Шевчук Р., Манжула В., Адамів О. Оцінка технічних характеристикопераційних пристроїв процесорів хешування // Вісник ТДТУ. — 2009. — Том 14. — № 2. — С. 103-108. — (приладобудування та інформаційно-вимірювальні технології).

УДК 681.3

Р. Шевчук, канд. техн. наук; В. Манжула, канд. техн. наук; О. Адамів, канд. техн. Наук

Тернопільський національний економічний університет

ОЦІНКА ТЕХНІЧНИХ ХАРАКТЕРИСТИК ОПЕРАЦІЙНИХ ПРИСТРОЇВ ПРОЦЕСОРІВ ХЕШУВАННЯ

У роботі досліджено технічні характеристики операційних пристроїв процесорів хешування на базі алгоритмів MD5 та SHA-1. В рамках роботи проведено аналіз апаратної та часової складності алгоритмів хешування на основі запропонованих структур операційних пристроїв. Отримано аналітичні вирази, що дозволяють пов'язати побудовані структури операційних пристроїв та їх технічні характеристики.

Ключові слова: *технічні характеристики, операційних пристрій, процесори хешування, MD5, SHA-1.*

R. Shevchuk, V. Manzhula, O. Adamiv

ESTIMATION OF TECHNICAL CHARACTERISTICS OF OPERATION DEVICES OF HASH PROCESSORS

In work explored of technical characteristic of operation devices of hash processors on the base of algorithms MD5 and SHA-1. In work the analysis of hardware and time complexity of hashing algorithms on the basis of the offered structures of operation devices. The analytical expressions which allow to link the built structures of operation devices and their technical characteristics is developed.

Keywords: *technical characteristics, operation device, hash processors, MD5, SHA-1*

I. Вступ. Прогрес у розвитку теорії побудови алгоритмів хешування, доступність обчислювальної техніки та здешевлення технології виробництва надвеликих інтегральних мікросхем зумовлює широке використання процесорів хешування як у складі спеціалізованих систем захисту інформації, так і у складі пристроїв, орієнтованих на використання в універсальних системах. Однак невисока продуктивність обробки даних, згідно з алгоритмами хешування на програмованих процесорах, зумовлена невідповідністю системи команд універсальних процесорів характерним операціям алгоритмів хешування, породжує задачу створення спеціалізованих процесорів хешування. На сьогоднішній день відомі реалізації спеціалізованих процесорів [1-5], орієнтовані на виконання алгоритмів хешування MD5 [6] та SHA-1 [7]. Проведений аналіз даних процесорів показав значні переваги таких процесорів: завдяки структурній спеціалізації їх складових частин, зокрема відображенню структури виконуваного алгоритму на тракт обробки даних, досягається висока продуктивність обробки даних [8]. Однак актуальним залишається питання оцінки складності спеціалізованих процесорів хешування, що реалізують алгоритми хешування MD5 та SHA-1.

У даній роботі основна увага звертається на операційні пристрої (ОП) процесорів хешування, зокрема на їх базові структури та технічні характеристики. Метою роботи є оцінка технічних характеристик операційних пристроїв процесорів хешування.

II. Базові структури операційних пристроїв процесорів хешування. Враховуючи базові способи побудови алгоритмів хешування, наприклад [9,10], їх загальну структурну організацію можна представити у вигляді поєднання буфера та двох процедур: обчислення розпису повідомлення та обчислення хеш-значення (рисунок 1):

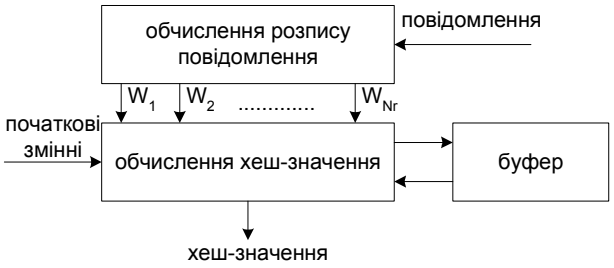

Рисунок 1 - Структура алгоритмів хешування

Процедура обчислення розпису повідомлення складається з набору функціональних операторів перетворення вхідного повідомлення в блоки, кратні 512 біт, які подаються в процедуру обчислення хеш-значення.. В процесі перетворення вхідне повідомлення доповнюється до довжини L (L≡448 mod 512). Для зберігання проміжних та кінцевих результатів хеш-значення використовується буфер, який, в свою чергу, ділиться на регістри, з яких дані блоками (32 біти) подаються у модуль обчислення хеш-значення.

Запропонована структурна організація узагальненого алгоритму хешування дозволяє детально проаналізувати усі структурні вузли процесора хешування. Оскільки процедура обчислення хеш-значення складає основу процесора хешування, доцільним є її детальний аналіз. Представлення даної процедури у вигляді операційного пристрою, запропоноване в [11], дозволяє визначити її технічні характеристики (часову та апаратну складність) для базових структур ОП. До складу базових структур ОП включено конвеєрний граф-алгоритмічний операційний пристрій (КГАОП), ітераційний граф-алгоритмічний операційний пристрій (ІГАОП) та ітераційно-конвеєрний граф-алгоритмічний операційний пристрій (ІКГАОП) [12].

КГАОП процесорів хешування складається з *Nr* послідовно з'єднаних комбінаційних схем (КС), що реалізують відповідні раунди алгоритму хешування, розділених конвеєрними регістрами (рисунок 2).

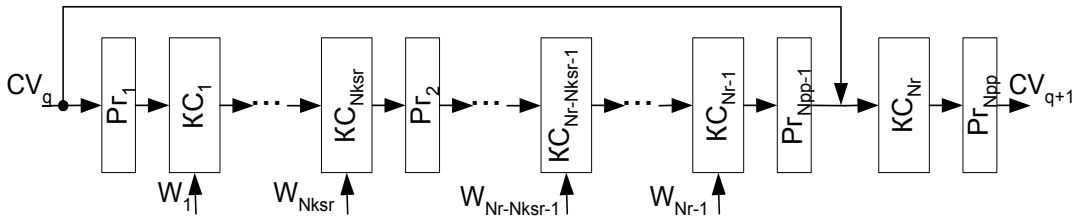

Рисунок 2 – Структура КГАОП процесора хешування

Для алгоритму хешування MD5 будемо вважати, що Nr_{MD5}=65, причому 64 раунди є структурно-подібними, а останній раунд виконує операцію додавання за модулем 2^{32}. Аналогічно, для алгоритму хешування SHA-1, $Nr_{SHA\text{-}1}$=81. Послідовність КС розбита конвеєрними регістрами із врахуванням вимоги (*Nr*–1) mod *Npp* = 0, де *Npp* – кількість конвеєрних регістрів. При цьому, кількість КС між конвеєрними регістрами буде визначатися числом *Nksr* = (*Nr*–1)/*Npp*.

Інший варіант побудови ОП процесора хешування полягає в ітераційному виконанні обчислень (рисунок 3).

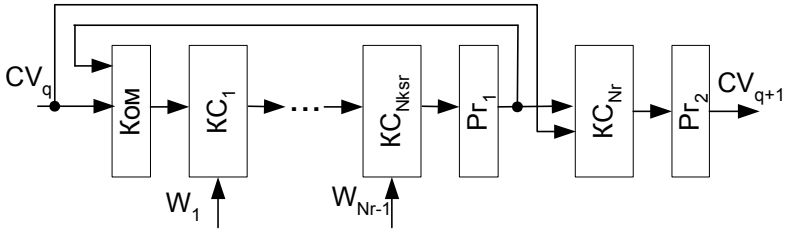

Рисунок 3 – Структура ІГАОП процесора хешування

Комбінаційні схеми ІГАОП реалізують проекцію потокового графу алгоритму хешування [14]. Розгортання структури графу проводиться послідовно у часі. Характерною особливістю цієї структури є використання комутатора даних (Ком) для забезпечення ітераційної обробки даних, двох конвеєрних регістрів ($Рг_1$ і $Рг_2$), перший з яких призначений для ітераційного виконання *Nr*-1 раундів алгоритму хешування, а другий – для зберігання проміжного результату хешування. Між комутатором і конвеєрним регістром $Рг_1$ розташовують таку кількість КС *Nksr*, щоб виконувалася рівність (*Nr*-1) mod *Nksr* = 0. В ІГАОП процесора хешування обчислення проводиться шляхом багатократного проходження векторів даних ($W_1, W_2,...,W_{Nr-1}$) через операційний пристрій.

Проміжне місце між ітераційними та конвеєрними граф-алгоритмічним ОП займає ІКГАОП. Так як згідно з алгоритмом хешування блоки даних обробляються за фіксовану кількість структурно подібних раундів, то ІКГАОП повинен містити дві чи декілька КС, що реалізують проекцію функціональних операторів потокового графу (раундів), через які блоки даних проходять задану кількість разів та надходять на вихід (рисунок 4).

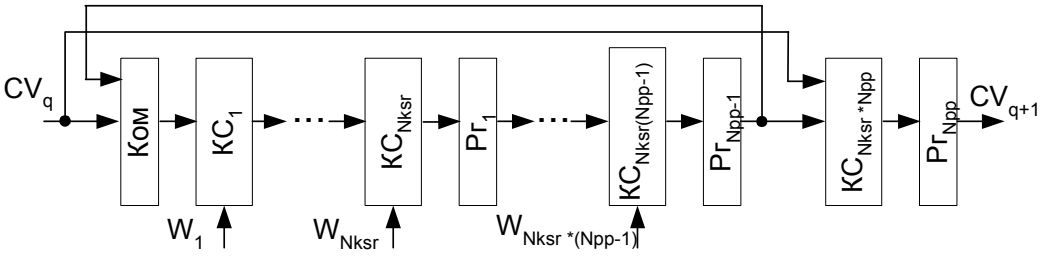

Рисунок 4 – Структура ІКГАОП процесора хешування.

Кількість конвеєрних регістрів для цієї структури ОП визначається числом *Npp*, яке визначається з нерівності 1 < *Npp* < (*Nr*–1)/*Nksr*, де *Nksr* – кількість реалізованих КС між конвеєрними регістрами, *(Nr–1) mod Npp = 0*. При інших значеннях числа конвеєрних регістрів ускладнюється керування ОП внаслідок необхідності організації асинхронної роботи складових ОП та пропуску чи обходу КС, які розташовані ближче до останнього конвеєрного регістра. Дані в ОП подаються у вигляді матриці, де кількість рядків матриці визначається кількістю тактів для обробки одного буферу, а кількість стовпців – число реалізованих КС і конвеєрних регістрів.

ІІІ. Оцінка технічних характеристик процесорів хешування. До технічних характеристик процесорів хешування віднесемо їх апаратну та часову складності [13].

Апаратна складність характеризується кількістю елементів деякого ієрархічного рівня представлення апаратних засобів, які утворюють алгоритмічний пристрій [13]. Надалі під алгоритмічним пристроєм будемо розуміти ОП процесора хешування.

Так як процес обробки вхідних даних починається з обчислення розпису повідомлення, оцінку складності даної процедури будемо проводити згідно з виразом:

$$A_{RP}=A_{RP}^{ADD}+A_{RP}^{LEN}+A_{RP}^{CUT}(L), \quad (1)$$

де A_{RP}^{ADD}- апаратна складність процедури доповнення повідомлення;

A_{RP}^{LEN} – апаратна складність процедури доповнення значення довжини початкового повідомлення;

A_{RP}^{CUT} – апаратна складність процедури формування вхідних блоків по L біт, $L_{MD5}=L_{SHA-1}=512$.

Оцінку апаратної складності процедури обчислення значення хеш-функції (A_{MD}^{A}) алгоритму *A, A*={MD5, SHA-1} проведемо за формулою:

$$A_{MD}^{A}=A_{SN(Nksr,Npp)}^{A}+A_{BUF}, \quad (2)$$

де $A_{SN(Nksr,Npp)}^{A}$ – апаратна складність операційного пристрою алгоритму A з структурою $SN(Nksr, Npp)$, де SN – код назви структури операційного пристрою ("і" – ІГАОП, "к" – КГАОП, "ік" – ІКГАОП),

$Nksr$, Npp – параметри структур операційних пристроїв: кількість реалізованих комбінаційних схем і конвеєрних регістрів відповідно;

A_{BUF} – апаратна складність буфера, в який записуються проміжні та кінцеві результати.

Формули (1), (2) в сумі будуть визначати складність ОП процесора хешування:

$$A_{HASH}^{A}=A_{RP}^{ADD}+A_{RP}^{LEN}+A_{RP}^{CUT}(L)+A_{SN(Nksr,Npp)}^{A}+A_{BUF} \quad (3)$$

Апаратна складність процедури обчислення хеш-значення буде різною для кожної структури операційного пристрою. Для обчислення складності структур цих операційних пристроїв введемо поняття затрати обладнання. Під затратами обладнання розуміють кількість апаратури, виражену в деяких одиницях [1]. Для оцінки затрат обладнання в деяких одиницях на реалізацію ОП процесорів хешування (для структурно-подібних раундів необхідно (в умовних одиницях виміру затрат обладнання): W_{KC}^{A} – для реалізації КС алгоритму А, $W_{PГ}^{A}$ - затрати на конвеєрні регістри алгоритму А, W_{K}^{A} – затрати обладнання на комутатори даних алгоритму А(для ітераційних та ітераційно-конвеєрних структур). Також в затрати обладнання включимо: W_{KCNr}^{A} - для реалізації комбінаційної схеми, яка виконує операцію додавання за модулем 2^{32} для алгоритму А.

Для запропонованих структур ОП [2] процесорів хешування отримаємо такі вирази для оцінки затрат обладнання:

- для КГАОП:

$$W_{K}^{A}=Npp*W_{PГ}^{A}+(Nr-1)*W_{KC}^{A}+W_{KCNr}^{A} \quad (4)$$

- для ІГАОП:

$$W_{ITEP}^{A}=W_{K}^{A}+2*W_{PГ}^{A}+Nksr*W_{KC}^{A}+W_{KCNr}^{A} \quad (5)$$

- для ІКГАОП:

$$W_{IK}^{A}=W_{K}^{A}+Npp*W_{PГ}^{A}+((Nr-1)/Nksr*Npp*W_{KC}^{A})+W_{KCNr}^{A} \quad (6)$$

Одержані вирази (4), (5), (6) дозволяють більш детально проаналізувати апаратну складність операційного пристрою процедури обчислення хеш-значення та визначити складність цієї процедури в умовних одиницях на реалізацію ОП.

В таблиці 1 наведено складність складових процедур операційних пристроїв алгоритмів хешування. Одиницями складності в даній таблиці є комбінаційні схеми, конвеєрні регістри та комутатори даних.

Таблиця 1 - Апаратна складність складових процедур операційних пристроїв процесорів хешування

	A_{RP}	A_{BUF}	$\min(W_K^A)$	$\max(W_K^A)$	$\min(W_{ITEP}^A)$	$\max(W_{ITEP}^A)$	$\min(W_{IK}^A)$	$\max(W_{IK}^A)$
MD5	3КС	8Рг	65КС+2Рг	65КС+ 64Рг	2КС+2Рг+ 1Кд	65КС+2Рг+ 1Кд	3КС+2Рг+ 1Кд	33КС+32Рг +1Кд
SHA-1	3КС	10Рг	81КС+2Рг	81КС+ 80Рг	2КС+2Рг+ 1Кд	81КС+2Рг+ 1Кд	3КС+2Рг+ 1Кд	41КС+40Рг +1Кд

Часова складність операційного пристрою визначається кількістю елементів схеми, розташованих вздовж максимального критичного шляху розповсюдження сигналу [16]. Для алгоритму хешування A, в якому $e_{i,j}$ – і-тий елемент j-го критичного шляху, часова складність (L^A) буде задаватись виразом:

$$L_{HASH}^{A}=max(\sum_{i=j}^{j}E_{SN(Nksr,Npp)}^{A}(e_{i,j}),\ \sum_{i=j}^{j}E_{BUF}(e_{i,j}),\ \sum_{i=j}^{j}E_{RP}(e_{i,j})), \quad (7)$$

де $E_{SN(Nksr,Npp)}^{A}$ – часова складність процедури обчислення хеш-значення;

E_{BUF}^{A} – часова складність буфера;

E_{RP} – часова складність процедури обчислення розпису повідомлення.

За результатами таблиці 1, можна стверджувати, що найбільшою часовою складністю буде володіти процедура обчислення хеш-значення, оскільки її максимальний критичний шлях є значно більшим від критичних шляхів інших процедур.

Для детальнішого розгляду часової складності процедури обчислення хеш-значення приймемо: Z_1^A – кількість елементів, що міститься в КС, яка виконує елементарну операцію алгоритму хешування A; Z_2^A – кількість елементів що міститься в КС, яка виконує операцію додавання за модулем 2^{32} алгоритму хешування A; Z_3^A – кількість елементів, що містить конвеєрний регістр алгоритму A; Z_4^A – кількість елементів, що містить комутатор даних алгоритму A.

Запишемо вирази, які будуть визначати часову складність операційного пристрою, що обчислює хеш-значення, базуючись на структурах ОП:

- для КГАОП:

$$L_K=(Nr-1)*Z_1^A+Z_2^A+Npp*Z_3^A; \quad (8)$$

- для ІГАОП:

$$L_{ITEP}=Nksr*Z_1^A+Z_2^A+2*Z_3^A+Z_4^A; \quad (9)$$

- для ІКГАОП:

$$L_{IK}=Npp*Nksr*Z_1^A+Z_2^A+Npp*Z_3^A+Z_4^A. \quad (10)$$

Висновок

У роботі проведено оцінку технічних характеристик операційних пристроїв алгоритмів хешування MD5 та SHA-1. Проведені дослідження дозволили встановити, що на кінцевий результат – отримання хеш-значення, найбільше впливає процедура обчислення хеш-значення, тому основна увага в роботі була приділена даній процедурі. Зокрема, було дано оцінку апаратній та часовій складності алгоритмів хешування та одержано аналітичні вирази, які пов'язують технічні характеристики складових процедур алгоритмів хешування з параметрами їх структур. Встановлено, що найменшою апаратною складністю володіють ітераційні операційні пристрої процесорів хешування, а найбільшою – конвеєрні. Найменша часова складність буде в конвеєрних операційних пристроїв.

Література

1. Safe Net SafeXcel-2141 Processor Architecture. [Electronic resources]. – Режим доступу: www.safenet-inc.com
2. Net Octave NSP2000 Internet protocol Security Processor Datasheet. – 2001. – 15 p. [Electronic resources]. – Режим доступу: http://octave.sourceforge.net
3. HiFn Security Processors Selector Guide Hipp 7814, Hipp 7854, Hipp 7955. – 2001. – 12 p. [Electronic resources]. – Режим доступу: www.hifn.com
4. Motorola MPC185TS/D, MPC184TS/D Communication Processors. Datasheet. – 2001. – 56 p. [Electronic resources]. – Режим доступу: www.chipdocs.org
5. Semiconductors Processor Architecture. User Guide. – 2001. [Electronic resources]. – Режим доступу: www.springerlink.com
6. Rivest R. The MD5 Message-Digest Algorithm. MIT LCS and RSA Data Security, Inc., April 1992. Режим доступу: www.ietf.org/rfc/rfc1321.txt
7. National Institute of Standards and Technology. Secure Hash Standard (SHA-1). Federal Information Processing Standards Publication #180-1, 1993. Режим доступу: www.itl.nist.gov
8. Шевчук Р.П. Оптимізація програмно-апаратних засобів реалізації IPSec: маг. роб. : 8.091501 / Шевчук Руслан Петрович. – Тернопіль, 2003. – 121 с.
9. Merker R. Systematischer Entwurf und Modellierung systolischer Arrays. Habilitation, TU Dresden, 1989.
10. Damgård I.B. A Design Principle for Hash Functions. - Proceedings of CRYPTO '89, Springer Lecture Notes in Computer Science LNCS 435. -1989. P. 416-427
11. Коркішко Т. Базові структури операційних пристроїв хешування для процесорів підтримки протоколу IPSec / Т. Коркішко, Л. Коркішко, Р. Шевчук // Комп'ютинг. – 2003. – Т. 2, № 1. – С. 41–47.

12. Коркішко Т.А. Багатоканальні апаратно-орієнтовані процесори симетричного блокового шифрування : дис. ... канд.тех.наук : 05.13.05 / Коркішко Тимур Анатолійович. – Львів, 2002. – 213с.
13. Черкаський М. Складність апаратно-програмних комп'ютерних засобів / М. Черкаський // Сучасні проблеми в комп'ютерних науках. – 2000. С. 58-67.
14. Мельник А.О. Спеціалізовані комп’ютерні системи реального часу / А. О. Мельник. – Львів, 1996. – 54 с.

Одержано 06.05.2009 р.