УДК

Мельник А.О., Коркішко Т.А.
ДУ "Львівська політехніка", кафедра ЕОМ

СИСТЕМА ПІДТРИМКИ ВИКОНАННЯ АЛГОРИТМІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ПРОГРАМОВАНОГО ПРОЦЕСОРА ТА КРИПТОГРАФІЧНИХ АКСЕЛЕРАТОРІВ

Проведено аналіз застосування технології процесорних ядер для побудови системи криптографічного захисту інформації. На основі проведеного аналізу вибрані перелік алгоритмів та структура системи криптографічного захисту інформації. Запропонований новий підхід до проектування надвеликої інтегральної схеми системи криптографічного захисту інформації на основі ядра програмованого процесора та декількох ядер криптографічних акселераторів, що характеризується гнучкістю та високою ефективністю.

Вступ. Успішний розвиток електронних комунікацій значною мірою залежить від можливості безпечного передавання інформації по незахищених каналах зв'язку, збереженні її в електронному вигляді на носіях різних типів. Для обмеження доступу на модифікацію, осмислене читання та фальсифікацію інформації використовуються системи криптографічного захисту інформації (КЗІ). Проектування цих систем має на меті забезпечення високого ступеня захисту інформації, продуктивності роботи, низької споживаної потужності. При цьому існують додаткові вимоги, такі як короткий термін розробки та простота модифікації чи заміни використовуваних алгоритмів (так звана алгоритмічна незалежність).

Пропонується будувати у вигляді надвеликої інтегральної схеми (НВІС) систему для підтримки виконання алгоритмів КЗІ на основі програмованого процесора (ПП) та декількох криптографічних акселераторів (КА). В цій системі як ПП може використовуватись процесор із універсальною системою команд чи процесор із спеціалізованою системою команд. Гнучкість процесу проектування системи досягається інтеграцією у НВІС ПП. Як апаратні ядра пропонується використати КА – апаратні прискорювачі виконання часомістких операцій і алгоритмів КЗІ: модульної арифметики, алгоритмів симетричного і асиметричного шифрування, алгоритмів обчислення хеш-функції. Інтеграція КА як компонентів НВІС забезпечує досягнення високої продуктивності та низької споживаної потужності.

Складові операції алгоритмів КЗІ. Системи КЗІ призначені для вирішення основних підзадач захисту інформації – забезпечення конфіденційності, аутентифікації користувача, аутентифікації джерела даних, цілісності даних, неможливості зречення [1]. Дані підзадачі вирішуються за допомогою трьох алгоритмів: симетричне шифрування з таємним ключем, асиметричне шифрування із відкритим ключем, алгоритму хешування та їх комбінацій [2].

Кожен тип алгоритму КЗІ складається з досить обмеженого набору операцій. Однак є характерний набір операцій, що використовується для симетричних алгоритмів шифрування і хеш-функцій [1]:

- заміна вхідного елемента за таблицею – ця операція не є складною для універсальних ПП, однак виникають труднощі у випадках, коли розмір вхідних даних не вкладається у вигляді цілого числа разів у розмір слова (півслова) ПП;
- перестановка бітів у блоці даних – система команд універсальних ПП не містить команд для ефективного виконання таких операцій;
- додавання (віднімання), множення цілих беззнакових чисел за модулем 2^n – універсальні ПП мають команди для виконання таких операцій при $n = 2^i$, i=0,1,...,6. У випадку $n \neq 2^i$ для проведення обчислень необхідно використовувати більше команд;
- зсуви (у тому числі циклічні) вліво і вправо на фіксовану і змінну кількість розрядів – універсальні ПП мають команди для виконання цих операцій над даними, що поміщаються у внутрішні регістри;
- побітові логічні операції AND, NOT, OR, XOR;
- вибір з пам'яті слів змінної довжини.

Асиметричні алгоритми будуються на основі операцій модульної арифметики. Як операнди виступають беззнакові цілі числа, довжина розрядної сітки яких становить 256, 512, 1024, 2048 біт. Використовуються операції обчислення:

- модульного залишку $r = a \bmod m$;
- модульної суми $s = a+b \bmod m$;
- модульного добутку $s = ab \bmod m$;
- модульного піднесення до степеня $s = a^b \bmod m$;
- модульної мультиплікативної та адитивної інверсій.

За допомогою універсальних ПП можна ефективно проводити модульні обчислення лише для операндів із невеликою розрядною сіткою.

Тобто, при реалізації описаних алгоритмів на універсальних ПП для виконання деяких елементарних операцій необхідно виконати декілька команд процесора. Оскільки алгоритми КЗІ використовують досить велику кількість елементарних операцій та їх комбінацій при обробці одного блоку, то при обробці великої кількості блоків вхідних даних необхідні значні затрати процесорного часу. До найбільш часомістких операцій алгоритмів КЗІ при їх виконанні на ПП належать операції модульної арифметики над багаторозрядними числами, операції заміни, зсуву та перестановки.

Традиційні структури процесорів для систем КЗІ. Системи КЗІ, що вимагають високої продуктивності роботи, традиційно мають у своєму складі спеціалізовані НВІС процесорів криптографічного перетворення інформації (ПКП), архітектура яких орієнтована на виконуваний алгоритм [3, 4]. Вона містить спеціалізований тракт обробки даних, як правило конвеєрний, який апаратно відображає структуру виконуваного алгоритму. Оскільки алгоритми криптографічного перетворення працюють з досить малою порцією інформації, то ПКП не містить великого об'єму пам'яті для оброблюваних даних, хоча присутня пам'ять для зберігання ключової інформації. Блок управління ПКП керує потоком даних та забезпечує сигналами керування внутрішні вузли. Завдяки такій структурній спеціалізації досягається висока продуктивність процесора та мала споживана потужність.

Іншим типом процесорів, що можуть використовуватися в системах КЗІ, є стандартні універсальні ПП та ПП обробки сигналів. Оскільки архітектура таких процесорів не пристосована для виконання спеціальних операцій, що зустрічаються у задачах КЗІ, то їх застосування обмежується задачами, у яких є досить низька швидкість надходження вхідних даних.

Застосування технології процесорних ядер для побудови систем КЗІ Розглянемо можливість застосування технології процесорних ядер для побудови систем КЗІ. У рамках цього підходу для побудови систем обробки інформації передбачається використання ядер програмованих та апаратно-орієнтованих процесорів. Запропонований підхід для створення нарощуваних параметризованих ядер [5] не може бути прямо використаний при побудові систем КЗІ, оскільки в задачах КЗІ характерним є використання стандартизованих алгоритмів обробки, структури і параметри яких не можуть бути змінені із міркувань захищеності інформації. Крім цього, кожна держава має свої власні стандарти на алгоритми КЗІ. Створення ядра апаратно-орієнтованого ПКП, який може виконувати декілька стандартних алгоритмів для різних держав, є недоцільним, оскільки буде неефективно використовуватись апаратура і понизиться продуктивність порівняно із спеціалізованими процесорами, орієнтованими на виконання одного алгоритму.

Виходячи з цього, доцільним є використання кількох ядер апаратно-орієнтованих процесорів – криптографічних акселераторів та одного ПП. На КА покладається задача виконання найбільш часомістких операцій та алгоритмів КЗІ: алгоритми симетричного шифрування, обчислення хеш-функцій, операції модульної арифметики. При цьому параметризації піддається акселератор для модульної арифметики, оскільки не відоме строге математичне доведення безпеки алгоритмів КЗІ, що використовують модульні операції піднесення до степеня [6, 7, 8] та інші модульні операції. Тому для споживача такого акселератора важливою є можливість нарощування розрядності опрацьовуваних чисел для компенсації розвитку досліджень у галузі ламання асиметричних алгоритмів.

У загальному випадку побудови КА для реалізації симетричних алгоритмів шифрування їх можна параметризувати. Однак при цьому для кожного вектора параметрів алгоритму, що відрізняються від прийнятих за стандарт, необхідно аналізувати рівняння перетворення даних при шифруванні на предмет їх стійкості до різного виду атак. Тобто, при побудові параметризованих ядер симетричного шифрування інформації необхідно проводити додатковий аналіз щодо стійкості отриманих алгоритмів.

Стосовно хеш-функцій, то, як правило, в своїй основі вони містять алгоритми симетричного шифрування [9, 10], тому на базі наведених вище міркувань приймаємо, що акселератори обчислення хеш-функцій не параметризуються.

Структура пропонованої системи КЗІ. У загальному випадку структура системи КЗІ не повинна бути прив'язаною до типу використовуваних алгоритмів. Тому необхідно забезпечити легкий перехід від одного набору алгоритмів до іншого без особливих змін структури системи. Такий перехід можна робити при умові використання однотипових інтерфейсів складових блоків та однієї парадигми проектування системи в цілому.

Авторами пропонується будувати систему КЗІ із використанням ПП та декількох КА. Можливості вибору типу ПП а також параметризації деяких з акселераторів є суттєвою перевагою такої системи порівняно з існуючими НВІС для виконання алгоритмів КЗІ із строго визначеними параметрами [11, 12].

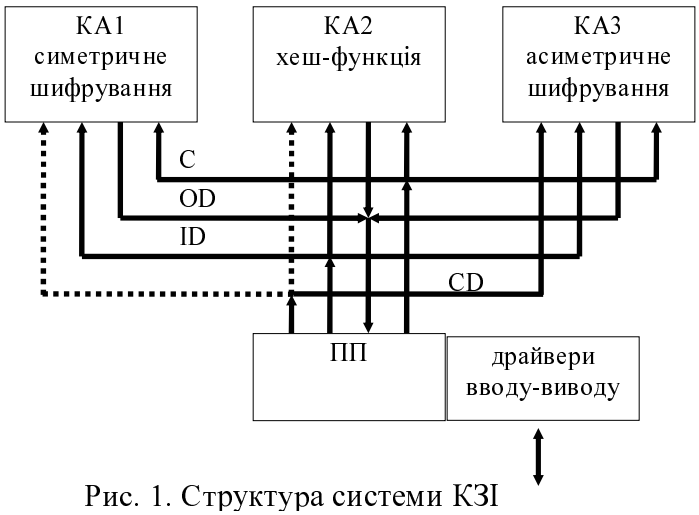

Рис. 1. Структура системи КЗІ

Структура системи КЗІ (рис. 1) містить ПП та криптографічні акселератори КА1, ... КА3, які реалізують відповідно алгоритми симетричного шифрування, хеш-функції, асиметричного шифрування. Пам'ять для зберігання ключової інформації, генератор випадкових чисел на рисунку не показані. Елементи системи з'єднані відповідними шинами: C – шина керуючих сигналів, OD – вихідні дані, ID – вхідні дані, CD – дані конфігурування.

Склад керуючих сигналів – це тактові імпульси та сигнали підтримки протоколу обміну даними.

Оскільки набір алгоритмів для системи КЗІ визначається стандартами, прийнятими в конкретній державі, то за допомогою КА передбачається реалізувати такий набір криптографічних перетворень: симетричного шифрування – ГОСТ28147-89, асиметричного шифрування – ГОСТ34.310-95, хеш-функції – ГОСТ34.311-95. Для спеціальних використань деякі із КА можуть не використовуватись.

При заміні алгоритмів роботи КА необхідно буде відповідним чином відкоригувати програмне забезпечення ПП. Таким чином досягається алгоритмічна незалежність системи.

Функції керування системою КЗІ, інтерфейсні функції, керування ключами та інші додаткові процедури КЗІ виконуються ПП. Вибір типу ПП залежить від того, які додаткові процедури будуть виконуватися системою КЗІ. Це може бути як простий цифровий автомат, так і процесор із спеціалізованою системою команд.

Висновки. В роботі проведений аналіз застосування технології процесорних ядер для побудови системи КЗІ. Виділені особливості складових операцій алгоритмів КЗІ, особливості параметризації алгоритмів криптографічних перетворень та їх реалізації за допомогою програмованих та апаратно-орієнтованих процесорів. На основі проведеного аналізу вибрані перелік алгоритмів та структура системи КЗІ.

Запропонований підхід до проектування НВІС системи КЗІ на основі ядра ПП та декількох ядер КА характеризується гнучкістю та високою ефективністю. Завдяки використанню ПП та КА із уніфікованим інтерфейсом отримується система, що мало залежить від типу криптографічних алгоритмів. Інтеграція ПП як компоненти замовленої НВІС забезпечує її програмованість, а криптографічних акселераторів – високу продуктивність роботи та низьку споживану потужність.

1. A.Menezes. Handbook of Applied Cryptography. CRC Press. 1996. 2. A Certicom Whitepaper. An Introduction to Information Security. The first in a series of ECC whitepapers. March 1997. 3. Пичуев А.В., Рябченко А.Г., Титов Д.Г., Фролов С.А. О проектировании СБИС высокоскоростного криптопроцессора. Автометрия, 1994. №6. С.91-97. 4. Jens-Peter Kaps. High Speed FPGA Architectures for the Data Encryption Standard. Magister thesis, Worcester Polytechnic Institute, May 1998. 5. Мельник А.О., Аль-Кхатіб А. Концепція побудови

нарощуваних параметризованих процесорних ядер спеціалізованих надвеликих інтегральних схем // Вісн. ДУ "Львівська політехніка". №350. С.44 – 47. 6. R.L. Rivest, A. Shamir, and L.M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2): 120-126, February 1978. 7. T. El Gamal. A Public Key Cryptosystem and a Signature System Based in Discrete Logarithms. IEEE Trans. on Information Theory. V.IT-31, no.4, pp.469-472, July 1985. 8. Информационная технология. Криптографическая защита информации. Процедуры проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма ГОСТ34.310-95, М., 1995. 9. Информационная технология. Криптографическая защита информации. Функция хеширования ГОСТ34.311-95, М., 1995. 10. J.Daemen. Cipher and Hash Function Design. Strategies Based on Linear and Differention Cryptanalysis. Doctoral Dissertation, Katholieke Universiteit Leuven, 1995. 11. Hi-Fi, Inc. The 7711 Encryption Processor Data sheet. DS-0001-001, 1998. 12. VLSI Technology, Inc. The VMS115 Data Sheet, 1999. 13. Системы обработки информа ции. Защита криптографическая. Алгоритм криптографического преобразования. ГОСТ 28147–89, М., 1989.

УДК 621.382

Мельник Р.А., Масько Д.В.
ДУ “Львівська політехніка”, кафедра ПЗ

ДЕКОМПОЗИЦІЙНИЙ АЛГОРИТМ ПОБУДОВИ МІНІМАЛЬНИХ ЗВ’ЯЗУВАЛЬНИХ ДЕРЕВ

Розглянуто декомпозиційний алгоритм побудови мінімального зв’язуючого дерева, що базується на методі побудови дерева оптимального згортання. Використано поняття нечіткого з’єднання між блоками (кластерами) та окремими точками на площині.

Вступ. Відсутність достатньо ефективних алгоритмів побудови МЗД [1] є причиною використання декомпозиційного підходу, який базується на факті, що для двох-трьох контактів ланцюга (назвемо їх елементами) точний розв’язок завжди може бути знайдений. Розглянемо метод, який дозволяє отримати близьке до оптимального МЗД і який базується на оптимальному згортанні цих елементів у нечіткі кластери (блоки) [2].

Стратегії та критерії згортання. За блок певного рівня приймаємо сукупність елементів, об’єднаних у вершинах дерева згортання в процесі його побудови. На площині (ДТРП) цьому блоку відповідає прямокутна область, яка охоплює елементи, що попадають у кластер в процесі об’єднання. Найнижчий рівень дерева відповідає елементам множини I, тобто контактам. В процесі побудови дерева згортання об’єднання вершин дерева відповідає трьом типам реального об’єднання на площині, а саме: “елемент-елемент”, “блок-елемент” і “блок-блок”. Критерієм для вибору найкращих пар вершин дерева $T_з$ для згортання є мінімальна віддаль між ними у ортогональній метриці, тобто

$$F_{ij} = \min_{i,j \in I} L\,(i,j),$$