3. Калашников И. Д., Степанов В. С., Чуркин А. В. Адаптивные системы сбора и передачи информации. – М.,1975.
4. Ю. Василик, О. Івахів. Порівняння альтернативних принципів організації абонентського пункту вимірювально-обчислювальної мережі // Вісник ДУ"Львівська політехніка". – 1994. – №283. – С. 66 – 74.
5. Базилевич О., Голдак А., Івахів О., Серкіз А. Дослідження доцільності проектування адаптивної вимірювальної системи // Тези доповідей VI Міжнародної науково-технічної конференції "Контроль і управління в складних системах"(КУСС-2001), Вінниця, 8-12 жовтня 2001 року. – С. 252.

О. Ліскевич, М. Яцимірський*
Національний університет "Львівська політехніка"
*Центр математичного моделювання ІППММ ім. Я.С. Підстригача НАН України

УДК 621.372.542:517.519:510.52

ПРОСТОРОВО-ПАРАЛЕЛЬНІ СТРУКТУРИ АПАРАТНОГО ШИФРУВАННЯ ДАНИХ

Проаналізовано структурні особливості алгоритмів симетричного шифрування даних. Запропоновано новий підхід до побудови просторово-паралельних криптографічних алгоритмів. На його основі розроблено структуру матричного криптопроцесора. Показано можливість досягнення вищої, порівняно з відомими алгоритмами, продуктивності та надійності шифрування даних.

Structural peculiarities of symmetric cryptoalgorithms have been investigated. The new approach to parallel cryptoalgorithms development is proposed. SIMD matrix processor based on the proposed approach is developed. Possibility of cipher reliability and system throughput improvement, comparative to known algorithms, is shown.

1. Вступ

Інформаційні ресурси в наш час не поступаються за вартістю таким традиційним цінностям, як енергія чи сировина. Відповідно гостро стоять задачі захисту інформації [1, 2, 3]. Серед сучасних методів захисту інформації важливе місце посідають криптографічні алгоритми, що поділяються на симетричні та асиметричні [1]. В симетричних криптосистемах один і той же ключ використовується для шифрування та дешифрування. Асиметричні системи використовують два різні ключі. Сучасні системи захисту інформації часто поєднують обидва підходи, наприклад, асиметричні алгоритми для розповсюдження ключів та симетричні – для безпосереднього шифрування даних

[1]. Останнє зумовлено, в першу чергу, перевагою симетричних алгоритмів у швидкодії. Існування широкого кола симетричних алгоритмів створює потребу їх стандартизації, аналізу надійності та ефективності. Кількість асиметричних алгоритмів, що застосовуються на практиці, є значно меншою.

Стрімке зростання обчислювальних потужностей, розвиток методів паралельного криптоаналізу за участі тисяч ПК, об'єднаних глобальною мережею, робить вразливими алгоритми, надійність яких тривалий час не підлягала сумніву. Водночас об'єми даних, що підлягають шифруванню, постійно зростають, піднімаючи вимоги до продуктивності криптосистем. З огляду на це актуальною є задача розробки нових алгоритмів, що відповідали б сучасним вимогам до продуктивності та надійності шифрування.

У даній роботі запропоновано новий підхід до побудови алгоритмів шифрування, орієнтованих на апаратну просторово-паралельну реалізацію. Він ґрунтується на застосуванні обчислювальних структур, що відповідають графам алгоритмів швидких тригонометричних перетворень. Тут базова операція алгоритму відіграє роль шифруючого або дешифруючого елементу.

2. Схема Файстеля

Переважна більшість сучасних алгоритмів симетричного шифрування базується на структурі блочного шифру Файстеля [2, 3]. Класичний шифр Файстеля складається з декількох етапів, на кожному з котрих виконуються операції підстановки та перестановки.

Структура, запропонована Файстелем, наведена на рис. 1. На вхід алгоритму подається блок вхідного тексту розміром N біт та ключ K. Вхідний текст розбивається на дві рівні частини R_0 та L_0, над якими послідовно виконується m етапів шифрування. При цьому для i-го етапу вхідними даними є R_{i-1} та L_{i-1}, отримані на попередньому етапі та підключ K_i, що обчислюється на основі K. На всіх етапах шифрування виконуються одні й ті ж самі операції (1).

$$\begin{cases} K_i = \varphi(K), \\ L_i = R_{i-1}, \\ R_i = F(R_{i-1}, K_i) \text{ xor } L_{i-1}, \end{cases} \tag{1}$$

де φ – функція обчислення підключа, F – функція етапу, xor – операція додавання за модулем два .

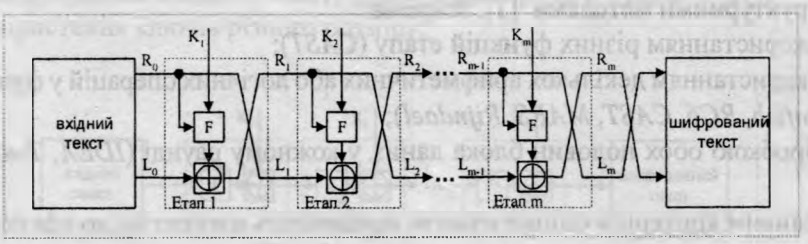

Рис. 1 Структура блочного шифру Файстеля

Загалом ефективність реалізації схеми Файстеля визначається такими характеристиками:

- розміром блока;
- розміром ключа;
- числом послідовних етапів обробки;
- алгоритмом обчислення значень підключів;
- видом функції етапу;
- обчислювальними затратами шифрування/дешифрування [3].

Надійність шифру при цьому визначається першими п'ятьма параметрами. Підвищення надійності, як правило, досягається за рахунок ускладнення алгоритму.

З тими чи іншими модифікаціями, схема Файстеля охоплює більшість симетричних алгоритмів шифрування, що застосовуються на практиці (*DES*, *IDEA*, *Twofish*, *RC5*, *RC6*, *MARS*, *CAST*) [1].

3. Сучасні модифікації схеми Файстеля

Найпопулярніша з сучасних схем шифрування базується на алгоритмі *DES*, що був державним стандартом США у 1977 – 2000 рр. та фактичним світовим стандартом шифрування комерційних даних. Однак зростання обчислювальних потужностей призвело до можливості криптоаналізу *DES* шляхом простого перебору ключів. Недостатню надійність 56-розрядного ключа *DES* було практично доведено в 1997 р. [1]. Окрім того, *DES* шифрування є обчислювально складною операцією. Постійно зростаючі обсяги інформації, що підлягає шифруванню, вимагають розробки нових алгоритмів з вищою продуктивністю.

Альтернативою традиційному *DES* може бути послідовне багатократне шифрування *DES* із використанням декількох ключів ("подвійний" та "потрійний" *DES*). Такий підхід забезпечує сумісність з існуючими програмними та апаратними реалізаціями *DES*, проте характеризується підвищеною обчислювальною складністю [1].

Іншим варіантом заміни стандарту може стати один з відомих алгоритмів, створених після розробки *DES*. Крім підвищеної надійності, привабливими виглядають також деякі специфічні характеристики, закладені розробниками. Зокрема сучасні алгоритми реалізують шифрування із змінним ступенем захисту [1, 6]. Цього може бути досягнуто за рахунок:

– змінної довжини ключа (*Twofish*, *RC6*, *Rijndael*, *MARS*);

– змінного розміру блока відкритого/шифрованого тексту (*RC6*, *Rijndael*);

– змінного числа етапів обробки (*RC6*, *Rijndael*).

Окрім збільшення довжини блока тексту та ключа, підвищення надійності досягається структурними методами [1], зокрема:

– використанням різних функцій етапу (*CAST*);

– використанням декількох арифметичних або логічних операцій у функції етапу (*IDEA*, *Twofish*, *RC6*, *CAST*, *MARS*, *Rijndael*);

– обробкою обох половин блока даних у кожному раунді (*IDEA*, *Twofish*, *RC6*, *Rijndael*).

Важливим критерієм оцінки є також придатність алгоритму до ефективної реалізації на сучасних апаратних та програмних засобах. Наприклад, в алгоритмах *Twofish*

та *Rijndael* закладено можливість паралельної реалізації із значним ступенем паралелізму. Більшість алгоритмів використовують лише елементарні обчислювальні операції, що апаратно реалізовані в мікропроцесорах. *RC6*, окрім цього, може працювати із словами довільної довжини, адаптуючись до розрядності конкретного мікропроцесора. Відомі алгоритми з низькими вимогами до об'єму пам'яті. Зокрема *Twofish*, *Rijndael* та *Serpent* можуть виконуватись в системах з пам'яттю менше одного кілобайта. Це дає можливість реалізації надійного шифрування у кишенькових комп'ютерах та смарт-картках [1].

Завдяки високій надійності та продуктивності шифрування, офіційним наступником *DES* став алгоритм *Rijndael*, що був затверджений державним стандартом США (*AES - Advanced Encryption standard*) у 2001 р. Серед 15 кандидатів на звання стандарту *AES* дев'ять алгоритмів базувалось на схемі Файстеля, чотири алгоритми – на підстановках та перестановках, та два – на інших принципах побудови [6]. Варто зазначити, що навіть алгоритми, не побудовані на основі схеми Файстеля, значною мірою використовують ідеї, закладені в її основу. Наприклад, алгоритм *Rijndael* зазвичай відносять до класу алгоритмів на основі підстановок та перестановок з архітектурою "квадрат". Однак, структура алгоритму може бути подана такою схемою (рис. 2). Як видно із схеми, даний алгоритм можемо розглядати як варіант схеми Файстеля з одночасною обробкою обох половин блока (фактично без поділу на половини) та функцією F, що не залежить від ключа K_i.

4. Просторово-паралельне шифрування даних

Апаратна реалізація алгоритмів шифрування можлива на основі спеціалізованих інтегральних схем або з використанням компонентів широкого застосування (наприклад, процесорів обробки сигналів). Використання спеціалізованих НВІС дозволяє досягнути вищої продуктивності та є більш доцільним, оскільки криптопроцесори в наш час стали продуктами масового виробництва.

Структурна схема спеціалізованого конвеєрного криптопроцесора, що реалізує схему Файстеля, наведена на рис 3. Тут $ПЕ_1$-$ПЕ_m$ – процесорні елементи, що реалізують функцію етапу алгоритму. Для охоплення процесором всіх алгоритмів класичної схеми Файстеля ПЕ повинні програмуватись на виконання різних видів функції етапу. Крім цього, потрібно забезпечити можливість програмування алгоритму обчислення підключів.

Для охоплення алгоритмів, що є модифікаціями схеми Файстеля, потрібно додатково забезпечити можливість:

– обробки блоків вхідного тексту різного розміру (64, 128, 256 біт);
– використання ключів різного розміру;

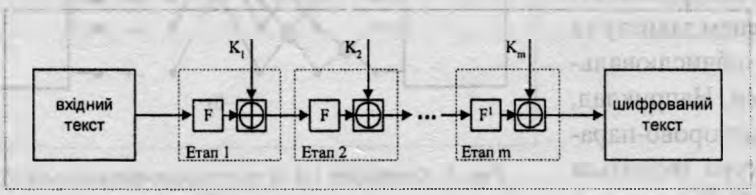

Рис. 2. Структура шифру Rijndael (AES)

Рис. 3. Структура конвеєрного криптопроцесора на основі схеми Файстеля

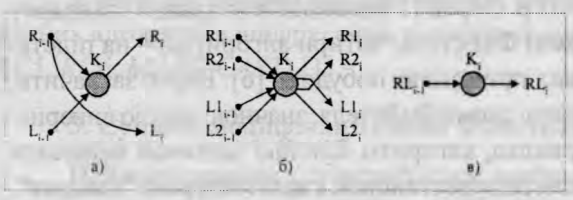

Рис. 4. Базові операції алгоритмів Файстеля (а), IDEA (б), AES (в)

– реалізації змінного числа етапів обробки (до 16, в окремих випадках – до 20);

– перепрограмування системи зв'язків між ПЕ;

Зрозуміло, що в останньому випадку побудова системи на базі НВІС вимагатиме невиправдано високих апаратних затрат. Альтернативою може бути використання технології програмованих логічних інтегральних схем (ПЛІС).

Аналіз схеми на рис. 3 дозволяє зауважити, що апаратні реалізації алгоритмів шифрування практично повністю повторюють структуру алгоритмів швидких тригонометричних перетворень (ШТП) [5, 7]. Так, схема на рис. 3 є варіантом запропонованої в [7] реалізації універсального алгоритму швидких тригонометричних перетворень (УАШТП) із спрощеною передачею даних між ПЕ та базовою операцією (БО), виду (1). Відомо, що ШТП та їх реалізації є одними з найкраще досліджених алгоритмів сучасної обчислювальної техніки. Отже, доцільним є використання досвіду, набутого при дослідженні ШТП для побудови ефективних систем моделювання та реалізації алгоритмів симетричного шифрування.

Розглянемо реалізацію схеми Файстеля на основі схеми УАШТП. Побудова матричного процесора потребуватиме k ПЕ, що реалізуватимуть БО алгоритму. Тут

$$k = mn,$$

де m – кількість етапів алгоритму, n – кількість ПЕ на кожному етапі. Використання елементів сортувальної пам'яті [7] дозволяє змінювати значення n та m, тобто реалізувати шифрування із змінним ступенем захисту та апаратними і обчислювальними затратами. Наприклад, при $n = 1$ просторово-паралельна структура зводиться до потокової [7]. Паралельна

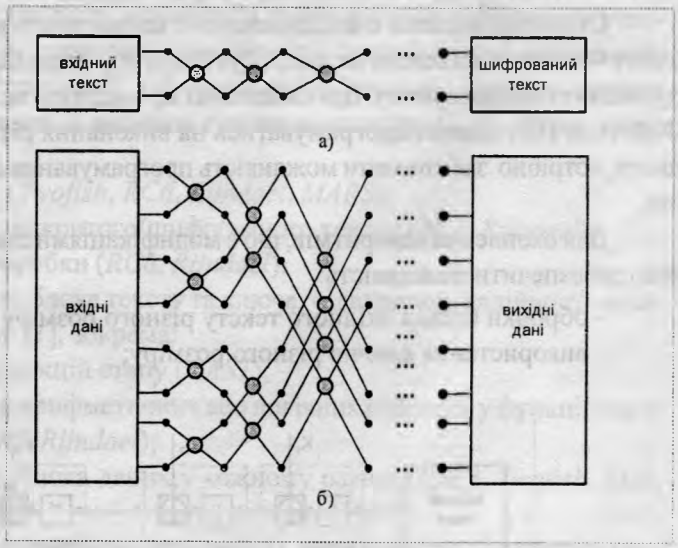

Рис. 5. Конвеєрна (а) та просторово-паралельна (б) структури шифрування даних

обробка *n* блоків даних дозволяє отримати реалізацію алгоритму із ефективнішою функцією дифузії [1] або досягнути заданого рівня дифузії за меншу кількість етапів обробки.

На рис. 4, а наведено базову операцію для шифру Файстеля. На рис. 4, б та 4, в наведено БО алгоритмів *IDEA* та *AES*, що є структурно найбільш віддаленими від класичної схеми Файстеля [1, 6]. Так, *IDEA* передбачає чотириточкову БО, *AES* – одноточкову, з двовимірною функцією етапу. Відповідно реалізація алгоритмів різниться лише видом функції етапу, організацією передачі даних між ПЕ та будовою вузла формування підключів. Порівняння конвеєрної (а) та просторово-паралельної (б) структур шифрування даних наведено на рис.5.

Отже, за умови вибору належної БО, структура УАШТП охоплює практично усі сучасні алгоритми шифрування. Це значно спрощує розробку нових алгоритмів, оскільки синтез алгоритму зводиться до пошуку оптимальної БО та схеми передачі даних між етапами. За умови використання асиметричної базової операції даний підхід може застосовуватись і для розробки асиметричних криптоалгоритмів.

5. Висновки

Розроблений метод побудови алгоритмів шифрування дозволяє підвищити надійність та продуктивність відомих криптографічних алгоритмів без збільшення їх обчислювальної складності. Крім цього, метод дозволяє будувати нові алгоритми з покращеними характеристиками. Покращення може досягатись за рахунок вибору розміру блоку даних, розміру ключа, впровадження нових базових операцій (зокрема асиметричних) та зміни схем міжетапної передачі даних.

1. Столлингс В.. Криптография и защита сетей: принципы и практика. – 2-е изд. – М.: Издательский дом "Вильямс", 2001. – 672 с.
2. Шеннон К. Работы по теории информации и кибернетике. – М., ИЛ, 1963. – С. 333 – 369.
3. H. Feistel. Cryptography and Computer Privacy, Scientific American, May 1973, Vol. 228, No. 5, pp. 15 – 23.
4. Винокуров А., Применко Э. Сравнение российского стандарта шифрования, алгоритма ГОСТ 28147-89, и алгоритма Rijndael, выбранного в качестве нового стандарта шифрования США // Системы безопасности. – М.; Гротэк. – 2001. – № 1,2.
5. Рабинер Л., Гоулд Б. Теория и применение цифровой обработки сигналов /Пер. с англ. А.Л.Зайцева, Э.Г.Назаренко, Н.Н.Тетекина; Под ред. Ю.Н.Александрова. – М.:Мир, 1978. – 848 с.
6. Federal Information Processing Standard FIPS-197. [веб-сервер]; http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf [23.01.2003].
7. Ліскевич О.І., Яцимірський М.М. Потоковий процесор швидких тригонометричних перетворень // Вісник Національного університету "Львівська політехніка". – 2001. – №433. – С. 22 – 27.