УДК 681.3

ПРОБЛЕМИ І ТЕНДЕНЦІЇ РОЗВИТКУ АПАРАТНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

Анатолій Мельник, Юрій Морозов, Віктор Мельник, Тимур Коркішко
ТзОВ "Інтрон"

Анотація: **В доповіді розглядаються сучасні апаратні засоби реалізації криптографічних алгоритмів, криптографічних функцій та криптографічних протоколів, їх параметри та напрямки розвитку.**

Summary: **hardware for realization of modern cryptographic algorithms, functions and protocols, their parameters and development directions are considered in report.**

Ключові слова: **захист інформації, апаратні засоби, криптографічні алгоритми, функції та протоколи.**

I. Вступ

Засоби захисту інформації реалізують алгоритмічні перетворення з метою забезпечення приватності або конфіденційності, цілісності даних, аутентифікації та неможливості зречення [1] та виготовляються у вигляді окремих закінчених продуктів. На сьогодні основна увага розробників систем захисту інформації приділяється програмним засобам, основними недоліками яких є недостатня стійкість до зламу, часто недостатня продуктивність, особливо при обробці інтенсивних потоків даних. Цих недоліків позбавлені апаратні засоби захисту інформації. Апаратні засоби захисту інформації можна поділити в порядку нарощення функціональності на засоби виконання криптографічних алгоритмів, засоби виконання криптографічних функцій та засоби виконання криптографічних протоколів. Метою даної роботи є окреслення проблем та тенденцій розвитку цих засобів захисту інформації.

II. Апаратні засоби виконання криптографічних алгоритмів

Для розв'язання задач захисту інформації, на практиці використовують достатньо вузький перелік алгоритмів перетворення інформації. Як за рубежем, так і в Україні запроваджено відповідні стандарти на алгоритми захисту інформації. До переліку алгоритмів входять алгоритми симетричного шифрування та алгоритми обчислення хеш-функцій. Додатково визначаються процедури цифрового підпису, основані на асиметричних алгоритмах шифрування. До переліку широко вживаних алгоритмів симетричного шифрування входять: ГОСТ28147-89 [2], DES [3], IDEA [4], AES [5], RC5 [6], CAST [7], BLOWFISH [8] тощо. До переліку широко вживаних алгоритмів обчислення хеш-функцій входять: ГОСТ Р 34.11–94 [9], SHA-1 [10], MD4 [11], MD5 [12]. Процедури цифрового підпису базуються на алгоритмах модульних операцій – додавання, віднімання, множення, піднесення до степеня, обчислення обернених елементів над числами великої розрядності [13 – 15].

В сучасних системах захисту інформації перелічені алгоритми традиційно реалізуються на базі універсальних програмованих процесорів [16]. При цьому забезпечується висока гнучкість систем, простота налаштування та експлуатації, однак в силу структурних особливостей універсальних програмованих процесорів важко досягти високих рівнів продуктивності, особливо при обробці даних, які надходять з одного чи декількох високошвидкісних каналів. Ситуація дещо покращується при використанні програмованих процесорів із спеціалізованою чи доповненою системами команд, де частина обчислень за алгоритмами виконується у спеціалізованих операційних пристроях [17]. Однак, внаслідок ітераційного виконання алгоритмів тут також важко досягти високих швидкісних показників.

Суттєвий приріст продуктивності обробки даних досягається при використанні апаратно-орієнтованих процесорів для виконання криптографічних алгоритмів [18]. Тут операційний пристрій процесора орієнтований на виконання повного чи частини потокового графу криптографічного алгоритму, при цьому часто використовується конвеєрна організація обчислень, що дозволяє досягти максимальних рівнів продуктивності.

На рис.1 показана досягнута на сьогодні продуктивність апаратних засобів реалізації різних криптографічних алгоритмів при використанні різних типів процесорів.

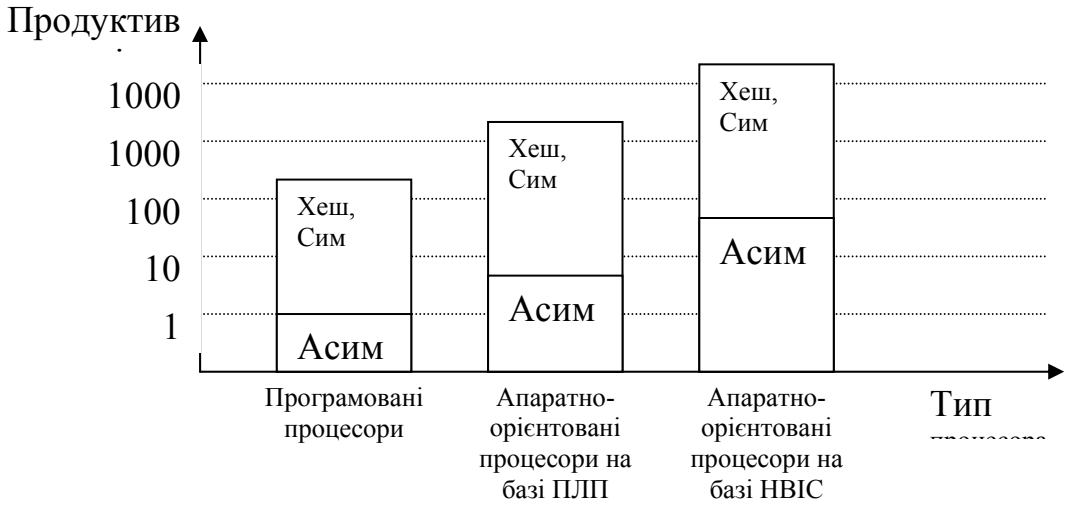

Рис. 1. Досягнуті рівні продуктивності виконання криптографічних алгоритмів на процесорах різної архітектури: Хеш – хеш-функції, Сим – симетричні шифри, Асим – асиметричні шифри.

Як видно з наведеної діаграми, найбільшу продуктивність обробки даних мають апаратно-орієнтовані процесори криптографічних алгоритмів.

III. Апаратні засоби виконання криптографічних функцій

Для захисту інформації у комп'ютерних системах та мережах використовують певний набір криптографічних функцій. До криптографічних функцій належать аутентифікація, шифрування, цифровий підпис, керування ключами.

При аутентифікації повідомлень можна виділити два основних рівні. На нижньому рівні виконується операція, що породжує аутентифікатор – значення, яке використовується для аутентифікації повідомлення. На верхньому рівні виконується операція, що перевіряє достовірність повідомлення виходячи із значення аутентифікатора. Для створення аутентифікатора використовуються алгоритми обчислення хеш-функцій - SHA-1, MD4, MD5, RIPEMD-160, ГОСТ Р 34.11–94, ін. Для перевірки аутентичності повідомлення використовується механізм аутентифікації повідомлень згідно алгоритму обчислення хеш-функції, який використовувався для створення ідентифікатора - HMAC-SHA-96, HMAC-MD-96, ін.

Шифрування реалізується з допомогою алгоритмів симетричного шифрування (ГОСТ28147-89, DES, IDEA, AES, RC5, CAST, BLOWFISH). Алгоритми симетричного шифрування зашифровують та розшифровують інформацію з використанням ключів шифрування, які є таємними.

Цифровий підпис реалізується з допомогою стандартів США FIPS PUB 186-2 (DSS) та стандарту ГОСТ Р 34.10-94. DSS передбачає використання в якості хеш-функції функцію, визначену стандартом SHS (алгоритм SHA-1). Для реалізації криптосистеми з відкритими ключами в американському стандарті передбачено три варіанти: використання алгоритму цифрового підпису DSA, що є варіантом алгоритмів цифрового підпису Schnorr та ElGamal, використання алгоритму RSA, використання математичного апарату еліптичних кривих для реалізації алгоритму DSA (ECDSA). Алгоритми цифрового підпису є дуже складні для апаратної реалізації, тому найбільш часомісткі операції реалізуються на апаратно-орієнтованих процесорах, а інші операції пов'язані з реалізацією циклів, ітерацій та логічних переходів виконуються програмованим процесором. Апаратно алгоритми цифрового підпису до останнього часу реалізовувались на додаткових програмованих процесорах. В останній час з'явились спеціалізовані криптопроцесори, що реалізують алгоритми MD5, SHA-1, RSA, наприклад фірм Hi-Fn, Інтрон.

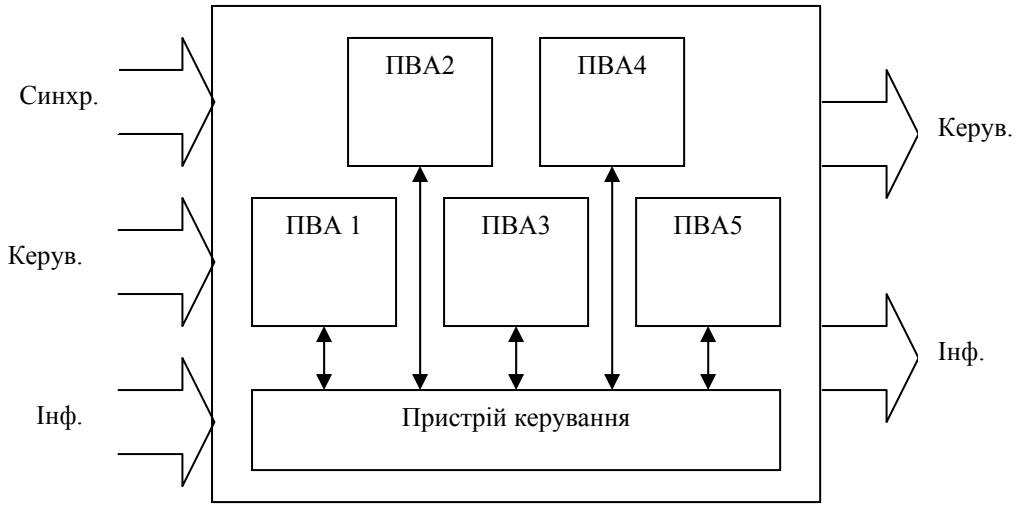

Рис.2. Структурна схема процесорів виконання криптографічних функцій: ПВА – пристрій виконання алгоритму.

Для задоволення потреб продуктивності апаратні засоби виконання криптографічних функцій реалізуються у вигляді набору апаратно-орієнтованих процесорів для виконання криптографічних алгоритмів. Як правило, процесори виконання криптографічних функцій можуть виконувати кілька алгоритмів (див. рис.2). Наприклад, процесори виконання функції аутентифікації виконують алгоритми SHA-1, MD4, MD5 та надають користувачеві можливість виконання операції обчислення хеш-функцій та операції перевірки аутентичності повідомлень згідно з цими алгоритмами. Процесори виконання функції шифрування виконують певний набір алгоритмів шифрування – DES, 3DES, AES та ін.

Керування ключами реалізується програмно на основі алгоритмів X.509v3 шляхом використання баз даних.

IV. Апаратні засоби виконання криптографічних протоколів

Як правило засоби захисту мережевих функцій вбудовані в усі сучасні операційні системи. Але таке рішення можна використовувати лише для захисту неконфіденційної інформації. Недоліки даних засобів широко відомі. Це шифрування з дуже короткими ключами (як правило 40 біт), використання слабких алгоритмів шифрування, генерація так званих слабких ключів і т.д. В зв'язку з цим широке розповсюдження отримали спеціалізовані програмні засоби, наприклад засоби фірми Check Point Software. Основними перевагами таких засобів є значна гнучкість, можливість легко нарощувати функціональність і виправляти помилки. Але є й значні недоліки: низька швидкодія, неможливість захистити код від дизасемблювання, необхідність використання потужних універсальних процесорів. Крім того, дані продукти важко використовувати в мережних пристроях.

В інтелектуальних мережних пристроях до недавнього часу використовувались програмні засоби захисту мережевих протоколів. Але, в зв'язку із зростанням пропускної здатності мереж, більшість фірм-виробників перейшла до використання апаратних засобів захисту інформації. При цьому для виконання криптографічних протоколів використовуються апаратні засоби, які включають універсальний або програмований процесор з спеціалізованою чи доповненою системою команд та апаратно-орієнтовані процесори для виконання криптографічних алгоритмів та функцій. В більшості випадків ці засоби реалізуються в вигляді системи на кристалі та доповнюються відповідними елементами пам'яті та інтерфейсними схемами.

Найбільш повними функціонально є криптопроцесори фірми Hi-Fn. Вони апаратно реалізують всі необхідні для захисту мережі протоколи. Недоліком цих криптопроцесорів (наприклад Hi-Fn 7811) є обмежений набір протоколів роботи, який неможливо змінити.

Фірма "Інтрон" розробила модульну структуру процесора, яка дає можливість працювати з вибраними алгоритмами захисту інформації, а при необхідності змінювати і навіть додавати їх зі збереженням швидкодії і надійності. Цей процесор переважає відомі аналоги за функціональними

можливостями, продуктивністю і вартістю, що дає можливість використовувати його навіть в мережних платах для персональних комп'ютерів.

V. Ядра комп'ютерних пристроїв захисту інформації

Завдяки досягненням в галузях засобів проектування та мікроелектронного виробництва на сьогодні зформувався новий підхід до проектування комп'ютерних засобів. Цей підхід передбачає розробку та виставлення на ринок ядер комп'ютерних пристроїв - конструкторської документації на виготовлення комп'ютерного пристрою в вигляді НВІС або її складової частини. До складу конструкторської документації входить програмна модель комп'ютерного пристрою, написана мовою опису апаратних засобів, програмні моделі комп'ютерного пристрою, орієнтовані на його реалізацію в конкретному кристалі, засоби перевірки функцій та параметрів пристрою, детальний опис його інтерфейсу та функціонування. При цьому конструкторська документація на комп'ютерний пристрій розробляється з орієнтацією на її самостійне використання покупцем з наданням йому можливостей її доповнення та модернізації.

Для використання ядер комп'ютерних пристроїв користувач купляє у їх розробника ліцензію. Ліцензовані ядра надаються користувачу для використання в кристалах, які виробляються на засобах за його вибором. Вони можуть бути виготовлені в формі готового до синтезу в НВІС опису комп'ютерного пристрою на регістровому рівні, фізичної схеми чи в обох варіантах. Ліцензовані ядра створюються як великими, так і малими та середнього розміру компаніями, які не обов'язково мають власні засоби виготовлення НВІС. Наприклад, до числа сьогоднішніх виробників ліцензованих ядер входять фірми IBM, Mentor Graphics, Altera, Xilinx, Інтрон, Amphion. Покупець, закупивши на ринку необхідні йому ядра комп'ютерних пристроїв, проводить їх компоновку, доповнює необхідним обрамленням, розробляє спеціалізоване програмне забезпечення для вирішення поставленої задачі і створює потрібну йому комп'ютерну систему на кристалі. За рубежем технологія проектування ядер комп'ютерних пристроїв має назву core-технологія (core - ядро, серцевина) [19].

Ядра комп'ютерних пристроїв захисту інформації включають наступні моделі, написані на одній із мов опису апаратних засобів, як правило VHDL чи Verilog:

- моделі тракту обробки даних та системи керування із найпростішими інтерфейсами даних та службової інформації – такий підхід дозволяє розробнику системи захисту інформації використати готову чи розробити свою специфічну інтерфейсну логіку і максимально наблизити технічні параметри отриманої таким чином НВІС до своїх потреб;
- закінченої моделі комп'ютерних пристроїв захисту інформації із фіксованою інтерфейсною логікою – такий підхід дозволяє будувати НВІС одразу, без додаткових затрат, однак отримана система захисту інформації не завжди має оптимальні параметри.

Обидва підходи дозволяють виготовити як закінчені НВІС захисту інформації у вигляді замовлених інтегральних схем чи систем захисту інформації, побудованих за принципом "системи-на-кристалі"[20].

ТзОВ "Інтрон" пропонує ядра апаратних засобів для реалізації наступних криптографічних алгоритмів: DES, 3DES, AES, SHA-1, SHA-2, MD5, RSA. На базі названих алгоритмів створені ядра комп'ютерних пристроїв для виконання функцій аутентифікації, шифрування, цифрового підпису та керування ключами. Ці пристрої використовуються для побудови апаратних засобів реалізації криптографічних протоколів VPN, IPSec та ін.

VI. Висновки

Таким чином апаратні засоби захисту інформації мають вищу стійкість до зламу в порівнянні з програмними. Вони можуть бути поділені на засоби виконання криптографічних алгоритмів, криптографічних функцій та криптографічних протоколів. Ці засоби можуть бути реалізовані як на програмованих, так і на апаратно-орієнтованих процесорах, які характеризуються значно вищою продуктивністю. Самостійним продуктом на ринку засобів захисту інформації є ядра комп'ютерних пристроїв для виконання криптографічних алгоритмів, функцій та протоколів. Розвиток апаратни засобів захисту іде в напрямку їх вузької спеціалізації на малу кількість режимів роботи, включаючи спеціалізацію лише на зашифрування чи розшифрування, оптимізація трактів обробки даних, використання оптимізованих інтерфейсів, які дозволяють проводити ввід/вивід даних за мінімальний час, розробки нових архітектур процесорів для виконання модульних операцій, орієнтованих на реалізацію у вигляді НВІС, створення параметризованих моделей та бібліотек ядер комп'ютерних пристроїв, що дозволить синтезувати нові та модифіковувати існуючі апаратні засоби захисту інформації.

Література: 1. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone "Handbook of Applied Cryptography", CRC Press, October 1996, 816p. 2. ГОСТ28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. 3. FIPS 46, "Data Encryption Standard", Federal Information Processing Standard (FIPS), Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C. 4. X. Lai, J.L. Massey A proposal for a New Block Encryption Standard. Advances in Cryptology – EUROCRYPT-90 Proceedings, New York, NY: Springer-Verlag, pp.389-404. 5. J. Daemen and V. Rijmen. AES Proposal: Rijndael. In First Advanced Encryption Standard(AES) Conference, Ventura, CA, 1998. 6. L. Rivest, "The RC5 encryption algorithm", B. Preneel, editor, Fast Software Encryption, Second International Workshop (LNCS 1008), 86–96, Springer-Verlag, 1995. 7. C.M.Adams, "Constucting symmetric ciphers using CAST design procedure", Designs, Codes, and Cryptography, Vol. 12, No. 3, Movember 1997, pp. 71-104. 8. B.Schneier, "Description of a new variable-length key, 64-bit block cipher (Blowfish)", Fast Software Encryption, LNCS 809, R.Anderson, Ed., Springer-Verlad, 1994, pp. 191-204. 9. Информационная технология. Криптографическая защита информации. Функция хеширования ГОСТ34.311-95, М., Госстандарт, 1995. 10. FIPS 180-1, "Secure Hash Standard", Federal Information Processing Standard (FIPS), Publication 180-1, National Bureau of Standards, U.S. Department of Commerce, Washington D.C. 11. R. Rivest. The MD4 Message-Digest Algorithm // Network Working Group, Request for Comments: 1320, April 1992. 12. R. Rivest. The MD5 Message-Digest Algorithm // Network Working Group, Request for Comments: 1321. 13. 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. 14. T. ElGamal, "A Public Key Cryptosystem and a Signature System Based in Discrete Logarithms", IEEE Trans. on Information Theory, vol.IT-31, no.4, pp.469-472, July 1985. 15. W.Diffie, M.Hellman New Directions in cryptography // IEEE Transactions on Information Theory, November 1976. 16. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях/Под ред. В.Ф. Шаньгина. – М.: Радио и связь, 1999. – 328 с. 17. Бодров А.В., Коркишко Т.А., Молдовян Н.А. Программные шифры: пути повышения производительности //Материалы II Межрегиональной конференции "Информационная безопасность регионов России ИБРР-2001" (Санкт-Петербург, 26 – 29 ноября 2001). – 210 с., с. 86 – 87. 18. Мельник А.О., Коркішко Т.А. "Система підтримки виконання алгоритмів криптографічного захисту інформації на основі програмованого процесора та криптографічних акселераторів" //Вісник державного університету "Львівська політехніка" Комп'ютерні системи і мережі №385, Львів, 2000, с. 77 – 81. 19. Мельник А.О., Аль-Кхатіб А. "Концепція побудови нарощуваних параметризованих процесорних ядер спеціалізованих надвеликих інтегральних схем" //Вісник Державного університету "Львівська політехніка" №350, "Комп'ютерні системи та мережі", стор. 44 – 47. 20. M.Keating, P.Bricaud "Reuse Methodology Manual for System-On-a-Chip Design", Kluwer Academic Publishers, 1999, 224 p.