overline{0,k-1}$, а другий користувач аналогічним чином обчислить $u_{b-i,k}$, $i=\overline{0,k-1}$, то, обмінявшись обчисленими значеннями, кожен з них зможе отримати $u_{a+b,k}$, продовжуючи обчислення на своєму боці за формулою (4), використовуючи, відповідно, свої числа a або b. В цьому випадку $u_{a+b,k}$ буде ключем розподілу, а числа a і b — секретним ключем кожного користувача. Причому a і b — це частини секретного ключа кожного користувача, оскільки попереднє отримання ключа розподілу будь-яким користувачем неможливе без отримання відповідної інформації від іншого користувача.

Виходячи з цього, схема розподілу секретних ключів відкритим каналом буде мати такий вигляд:



Операція за модулем в схемі розподілу ключів використовується для обмеження розрядності чисел під час виконання арифметичних операцій.

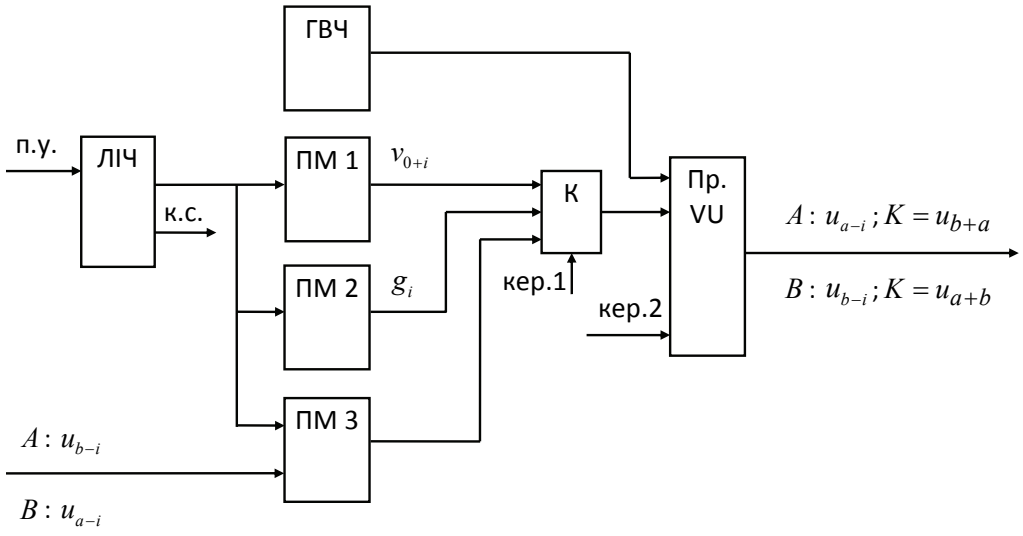
Відповідно до запропонованого методу основні обчислення виконуються за формулою (4). Для обчислення елемента $u_{n+m,k}$ за цією формулою потрібні елементи $v_{m+i,k}$, $i=\overline{-1,k-2}$, та елементи $u_{n-i,k}$, $i=\overline{0,k-1}$. Обчислення останнього набору елементів здійснюється за формулою (5), для чого необхідно мати елементи $v_{n+i,k}$, $i=\overline{-2k+1,-1}$. Звідси випливає, що всього для обчислення елемента $u_{n+m,k}$ за формулою (4) потрібно мати елементи $v_{n+i,k}$, $i=\overline{-2k+1,k-2}$. Задача знаходження цих елементів зводиться до отримання будь-яких послідовних k з них, оскільки інші можуть бути обчислені за формулами (1) або (2) на основі вже отриманих.

Проблема обчислення елемента $v_{n,k}$ полягає в тому, що для великих значень n, а саме такі значення повинні використовуватись в криптографічних перетвореннях, обчислення $v_{n,k}$ за формулою (1) є неприйнятним. Тому обчислення елемента $v_{n,k}$ може здійснюватись за алгоритмом прискореного обчислення елементів V_k^+-послідовності [7], реалізованому на основі відомого бінарного методу піднесення до степеня [1].

Розробка принципів побудови спеціалізованих процесорів розподілу секретних ключів

Для реалізації поданого методу розподілу секретних ключів необхідні процедури для обчислення за модулем p елементів $v_{n+i,k}$, $i=\overline{-(k-1),k-2}$, а також елементів $u_{n-i,k}$, $i=\overline{0,k-1}$, та $u_{n+m,k}$. Всі ці обчислення пропонується здійснювати на одному універсальному пристрої обчислення елементів V_k^+- та U_k-послідовностей, роботу якого організуємо в п'яти режимах. В першому режимі будемо здійснювати обчислення елементів $v_{n+i,k}$, $i=\overline{-2k+1,k-2}$, для додатних значень n, а в другому — обчислення елементів $v_{n+i,k}$, $i=\overline{-k,k-2}$, для від'ємних значень n. Третій, четвертий та п'ятий режими роботи пристрою будуть забезпечувати, відповідно, обчислення елементів $u_{n-i,k}$, $i=\overline{0,k-1}$, за формулою (5), $u_{n+m-i,k}$, $i=\overline{0,k-1}$, за формулою (4) та $u_{n-m-i,k}$, $i=\overline{0,k-1}$.

Не важко помітити, що згідно з поданим методом Користувач A та Користувач B виконують однакові операції. Тому реалізацію розподілу секретних ключів як з боку одного користувача, так і з боку другого, пропонується здійснювати на процесорі, схема якого показана на рисунку.



Структурна схема процесора для розподілу секретних ключів

Процесор містить: генератор випадкових чисел ГВЧ; пристрій обчислення елементів V_k^+- та U_k-послідовностей Пр.VU; блоки пам'яті ПМ 1, ПМ 2, призначені для зберігання, відповідно, елементів $v_{0+i,k}$, $i=\overline{-(k-1),0}$, та коефіцієнтів рекурентної залежності g_i, $i=\overline{1,k}$; блок пам'яті ПМ 3, призначений для зберігання Користувачем A елементів $u_{b-i,k}$, $i=\overline{0,k-1}$, та елементів $u_{a-i,k}$,

$i=\overline{0,k-1}$ 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. VU.

Далі здійснюється робота пристрою Пр. VU в першому режимі, після чого на вхід пристрою подаються дані з блока пам'яті ПМ 2, і в третьому режимі обчислюються за модулем p елементи $u_{a-i,k}$, $i=\overline{0,k-1}$, які передаються Користувачу B.

Потім з блока пам'яті ПМ 3 на вхід пристрою Пр. VU подаються елементи $u_{b-i,k}$, $i=\overline{0,k-1}$, прийняті від Користувача B, і в четвертому режимі роботи пристрою Пр. VU обчислюється елемент $u_{b+a,k}$ за модулем p як результат секретного ключа, що отримується на виході процесора.

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

В результаті дослідження встановлено, що час обчислення елементів V_k^+-послідовності в першому і другому режимах його роботи дорівнює

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

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; а час обчислення елементів U_k-послідовності в третьому, четвертому і п'ятому режимах дорівнює

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

Оскільки в сучасних криптосистемах оперують з числами 1024 або 4096 розрядів, тобто Hq приймає саме такі значення, то оцінкою обчислення елементів $u_{n,k}$ можна знехтувати. Враховуючи це, час обчислень кожним з користувачів на процесорі, показаному на рисунку, буде дорівнювати

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

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

За основу порівняння візьмемо за аналог відомий метод Діффі–Хеллмана. Основною операцією, що виконується в методі Діффі–Хеллмана, є піднесення до степеня за модулем. Ця операція може здійснюватись за методом Монтгомері [1], який має меншу складність обчислень, ніж відомий бінарний метод [1]. Метод піднесення до степеня за Монтгомері оснований на множенні за методом Монтгомері. Виходячи з цього, пристрій піднесення до степеня за Монтгомері можна побудувати на основі пристрою множення за Монтгомері, який використовується в процесорі, що реалізує запропонований метод розподілу секретних ключів.

Час виконання піднесення до степеня за модулем відповідним пристроєм буде дорівнювати

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

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

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

Аналіз отриманих оцінок показує, що час розподілу секретних ключів на процесорах, що реалізують відомий метод Діффі–Хеллмана, є меншим, ніж на процесорах, що реалізують запропонований метод на основі рекурентних V_k^+- та U_k-послідовностей, причому навіть для $k=2$ це майже у 1,5 рази. Однак, по-перше, розроблені процесори реалізують метод, який є більш криптографічно

стійким, ніж відомий метод. По-друге, розробка наведеного процесора зумовлена необхідністю використання в криптографічних системах разом з іншими спеціалізованими процесорами, що розв'язують різні криптографічні задачі на єдиному математичному апараті рекурентних V_k - та U_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.

І, по-третє, можливо найважливіше, що у більшості випадків в криптографічних системах є можливість обчислювати сеансовий ключ — випадкове число a чи b заздалегідь до безпосереднього процесу ключового обміну. Тоді обчислення елементів $v_{n+i,k}$, $i=\overline{-2k+1,k-2}$ з боку кожного користувача також може здійснюватись заздалегідь і зберігатись в блоках пам'яті пристрою Пр. VU до безпосереднього початку процесу ключового обміну. В такому випадку час роботи запропонованого процесора буде значно меншим (на порядки) оскільки за таких умов обчислення будуть проводитись лише за формулою (4) елемента $u_{b+a,k}$ або $u_{a+b,k}$, тобто час роботи буде дорівнювати приблизно $2(k-1)\cdot T_{\text{мн.Монт.}}$, що в декілька десятків разів менше, ніж за відомим метод Діффі–Хеллмана, коли необхідно виконувати піднесення до степеня великого числа і час роботи процесора в цьому випадку буде дорівнювати $2\left(Hq+1\right)\cdot T_{\text{мн. Монт.}}$.

Висновки

Таким чином, на основі математичного апарата рекурентних V_k^+ - та U_k-послідовностей розглянуто метод розподілу секретних ключів та розроблено спеціалізовані процесори, які його реалізують.

Проведено дослідження часу роботи розроблених процесорів. Дослідження показало, що в цілому час розподілу секретних ключів на процесорах, що реалізують відомий метод Діффі–Хеллмана, є меншим, ніж на розроблених процесорах. Однак, у разі можливості в криптографічних системах здійснювати виконання обчислень сеансового ключа — випадкового числа заздалегідь, час роботи розроблених спеціалізованих процесорів буде в десятки разів меншим.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

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. — No 22, — P. 644—654.

3. Smith P. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms / P. Smith and C. Skinner // In Advances in Cryptology Asiacrypt '94, Springer-Verlag. — 1995. — P. 357—364.

4. Bleichenbacher D. Some remarks on Lucas-based cryptosystems / D. Bleichenbacher, W. Bosma, and A. Lenstra // In Advances in Cryptology Crypto '95, Springer-Verlag. — 1995. — P. 386—396.

5. Smart N. The Discrete Problem on Elliptic Curves of Trace One / N. Smart // Journal of Cryptology. — 1999. — No 12. P. 29—34.

6. Ростовцев А. Г. Подпись и шифрование на эллиптической кривой: анализ безопасности и безопасная реализация / А. Г. Ростовцев, Е. Б. Маховенко // Проблемы информационной безопасности. Компьютерные системы. — 2003. — № 1. — С. 64—73.

7. Яремчук Ю. Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем / Ю. Є. Яремчук // Захист інформації. — 2012. — № 4. — С. 120—127.

Рекомендована кафедрою комп'ютерних наук

Стаття надійшла до редакції 11.02.13
Рекомендована до друку 20.02.13

Яремчук Юрій Євгенович — професор кафедри адміністративного та інформаційного менеджменту.
Вінницький національний технічний університет, Вінниця