Міністерство освіти і науки, молоді та спорту України
Вінницький національний технічний університет

БАРИШЕВ ЮРІЙ ВОЛОДИМИРОВИЧ

УДК 004.31 + 004.42 : 004.424.47

МЕТОДИ ТА ЗАСОБИ ШВИДКОГО БАГАТОКАНАЛЬНОГО ХЕШУВАННЯ ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Спеціальність 05.13.05 – Комп’ютерні системи та компоненти

Автореферат дисертації на здобуття наукового ступеня
кандидата технічних наук

Вінниця – 2012

Дисертацією є рукопис.

Робота виконана в Вінницькому національному технічному університеті Міністерства освіти і науки, молоді та спорту України.

Науковий керівник: доктор технічних наук, професор
Лужецький Володимир Андрійович,
Вінницький національний технічний університет,
завідувач кафедри захисту інформації

Офіційні опоненти: доктор технічних наук, професор
Корченко Олександр Григорович,
Національний авіаційний університет, м. Київ, завідувач кафедри безпеки інформаційних технологій

доктор технічних наук, професор
Рудницький Володимир Миколайович,
Черкаський державний технологічний університет,
завідувач кафедри системного програмування

Захист відбудеться «17» березня 2012 р. о 10 годині на засіданні спеціалізованої вченої ради Д 05.052.01 у Вінницькому національному технічному університеті за адресою: 21021, м. Вінниця, вул. Хмельницьке шосе, 95, ГНК, ауд. 210.

З дисертацією можна ознайомитись у бібліотеці Вінницького національного технічного університету за адресою: 21021, м. Вінниця, вул. Хмельницьке шосе, 95.

Автореферат розісланий «15» лютого 2012 р.

Учений секретар
спеціалізованої вченої ради С. М. Захарченко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми

Останніми роками спостерігається значне збільшення обсягів інформації, що зберігається, обробляється та передається за допомогою комп'ютерних систем. Різке розширення кола користувачів, що мають безпосередній доступ до ресурсів системи та постійне збільшення атак на комп'ютерні системи породжують проблему захисту інформації. Спільне використання та оброблення інформації в комп'ютерних системах породжує для кожного конкретного користувача комп'ютерної системи необхідність підтвердження його автентичності, а також автентичності джерела інформації.

Задачі забезпечення автентичності даних та користувачів розв'язуються за допомогою засобів комп'ютерної криптографії, а саме криптографічного хешування. При цьому засоби комп'ютерної криптографії дозволяють забезпечувати певний рівень стійкості до атак зловмисників за рахунок реалізації складних обчислень, які потребують значних часових витрат на своє виконання. Внаслідок цього комп'ютерна система стає недружньою до користувача або взагалі не виконує поставлені перед нею задачі, зокрема ускладнюється обмін інформацією в режимі реального часу. Саме тому для комп'ютерних систем є актуальним створення криптографічних методів та засобів хешування даних підвищеної швидкості.

Свідченням актуальності створення нових методів хешування є проведення Національним інститутом стандартів та технологій США міжнародного конкурсу на нову хеш-функцію, яка буде прийнята як стандарт.

Важливий внесок у розробку методів та засобів комп'ютерної криптографії взагалі та хешування зокрема зробили такі вітчизняні та зарубіжні вчені: А. Я. Білецький, І. Д. Горбенко, В. К. Задірака, О. Г. Корченко, О. О. Кузнєцов, В. М. Рудницький, М. М. Савчук, К. Г. Самофалов, Г. Бертоні, Е. Біхам, П. Гаураварам, І. Дамгаард, О. Данкелман, А. Жукс, Дж. Келсі, Т. Кохно, Ш. Люкс, Р. Меркль, М. А. Молдовян, О. А. Молдовян, Б. Преніл, Р. Рівест, А. Шамір, Б. Шнайер, В. В. Ященко та інші.

Зв'язок роботи з науковими програмами, планами, темами

Тема наукового дослідження відповідає підпункту 1.2.5.9 "Розробка теоретичних основ і прикладних методів створення комп'ютерних інформаційно-аналітичних систем, дослідження та розробка методів захисту інформації в комп'ютерних системах і мережах. Методи та системи підтримки прийняття рішень" "Основних наукових напрямів та найважливіших проблем фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук на 2009–2013 роки" (затверджено спільним наказом Міністерства освіти і науки та Національної академії наук України від 26.11.2009 р. № 1066/609).

Результати дисертаційної роботи отримані при виконанні науково-дослідних робіт кафедри захисту інформації Вінницького національного технічного університету: «Розробка програмного модуля парольної автентифікації користувачів бази даних клієнтів» (ДР №0111U001770) та «Розробка програмного засобу для криптографічно стійкої автентифікації даних» (договір про творчу співдружність №51/4), у яких автор брав участь як відповідальний виконавець.

Мета і задачі дослідження

Метою роботи є підвищення швидкості автентифікації даних та користувачів в комп'ютерних системах шляхом створення нових методів та засобів хешування на основі багатоканальних конструкцій хешування, які забезпечують розпаралелення обчислень.

Відповідно до поставленої мети в дисертаційній роботі ставилися і розв'язувалися такі задачі дослідження:

- аналіз відомих методів хешування, використовуваних для автентифікації даних та користувачів в комп'ютерних системах та атаки на ці методи;
- розробка математичних моделей ітерацій стійкого розпаралеленого хешування;

- розробка методів багатоканального хешування на основі задач, що мають теоретично доведену складність;
- розробка методів багатоканального хешування "з нуля";
- розробка програмних та апаратних засобів хешування.

Об'єкт дослідження. Процес криптографічного захисту інформації в комп'ютерних системах.

Предмет дослідження. Методи та засоби криптографічного хешування даних в комп'ютерних системах.

Методи дослідження

При розв'язанні поставлених наукових задач в дисертаційній роботі були використані методи теорії абстрактних автоматів – для опису керованого хешування; методи криптології – при аналізі відомих атак на хеш-функції, розробці конструкцій хешування, під час аналізу стійкості розроблених методів хешування; методи теорії чисел – при розробці методів хешування теоретично доведеної стійкості; методи булевої алгебри – при розробці методів хешування "з нуля"; методи теорії складності та методи теорії алгоритмів – при визначенні оцінок стійкості методів хешування; методи математичної статистики – при дослідженні розподілу вихідних значень під час експерименту.

Наукова новизна одержаних результатів.

Науковими результатами дисертаційної роботи є такі:

- вперше запропоновано узагальнену модель ітерацій (конструкцію) багатоканального хешування, яка на відміну від відомих передбачає можливість керування параметрами перетворень в процесі хешування, що дозволяє розробляти нові методи багатоканального хешування підвищеної швидкості та стійкості до загальних атак;
- вперше запропоновано конструкції багатоканального хешування, стійкі до загальних атак на основі мультиколізій, з опосередкованим зав'язуванням всіх каналів один з одним, які порівняно з конструкціями багатоканального хешування з безпосереднім зав'язуванням каналів один з одним дозволяють розробляти методи хешування, що забезпечують зменшення часу хешування від 1,4 до 16 раз;
- удосконалено методи багатоканального хешування на основі операції піднесення до степеня за модулем простого числа та структури спеціалізованих процесорів, що їх реалізують, які за рахунок зав'язування каналів дозволяють виконувати операцію піднесення до степеня для чисел в q раз меншої розрядності порівняно з відомими (де q – кількість каналів), що забезпечує збільшення швидкості хешування у q раз;
- отримали подальший розвиток конструкції багатоканального хешування, стійкі до загальних атак на основі мультиколізій, із безпосереднім зав'язуванням всіх каналів один з одним, які дозволяють, порівняно з відомими, розробляти методи хешування для кількості каналів $q>2$, що за рахунок розпаралелення обчислень дозволяє досягти підвищення швидкості хешування у $q/2$ раз;
- отримали подальший розвиток методи формування вектора керування параметрами хешування, які забезпечують адаптування до зміни параметрів конструкцій хешування, що, в свою чергу, дозволяє розробляти програмно-апаратні засоби хешування з різними характеристиками швидкість/стійкість.

Практичне значення одержаних результатів

Практичне значення одержаних результатів полягає в тому, що використання запропонованих формальних методів і конкретних рішень дозволяє отримувати більш досконалі, порівняно з відомими, програмні та апаратні засоби, які використовуються для автентифікації даних та користувачів в комп'ютерних системах. Основними практичними результатами дисертаційної роботи є:

- програмні засоби для тестування методів багатоканального керованого хешування за допомогою Known Answer Tests;

- програмні засоби багатоканального керованого хешування із вихідним хеш-значенням довільної довжини (кратним розрядності обчислювальної платформи – 16/32/64 біти) та різними параметрами конструкції хешування;
- рекомендації щодо побудови спеціалізованих процесорів для швидкого хешування даних в комп'ютерних системах.

Програмний засіб багатоканального керованого хешування впроваджено у ТОВ "ВІАТЕЛ" (м. Вінниця) у комп'ютерній системі підприємства при парольній автентифікації користувачів бази даних клієнтів підприємства (акт про впровадження результатів дисертаційної роботи від 09 серпня 2011). Програмний засіб багатоканального хешування на основі операції піднесення до степеня за модулем простого числа впроваджено у ПП "ВІНБУДІЗОЛ" (м. Вінниця) у комп'ютерній системі підприємства в програмному засобі перевірки автентичності даних (акт про впровадження результатів дисертаційної роботи від 18 серпня 2011).

Конструкції та методи багатоканального хешування, а також структури спеціалізованих процесорів, які їх реалізують, впроваджені в навчальний процес Вінницького національного технічного університету на кафедрі захисту інформації в курсах лекцій і курсовому проектуванні з дисциплін "Криптографія та криптоаналіз", "Проектування мікропроцесорних пристроїв" і при виконанні кваліфікаційних робіт студентами кафедри (акт про впровадження результатів дисертаційної роботи від 23 червня 2011).

Особистий внесок здобувача

Основні наукові результати дисертаційної роботи отримані автором самостійно. У спільних наукових працях особисто автору належать: узагальнена конструкція багатоканального хешування та підходи до зав'язування каналів [1]; обґрунтування вимог до криптографічних примітивів; криптографічні примітиви, керування параметрами яких відбувається за допомогою операції циклічного зсуву [2]; узагальнена конструкція багатоканального керованого хешування; функції ущільнення, що містять керовані операції; методи формування вектора керування [3]; структури спеціалізованих процесорів багатоканального керованого хешування, функціональні блоки спеціалізованих процесорів [4]; конструкції багатоканального керованого хешування із безпосереднім зав'язуванням каналів один з одним; конструкції багатоканального хешування, стійкі до загальних атак на основі мультиколізій, з опосередкованим зав'язуванням всіх каналів один з одним; методи багатоканального керованого хешування [5]; конструкції багатоканального хешування із зав'язування всіх каналів один з одним; методи багатоканального хешування, які базуються на операції піднесення до степеня за модулем простого числа [6]; узагальнена конструкція багатоканального керованого хешування; методи багатоканального керованого хешування; оцінки швидкості хешування [7]; процедура побудови ітерацій хешування, структура спеціалізованого процесора для багатоканального хешування на основі операції піднесення до степеня за модулем простого числа із безпосереднім зав'язуванням каналів на основі операції додавання за модулем двох [13]; структура спеціалізованого процесора для багатоканального хешування на основі операції піднесення до степеня за модулем простого числа із опосередкованим зав'язуванням каналів на основі операції додавання за модулем двох [14]; структура спеціалізованого процесора для багатоканального хешування на основі операції піднесення до степеня за модулем простого числа із безпосереднім зав'язуванням каналів на основі операції множення [15].

Всі роботи виконані у Вінницькому національному технічному університеті.

Апробація результатів дисертації

Основні результати досліджень доповідалися та обговорювалися на таких конференціях:

- 2-й міжнародній науково-практичній конференції "Методи та засоби кодування, захисту й ущільнення інформації", м. Вінниця, 2009 р.;

- 1-й міжнародній конференції "Проблеми й перспективи розвитку ІТ-індустрії в Україні", м. Харків, 2009 р.;
- 4-й міжнародній науково-технічній конференції "Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування", м. Вінниця, 2009 р.;
- міжнародній науково-технічній конференції "Інформаційна та економічна безпека", м. Харків, 2010 р.;
- 3-й міжнародній науково-практичній конференції "Методи та засоби кодування, захисту й ущільнення інформації", м. Вінниця, 2011 р.;
- 5-й міжнародній науково-технічній конференції "Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування", м. Вінниця, 2011 р.;
- 3-й міжнародній науково-практичній конференції "Обробка сигналів і негауссівських процесів", м. Черкаси, 2011 р.

Публікації

Основні результати дисертації опубліковано в 15 роботах, з яких 5 статей у фахових виданнях з переліку ВАК України, 7 тез доповідей та 3 патенти на корисну модель.

Структура і обсяг дисертації

Робота складається зі вступу, чотирьох розділів, висновків, списку використаної літератури, трьох додатків. Загальний обсяг дисертації – 168 сторінок, з них основний зміст – 132 сторінки, 10 таблиць, 38 рисунків. Список використаних джерел містить 114 найменувань.

ОСНОВНИЙ ЗМІСТ РОБОТИ

Вступ до дисертації містить обґрунтування актуальності теми дисертаційної роботи, визначення мети, задач, об’єкту та предмета дослідження, опис наукових та практичних результатів, отриманих в роботі, відомості щодо впровадження результатів роботи, публікацій та апробації результатів роботи.

У першому розділі дисертаційної роботи визначаються задачі, які розв’язуються за допомогою криптографічного хешування в комп’ютерних системах, а також аналізуються атаки на хеш-функції та методи збільшення стійкості до них. Проведений аналіз показав, що методи криптографічного хешування використовуються для розв’язання таких задач в комп’ютерних системах: авторизації та автентифікації користувачів; автентифікації даних; перевірці цілісності даних; генерування псевдовипадкових чисел.

У ході досліджень було визначено, що атаки на хеш-функції поділяються на атаки "грубої сили" та криптоаналітичні атаки. Криптоаналітичні атаки в свою чергу поділяються на загальні та спеціальні. У зв’язку з тим, що загальні атаки можуть бути застосовані до всіх хеш-функцій певної конструкції, відповідно, вони є більш небезпечними, ніж спеціальні, оскільки збільшити стійкість до останніх можна шляхом внесення певних змін у перетворення, що використовуються у функції ущільнення або шляхом використання іншої функції ущільнення. Протидіяти ж загальним атакам можливо лише після виявлення недоліків в моделях ітерацій (конструкціях) хешування та розроблення нових конструкцій. При цьому визначено, що серед загальних атак на хеш-функції найбільш небезпечними є атаки, які використовують мультиколізії, оскільки вони дозволяють отримувати степеневий приріст кількості колізій з лінійним зростанням складності реалізації цих атак.

Аналіз відомих підходів до розв’язання задачі підвищення стійкості хеш-функцій до загальних атак показав, що дані підходи не дозволяють протидіяти загальним атакам, що базуються на мультиколізіях, без збільшення довжини проміжного хеш-значення, отримання якого потребує більших витрат часу і/або обчислювальних ресурсів комп’ютерної системи.

Аналіз відомих хеш-функцій показав, що як хеш-функції, які базуються на задачах теоретично доведеної стійкості, так і хеш-функції, які базуються на відомих шифрах, внаслідок неприродності виконуваних перетворень для сучасних універсальних мікропроцесорів не дозволяють досягти високої швидкості хешування, хоча забезпечують високий рівень стійкості. На противагу ним хеш-функції, розроблені "з нуля", можуть

забезпечити вищу швидкість хешування, однак не гарантують такої ж високої стійкості. Визначено, що найбільш перспективними для реалізації хешування є підходи, які передбачають використання перетворень, оборотність яких зводиться до задач теоретично доведеної складності, оскільки вони забезпечують гарантований рівень стійкості хеш-функцій, та підходи до побудови перетворень, розроблені "з нуля", оскільки вони дозволяють забезпечити високу швидкість обчислень.

На основі результатів проведеного аналізу сформульовано завдання дисертаційних досліджень.

У другому розділі дисертаційної роботи досліджено моделі ітерацій багатоканального хешування даних. Для цього розроблено узагальнену модель ітерацій (конструкцію) багатоканального хешування:

$$\begin{cases} h_i^{(1)} = f_{v_i^{(1)}}\left(h_0^{(1)}, h_1^{(1)}, \ldots, h_{i-1}^{(1)}, h_0^{(2)}, \ldots, h_{i-1}^{(q)}, m_1, m_2, \ldots, m_l, r_1^{(1)}, r_2^{(1)}, \ldots, r_z^{(1)}, c_i\right); \\ h_i^{(2)} = f_{v_i^{(2)}}\left(h_0^{(1)}, h_1^{(1)}, \ldots, h_{i-1}^{(1)}, h_0^{(2)}, \ldots, h_{i-1}^{(q)}, m_1, m_2, \ldots, m_l, r_1^{(2)}, r_2^{(2)}, \ldots, r_z^{(2)}, c_i\right); \\ \ldots \\ h_i^{(q)} = f_{v_i^{(q)}}\left(h_0^{(1)}, h_1^{(1)}, \ldots, h_{i-1}^{(1)}, h_0^{(2)}, \ldots, h_{i-1}^{(q)}, m_1, m_2, \ldots, m_l, r_1^{(q)}, r_2^{(q)}, \ldots, r_z^{(q)}, c_i\right), \end{cases} \quad (1)$$

де $h_i^{(j)}$ – i-е канальне проміжне хеш-значення, отримане у j-му каналі;

m_i – i-й блок даних;

$r_i^{(j)}$ – псевдовипадкове число;

c_i – довжина вже захешованої частини повідомлення;

$f_{v_i^{(j)}}(\cdot)$ – функція ущільнення, параметри перетворень якої визначаються значенням вектора керування $v_i^{(j)}$.

На рис. 1 наведено схемну інтерпретацію узагальненої конструкції багатоканального хешування.

Запропоновано таке позначення для параметричного опису багатоканального хешування (MultiPipe Hash) конструкції (1):

$$MPH_q(k; d; z; \gamma; \phi), \quad (2)$$

де q – кількість каналів хешування;

k – кількість каналів, від проміжних хеш-значень яких залежить наступне проміжне хеш-значення j-го $(j = 1, 2, ..., q)$ каналу;

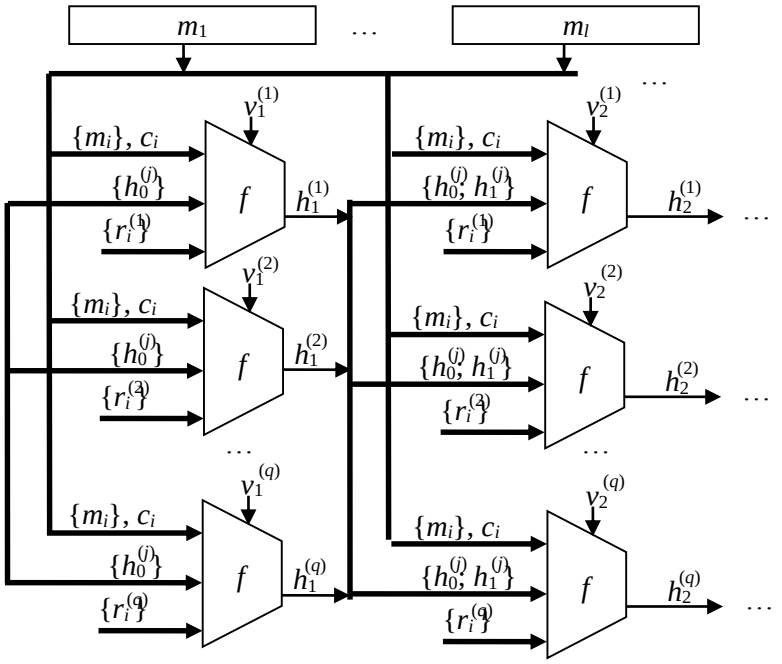

Рисунок 1 – Схемна інтерпретація узагальненої конструкції багатоканального хешування

d – кількість блоків даних, які беруть участь у формуванні хеш-значення в одному каналі;

z – кількість псевдовипадкових чисел, що використовуються під час однієї ітерації в одному каналі;

γ – співвідношення довжини проміжного хеш-значення до довжини хеш-значення всього повідомлення;

ϕ – кількість проміжних хеш-значень з інших каналів, що використовуються при формуванні вектора керування у j-му каналі.

Аналіз параметрів хешування (2) показав, що стійкість конструкцій багатоканального хешування до загальних атак залежить від параметра γ та зав'язування каналів один з одним, на який впливають параметри хешування k та ϕ При зав'язуванні каналів за допомогою проміжних хеш-значень пропонується така конструкція багатоканального хешування $MPH_q(q;1;0;1;0)$:

$$\begin{cases} h_i^{(1)} = f^{(1)}\left(h_{i-1}^{(1)}, h_{i-1}^{(2)}, \ldots, h_{i-1}^{(q)}, m_i\right); \\ h_i^{(2)} = f^{(2)}\left(h_{i-1}^{(2)}, h_{i-1}^{(1)}, h_{i-1}^{(3)}, \ldots, h_{i-1}^{(q)}, m_i\right); \\ \ldots \\ h_i^{(q)} = f^{(q)}\left(h_{i-1}^{(q)}, h_{i-1}^{(1)}, \ldots, h_{i-1}^{(q-1)}, m_i\right). \end{cases} \quad (3)$$

Зменшення довжини проміжних хеш-значень у конструкції хешування $MPH_q(q;1;0;1;0)$ призведе до зменшення стійкості багатоканального хешування до мультиколізій порівняно з хешуванням $MPH_q(q;1;0;q;0)$, якщо зловмисник буде розглядати процес хешування як "чорну скриньку". Однак конструкція хешування $MPH_q(q;1;0;1;0)$ забезпечить стійкість до атаки на окремо взятий канал.

Для того, щоб ускладнити зловмиснику попередню підготовку до атак пропонується використовувати підсилення конструкцій багатоканального хешування за допомогою домішування на кожній ітерації в кожен канал "динамічної криптографічної солі", тобто псевдовипадкового числа $r_i^{(j)}$, яке змінюється від ітерації до ітерації $r_i^{(j)} = rand^{(j)}\left(r_{i-1}^{(j)}\right)$ (де $rand(\cdot)$ – функція генерування псевдовипадкової послідовності чисел), а також довжини вже захешованої частини повідомлення c_i.

Велика кількість аргументів у канальних функціях ущільнення в конструкції (3) вимагає більшої кількості операцій для своєї реалізації, тому для збільшення швидкості хешування запропоновані конструкції багатоканального хешування із опосередкованим зав'язуванням каналів хешування, зокрема конструкція хешування $MPH_q(2;1;1;1;0)$:

$$\begin{cases} h_i^{(1)} = f^{(1)}\left(h_{i-1}^{(1)}, h_{i-1}^{(2)}, m_i, r_i^{(1)}, c_i\right); \\ h_i^{(2)} = f^{(2)}\left(h_{i-1}^{(2)}, h_{i-1}^{(3)}, m_i, r_i^{(2)}, c_i\right); \\ \ldots \\ h_i^{(q)} = f^{(q)}\left(h_{i-1}^{(q)}, h_{i-1}^{(1)}, m_i, r_i^{(q)}, c_i\right). \end{cases} \quad (4)$$

Проведений аналіз підходів до формування векторів керування показав, що найдоцільніше формувати вектор керування на основі проміжних хеш-значень, отриманих в інших каналах на попередній ітерації, що реалізує конструкція багатоканального хешування $MPH_q(1;1;0;1;q-1)$:

$$\begin{cases} h_i^{(1)} = f_{v_i^{(1)}}\left(h_{i-1}^{(1)}, m_i\right); \\ h_i^{(2)} = f_{v_i^{(2)}}\left(h_{i-1}^{(2)}, m_i\right); \\ \ldots \\ h_i^{(q)} = f_{v_i^{(q)}}\left(h_{i-1}^{(q)}, m_i\right); \\ v_i^{(1)} = g\left(h_{i-1}^{(2)}, h_{i-1}^{(3)}, \ldots, h_{i-1}^{(q)}\right); \\ v_i^{(2)} = g\left(h_{i-1}^{(1)}, h_{i-1}^{(3)}, \ldots, h_{i-1}^{(q)}\right); \\ \ldots \\ v_i^{(q)} = g\left(h_{i-1}^{(1)}, h_{i-1}^{(2)}, \ldots, h_{i-1}^{(q-1)}\right), \end{cases} \quad (5)$$

де $g(\cdot)$ – функція формування вектора керування.

Оскільки до функції формування вектора керування висувається менше вимог, ніж до функції ущільнення, то її реалізація є швидшою. Тому зав'язування за допомогою векторів керування дозволяє досягти більшої швидкості порівняно з опосередкованим зав'язуванням каналів. На рис. 2 наведено схемну інтерпретацію конструкції багатоканального керованого хешування $MPH_q(1;1;0;1;q-1)$ (5).

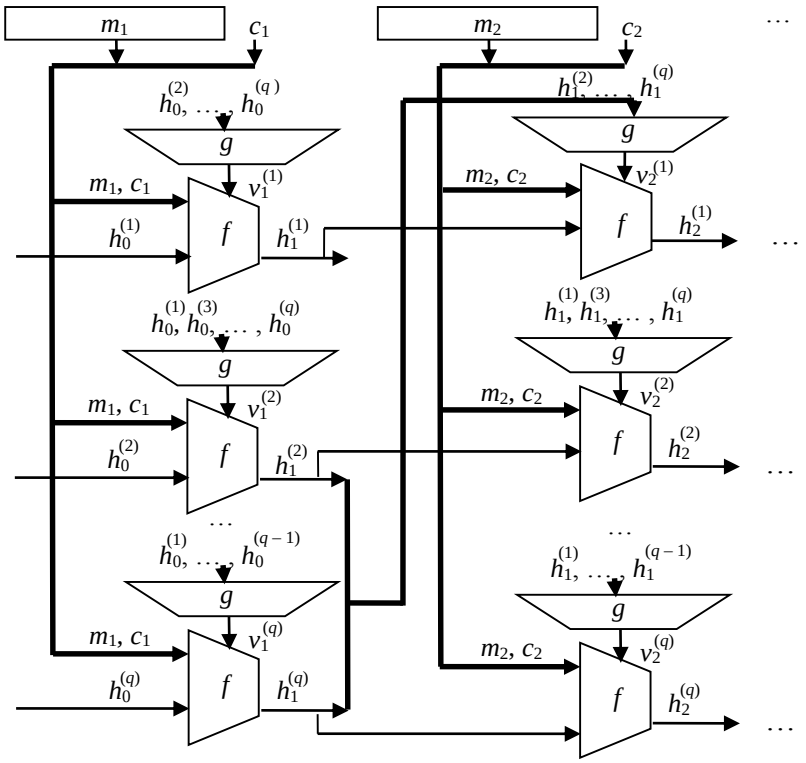

Рисунок 2 – Схемна інтерпретація узагальненої конструкції багатоканального хешування $MPH_q(1;1;0;1;q-1)$

Оскільки обидва методи зав'язування каналів не виключають один одного, то пропонується комбінувати їх. Виходячи з цього, узагальнена для q каналів конструкція багатоканального хешування $MPH_q(k;1;1;1;\phi)$ з комбінованим зав'язуванням каналів має такий вигляд:

$$\begin{cases} h_i^{(1)} = f_{v_i^{(1)}}\left(h_{i-1}^{(1)}, h_{i-1}^{(2)}, \ldots, h_{i-1}^{(k)}, m_i,\ r_i^{(1)},\ c_i\right); \\ h_i^{(2)} = f_{v_i^{(2)}}\left(h_{i-1}^{(2)}, h_{i-1}^{(3)}, \ldots, h_{i-1}^{(k+1)}, m_i,\ r_i^{(2)},\ c_i\right); \\ \ldots \\ h_i^{(q)} = f_{v_i^{(q)}}\left(h_{i-1}^{(q)}, h_{i-1}^{(1)}, \ldots, h_{i-1}^{(k-1)}, m_i,\ r_i^{(q)},\ c_i\right); \\ v_i^{(1)} = g\left(h_{i-1}^{(q)}, h_{i-1}^{(q-1)}, \ldots, h_{i-1}^{(q-\phi+1)}\right); \\ v_i^{(2)} = g\left(h_{i-1}^{(1)}, h_{i-1}^{(q)}, h_{i-1}^{(q-1)}, \ldots, h_{i-1}^{(q-\phi+2)}\right); \\ \ldots \\ v_i^{(q)} = g\left(h_{i-1}^{(q-1)}, h_{i-1}^{(q-2)}, \ldots, h_{i-1}^{(q-\phi)}\right), \end{cases} \tag{6}$$

де $k < (q-\phi)$.

Конструкції хешування із комбінованим зав'язуванням каналів дозволяють досягти більшої швидкості хешування, за умов однакової реалізації функцій ущільнення, порівняно з конструкціями хешування із зав'язуванням каналів хешування за допомогою проміжних хеш-значень та більш стійкими порівняно з конструкціями хешування із зав'язуванням каналів за допомогою векторів керування, які є їх частковими випадками. Саме тому, конструкції хешування із комбінованим зав'язуванням каналів є узагальненням конструкцій зав'язування каналів хешування.

У третьому розділі дисертаційної роботи розроблено методи багатоканального хешування на основі операції піднесення до степеня за модулем простого числа та методи багатоканального керованого хешування, розроблені "з нуля".

Метод хешування $MPH_q(q;1;1;1;0)$, який базується на операції піднесення до степеня за модулем простого числа полягає у виконанні таких дій:

- розбивання повідомлення M на блоки рівної довжини. Якщо довжина повідомлення $\|\mathrm{M}\|$ не кратна довжині блоку даних $\|m_i\|$, то повідомлення попередньо доповнюється псевдовипадковою послідовністю бітів;
- визначення вектора ініціалізації h_0. У разі ключового хешування вектор ініціалізації визначається з ключа, інакше як вектор ініціалізації використовується псевдовипадкове число;
- знаходження примітивних елементів $s^{(1)}, s^{(2)}, ..., s^{(q)}$ за модулями $p^{(1)}, p^{(2)}, ..., p^{(q)}$ відповідно;
- ітеративна обробка даних за формулою:

$$\begin{cases} h_i^{(1)} = \left(s^{(1)}\right)^{x_i^{(1)}} \bmod p^{(1)}; \\ h_i^{(2)} = \left(s^{(2)}\right)^{x_i^{(2)}} \bmod p^{(2)}; \\ ... \\ h_i^{(q)} = \left(s^{(q)}\right)^{x_i^{(q)}} \bmod p^{(q)}; \\ x_i^{(1)} = h_{i-1}^{(1)} \oplus h_{i-1}^{(2)} \oplus ... \oplus h_{i-1}^{(q)} \oplus r^{(1)} \oplus m_i^{(1)}; \\ x_i^{(2)} = h_{i-1}^{(1)} \oplus h_{i-1}^{(2)} \oplus ... \oplus h_{i-1}^{(q)} \oplus r^{(2)} \oplus m_i^{(2)}; \\ ... \\ x_i^{(q)} = h_{i-1}^{(1)} \oplus h_{i-1}^{(2)} \oplus ... \oplus h_{i-1}^{(q)} \oplus r^{(q)} \oplus m_i^{(q)}; \end{cases} \quad (7)$$

- формування хеш-значення повідомлення шляхом конкатенації вихідних хеш-значень, отриманих у кожному з каналів після обробки останнього *l*-го блоку даних $h = h_l^{(1)} \| h_l^{(2)} \| ... \| h_l^{(q)}$.

Розглянуто різні варіанти модифікації даного методу, які базуються на різних конструкціях багатоканального хешування, а також зав'язуванні каналів за допомогою операції множення, замість операції додавання за модулем 2.

Аналіз природних для універсального мікропроцесора операцій показав, що для реалізації функції ущільнення у методах багатоканального керованого хешування доцільно використовувати додавання за модулем 2 ($\oplus$), інвертування ($\sim$), логічне множення ($\wedge$), логічне додавання ($\vee$) та циклічний зсув на *u* бітів праворуч $>>> u$ (параметр *u* змінний). Запропоновано функції ущільнення такого виду:

$$h_i^{(j)} = \left(m_i >>> u_i^{(j)(m1)} \wedge h_{i-1}^{((j+1) \bmod q)} >>> u_i^{(j)(h1)}\right) \oplus \\ \oplus \left(\sim m_i >>> u_i^{(j)(m1)} \wedge h_i^{((j-1) \bmod q)} >>> u_i^{(j)(h2)}\right); \quad (8)$$

$$h_i^{(j)} = \left(m_i >>> u_i^{(j)(m1)} \wedge h_{i-1}^{((j+1) \bmod q)} >>> u_i^{(j)(h1)}\right) \oplus \\ \oplus \left(m_i >>> u_i^{(j)(m1)} \wedge h_i^{((j-1) \bmod q)} >>> u_i^{(j)(h2)}\right) \oplus \\ \oplus \left(h_{i-1}^{((j+1) \bmod q)} >>> u_i^{(j)(h1)} \wedge h_i^{((j-1) \bmod q)} >>> u_i^{(j)(h2)}\right), \quad (9)$$

де $v_i^{(j)} = u_i^{(j)(m1)} \| u_i^{(j)(h1)} \| u_i^{(j)(h2)}$.

У ході досліджень було визначено, що вибір методу формування векторів керування залежить від параметрів довжини вектора керування n_v та довжини проміжних хеш-значень, отриманих в одному каналі, n/q (де *n* – довжина вихідного хеш-значення).

Запропоновано метод формування векторів керування, який передбачає виконання таких дій:

- об’єднання в блоки аргументів функції формування вектора керування (проміжних хеш-значень) за допомогою конкатенації. Якщо при конкатенації чергового проміжного хеш-значення результат на $n/q-\beta$ (де β – константа) бітів більший за довжину вектора керування n_v, то це проміжне хеш-значення розділяється на дві частини довжиною β та $n/q-\beta$ бітів. Частина проміжного хеш-значення довжиною β бітів об’єднується з результатом конкатенації аргументів, а частина довжиною $n/q-\beta$ бітів бере участь у формуванні наступного блоку аргументів;

- додавання значень отриманих блоків за модулем 2.

Даний метод формалізується так:

$$v_i^{(j)} = \left(h_{i-1}^{(j+x_1)} \| h_{i-1}^{(j+x_2)} \| \ldots \| h_{i-1}^{(j+x_\alpha)} \| \overbrace{h_{i-1}^{(j+x_\alpha+1)}}^{\beta} \right) \oplus$$
$$\oplus \left(\underbrace{h_{i-1}^{(j+x_\alpha+1)}}_{n/q-\beta} \| h_{i-1}^{(j+x_{\alpha+2})} \| \ldots \right) \oplus \ldots \quad , \tag{10}$$

де $\overbrace{h_{i-1}^{(j+x_\alpha+1)}}^{\beta}$ – старші β бітів змінної $h_{i-1}^{(j+x_\alpha+1)}$;

$\underbrace{h_{i-1}^{(j+x_\alpha+1)}}_{n/q-\beta}$ – молодші ($n/q-\beta$) бітів змінної $h_{i-1}^{(j+x_\alpha+1)}$.

В ході досліджень розглянуто модифікації даного методу формування векторів керування, які дозволяють формувати вектор керування за меншу кількість операцій, однак їх застосування можливе при накладанні обмежень на параметри багатоканального хешування.

Методи багатоканального керованого хешування пропонується створювати, використовуючи комбінування підходів до формування вектора керування та функцій ущільнення, описані вище. Те, що вектор керування формується залежно від проміжних хеш-значень, отриманих на попередній ітерації, та те, що відбувається керування параметрами операції циклічного зсуву, дозволяє досягти лавинного ефекту без повторень перетворень. Тому в методах багатоканального керованого хешування пропонується не використовувати багатораундову обробку кожного блоку даних. Це суттєво відрізняє методи, що пропонуються автором від відомих методів хешування. Саме це є одним з факторів зменшення часу хешування при використанні пропонованих методів.

Оскільки конструкції багатоканального керованого хешування передбачають наявність затримки у поширенні впливу каналів один на одного, то у методах багатоканального керованого необхідно передбачити додаткові ітерації для реалізації поширення впливу проміжних хеш-значень, отриманих після обробки останнього l-го блоку даних m_l в кожному каналі, на всі інші канали. Для цього пропонується доповнити повідомлення псевдовипадковими числами, кількість яких дорівнює кількості ітерацій затримки, що для методів багатоканального керованого хешування визначається за такою формулою:

$$\xi = \frac{q}{k+\phi}. \tag{11}$$

Наприклад, метод багатоканального керованого хешування $MPH_q(4;1;0;1;\phi)$ передбачає виконання таких дій:

- розбивання повідомлення M на блоки рівної довжини. Якщо довжина повідомлення $\|\mathrm{M}\|$ не кратна довжині блоку даних $\|m_i\|$, то повідомлення попередньо доповнюється псевдовипадковою послідовністю бітів;

- визначення вектора ініціалізації h_0 на основі ключа або псевдовипадковим чином (залежно від виду хешування – ключове або безключове, відповідно);

- доповнення повідомлення блоками даних у кількості ξ, що обчислюється за формулою (11);

- ітеративна обробка блоків даних за такою формулою:

$$\begin{aligned} h_i^{(j)} = &\left(m_i >>> u_i^{(j)(m1)} \wedge h_i^{((j+1) \bmod q)} >>> u_i^{(j)(h1)}\right) \oplus \\ &\oplus \left(\sim m_i >>> u_i^{(j)(m1)} \wedge h_i^{((j+2+q/4) \bmod q)} >>> u_i^{(j)(h2)}\right) \oplus \\ &\oplus \left(m_i >>> u_i^{(j)(m2)} \vee h_i^{((j+3+2q/4) \bmod q)} >>> u_i^{(j)(h3)}\right) \oplus \\ &\oplus \left(\sim m_i >>> u_i^{(j)(m2)} \vee h_i^{((j+4+3q/4) \bmod q)} >>> u_i^{(j)(h4)}\right) \end{aligned}; \quad (12)$$

- формування хеш-значення повідомлення шляхом конкатенації вихідних хеш-значень, отриманих у кожному з каналів $h = h_l^{(1)} \| h_l^{(2)} \| \ldots \| h_l^{(q)}$ по завершенню останньої l-ї ітерації.

Одержані теоретичні оцінки кількості операцій, необхідних для реалізації методів багатоканального керованого хешування показали, що вибір того чи іншого методу для використання в комп'ютерних системах та мережах залежить від особливостей конкретних задач, зокрема, від довжини даних, які необхідно хешувати. Рекомендується для повідомлень великої довжини використовувати методи багатоканального керованого хешування, які мають більшу затримку в поширенні впливу каналів один на одного, а для хешування повідомлень малої довжини – з малою затримкою або без затримки.

У четвертому розділі дисертаційної роботи наводиться опис програмних засобів, розроблених мовою ANSI C відповідно до вимог, які висуваються до хеш-функцій, що є конкурсантами на стандарт хешування SHA-3. Дані програмні засоби адаптовані для виконання тестування Known Answer Tests, а також визначення швидкості хешування. Тестування відбувалося на комп'ютері з такою конфігурацією: операційна система – MS Windows XP SP3, процесор Intel Pentium IV 3.0 ГГц; оперативна пам'ять – 3,25 Гбайт. Аналіз результатів Known Answer Tests не виявив виродження хеш-значень, що свідчить про наявність практичної стійкості хешування. Дослідження швидкості хешування за допомогою розроблених програмних засобів багатоканального керованого хешування показало, що вона перевищує від 3,1 до 16 разів швидкість хешування засобами, які є фіналістами конкурсу на стандарт хешування SHA-3 при хешування повідомлень довжиною більше 10 Кбайт. Це пояснюється опосередкованим зав'язуванням каналів та відсутністю раундових перетворень в запропонованим методах багатоканального хешування.

Наведено опис програмних засобів у вигляді динамічних бібліотек, що реалізують методи багатоканального керованого хешування та методи багатоканального хешування на основі операції піднесення до степеня за модулем простого числа, розроблених мовою C++, призначених для інтегрування до різних комп'ютерних систем. Програмні бібліотеки для багатоканального керованого хешування впроваджені при парольній автентифікації користувачів комп'ютерної системи ТОВ "ВІАТЕЛ", яка відбувається перед наданням їм доступу до бази даних. Діяльність декількох користувачів підприємства ТОВ "ВІАТЕЛ", пов'язана з періодичним звертанням до бази даних, причому коло працівників, які мають право вносити зміни до цієї бази обмежено. Відповідно розроблений програмний засіб використовується для хешування паролів користувачів, які мають право вносити зміни до бази даних, та порівнянням його з хеш-значенням пароля відповідного користувача, яке зберігається в комп'ютерній системі.

Програмний засіб для багатоканального хешування на основі операції піднесення до степеня за модулем простого числа впроваджено в комп'ютерній системі ПП "ВІНБУДІЗОЛ"

при перевірці автентичності даних. До критичних даних, що зберігаються в комп'ютерній системі ПП "ВІНБУДІЗОЛ" дописуються хеш-значення, яке перевіряється перед початком оброблення цих даних та замінюється на нове по завершенню роботи з даними.

Розроблено структури спеціалізованих процесорів для багатоканального хешування на основі операції піднесення до степеня за модулем простого числа. Один з варіантів структури наведено на рис. 3. Тут кожен з q каналів хешування складається з чотирьох регістрів, блока додавання за модулем 2 та блока піднесення до степеня за модулем. Зав'язування каналів реалізується за допомогою блока додавання за модулем 2 з номером q+1 та зворотного зв'язку.

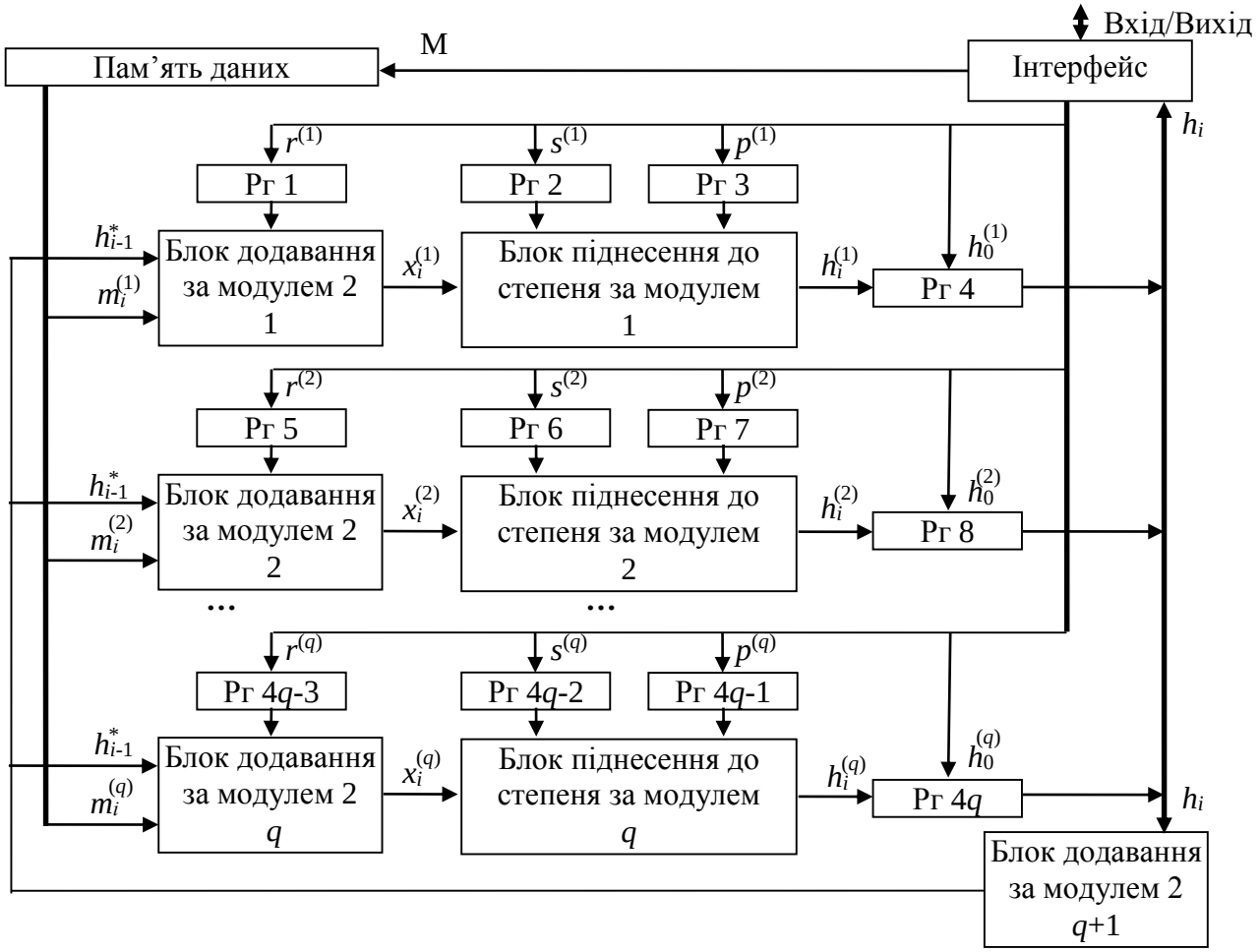

Рисунок 3 – Структура спеціалізованого процесора для багатоканального хешування на основі операції піднесення до степеня за модулем простого числа

На рис. 4 зображено узагальнену структуру спеціалізованого процесора для багатоканального керованого хешування.

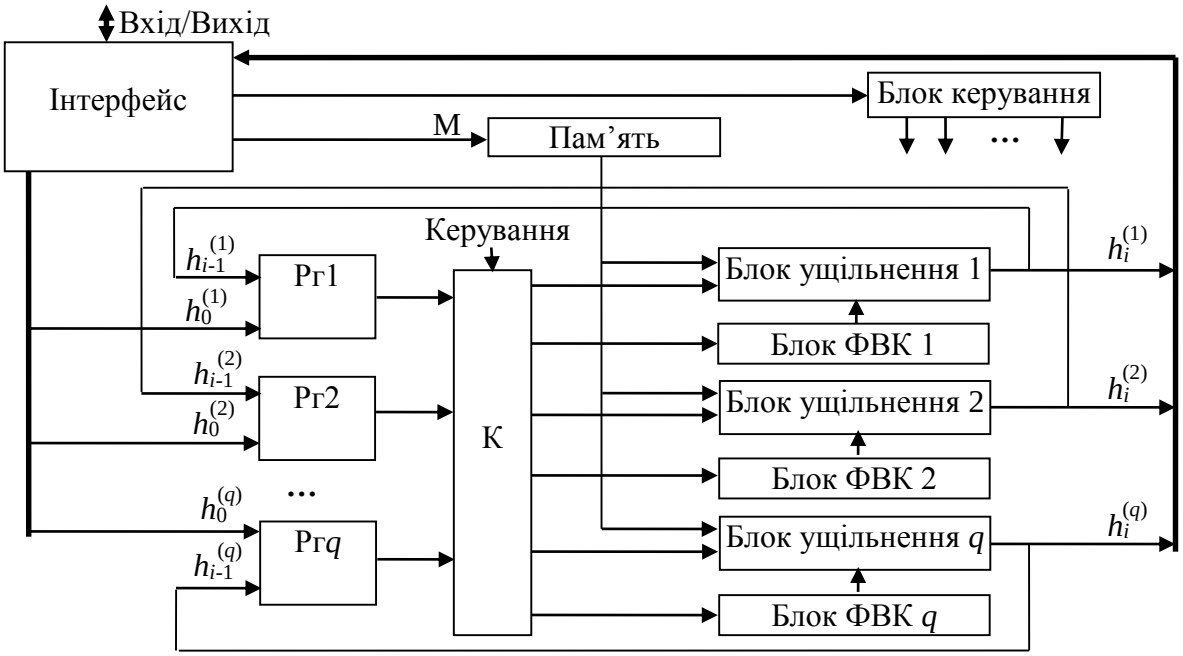

Рисунок 4 – Узагальнена структура спеціалізованого процесора для багатоканального керованого хешування

Ця структура складається з q каналів, кожен з яких містить регістр, блок ущільнення та блок формування вектора керування (ФВК), а також з блока керування, який визначає правило зав'язування каналів за допомогою комутатора К. Для інтегрування до комп'ютерних систем в структурах спеціалізованих процесорів передбачені інтерфейси.

Аналіз різних реалізацій спеціалізованих процесорів показав, що для практичної реалізації за критерієм швидкості кращими є 64-х розрядні процесори.

ВИСНОВКИ

У дисертаційній роботі розв'язана важлива науково-технічна задача підвищення швидкості автентифікації даних та користувачів в комп'ютерних системах за допомогою створення нових методів та засобів хешування на основі багатоканальних конструкцій хешування, що забезпечують розпаралелення обчислень.

Основні результати роботи є такими:

1. Проведений аналіз відомих атак на хеш-функції показав, що найбільш небезпечними для розпаралелених процесів формування хеш-значень є загальні атаки, що використовують мультиколізії, тому при побудові багатоканальних конструкцій, в першу чергу, необхідно врахувати саме ці атаки, щоб забезпечити потрібну крипостійкість хеш-функцій. Основною причиною вразливості відомих конструкцій багатоканального хешування до загальних атак, що використовують мультиколізії, є невисокий ступінь залежності результатів хешування кожного з каналів від результатів хешування інших каналів.

2. Вперше запропоновано узагальнену модель ітерацій (конструкцію) багатоканального хешування, яка передбачає зав'язування каналів різними способами, що забезпечує побудову хеш-функцій, стійких до загальних атак, які використовують мультиколізії. Така модель забезпечує формалізований опис відомих методів хешування і надає можливість побудувати нові методи хешування, задаючи певні параметри цієї моделі.

3. Отримали подальший розвиток конструкції багатоканального хешування, стійкі до загальних атак на основі мультиколізій, із безпосереднім зав'язуванням всіх каналів один з одним, які, порівняно з відомими, передбачають наявність q ($q > 2$) каналів у конструкції (для вихідного хеш-значення довжиною 256 бітів $q \in \{4; 8; 16; 32\}$) та однакові довжини проміжного та вихідного хеш-значеннь.

4. Вперше запропоновано конструкції багатоканального хешування з опосередкованим зав'язування всіх каналів один з одним, які забезпечують таку саму стійкість до загальних атак, що використовують мультиколізії, як конструкції багатоканального хешування з безпосереднім зав'язуванням каналів один з одним, проте забезпечують підвищення швидкості процесу хешування від 1,4 до 16 раз.

5. Удосконалено методи багатоканального хешування на основі операції піднесення до степеня за модулем простого числа, які за рахунок зав'язування каналів дозволяють виконувати операцію піднесення до степеня для чисел в q раз меншої розрядності порівняно з відомими, що забезпечує збільшення швидкості хешування у q раз. Для реалізації даних методів розроблені структури спеціалізованих процесорів.

6. Особливість запропонованих і удосконалених конструкцій полягає в тому, що передбачається можливість зміни способів зав'язування каналів і алгоритмів ітерацій процесу хешування за допомогою вектора керування. Тому в роботі отримали подальшого розвитку методи формування вектора керування, які забезпечують розробку програмних й апаратних засобів для хешування даних з різними характеристиками стійкість/швидкість. Використовуючи дані методи, розроблено програмні засоби багатоканального керованого хешування, які дозволяють отримати вихідні хеш-значення довжини, кратної розрядності обчислювальної платформи – 16/32/64 біти, а також реалізувати багатоканальне хешування із різними способами зав'язування каналів. Крім того, розроблено структури спеціалізованих процесорів, що реалізують методи багатоканального керованого хешування.

7. Експериментальні дослідження показали практичну стійкість розроблених програмних засобів, що реалізуються методи багатоканального керованого хешування, до набору тестів Known Answer Tests, які використовуються при оцінюванні сучасних хеш-функцій. Крім того, за допомогою даних програмних засобів визначено оцінки швидкості хешування даних різної довжини, які свідчать про збіжність теоретичних оцінок з експериментальними. Порівняння запропонованих методів з відомими за показником швидкості хешування показало, що збільшення швидкості при реалізації багатоканального керованого хешування на основі запропонованих методів досягається за рахунок можливості розпаралелення обчислень та відсутності в цих методах повторень раундових перетворень.

8. Результати проведених досліджень впроваджено в ТОВ "ВІАТЕЛ" при парольній автентифікації користувачів комп'ютерної системи, ПП "ВІНБУДІЗОЛ" при автентифікації даних, що зберігаються в комп'ютерній системі підприємства, а також у навчальний процес у Вінницькому національному технічному університеті на кафедрі захисту інформації.

Таким чином основні наукові та практичні результати, отримані при розв'язанні сформульованих задач досліджень, свідчать про досягнення мети дисертаційної роботи.

ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Баришев Ю. В. Підходи до побудови швидких алгоритмів хешування / В. А. Лужецький, Ю. В. Баришев // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – №. 2 (19). – 2009. – С. 57-65.

2. Баришев Ю. В. Криптографічні примітиви для реалізації керованого хешування / В. А. Лужецький, Ю. В. Баришев // Вісник Вінницького політехнічного інституту. – №1. – 2011. – С. 108-111.

3. Баришев Ю. В. Методи формування векторів керування для керованого багатоканального хешування даних. / В. А. Лужецький, Ю. В. Баришев, О. В. Оводенко. // Наукові праці Донецького національного технічного університету. Серія: "Обчислювальна техніка та автоматизація". – №21(183). – 2011. – С. 103-108.

4. Баришев Ю. В. Апаратні засоби для реалізації багатоканального керованого хешування. / В. А. Лужецький, Ю. В. Баришев. // Системи обробки інформації. – №3. – 2011. – С. 130-133.

5. Баришев Ю. В. Методи та засоби паралельного керованого хешування / В. А. Лужецький, Ю. В. Баришев // Наукові праці ВНТУ. – №2. – 2011. – 5 с. – Режим доступу до статті : http://www.nbuv.gov.ua/e-journals/VNTU/2011_2/2011-2.files/uk/11valpch_ua.pdf

6. Баришев Ю. В. Узагальнена модель стійкого паралельного хешування / В. А. Лужецький, Ю. В. Баришев // Проблеми й перспективи розвитку ІТ-індустрії в Україні. Матеріали Першої Міжнародної науково-технічної конференції. м. Харків, 18-19 листопада 2009 року. – Харків: ХНЕУ, 2009. – С. 166-167.

7. Баришев Ю. В. Багатоканальне кероване хешування даних/ В. А. Лужецький, Ю. В. Баришев // Праці ІІІ Міжнародної науково-практичної конференції "Обробка сигналів і негауссівських процесів", присвяченої пам'яті професора Ю. П. Кунченка : Тези доповідей. – Черкаси: ЧДТУ, 2011. – С. 204 - 206.

8. Баришев Ю. В. Методи побудови швидких алгоритмів хешування / Ю. В. Баришев // Методи та засоби кодування, захисту й ущільнення інформації. Тези доповідей другої Міжнародної науково-практичної конференції. м. Вінниця, 22-24 квітня 2009 року. – Вінниця: ВНТУ, 2009. – С. 138-139.

9. Баришев Ю. В. Методи та програмні засоби керованого багатоканального хешування. / Ю. В. Баришев // Методи та засоби кодування, захисту й ущільнення інформації. Тези доповідей Третьої Міжнародної науково-практичної конференції. м. Вінниця, 20-22 квітня 2011 року. – Вінниця: ВНТУ, 2011. – С. 100-101.

10. Баришев Ю. В. Підхід до хешування, що стійке до аналізу зловмисника / Ю. В. Баришев // Системи обробки інформації. – №3(84). – 2010. – С. 99-100.

11. Баришев Ю. Алгоритм паралельного хешування даних / Ю. Баришев // Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2009). Тези Четвертої Міжнародної науково-технічної конференції. м. Вінниця, 8-10 жовтня 2009 року. Частина 1. – Вінниця: ВНТУ, 2011. – С. 9

12. Баришев Ю. Структура спеціалізованого криптографічного процесора для керованого хешування / Юрій Баришев // Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2011): матеріали V Міжнародної науково-технічної конференції, м. Вінниця, 19-21 травня 2011 р. – Вінниця: ВНТУ, 2011. – С. 169-170. – ISBN 978-966-641-411-6.

13. Патент України на корисну модель № 41313 МПК G 09 C 1/00. Спосіб паралельного ключового хешування теоретично доведеної стійкості / Лужецький В. А., Баришев Ю. В., Дмитришин О. В.; заявник та патентовласник Вінницький національний технічний університет. – №u200900489; заявл. 23.01.09; опубл. 12.05.09, Бюл. №9.

14. Патент України на корисну модель № 48279 МПК G 09 C 1/00. Спосіб паралельного ключового хешування / Лужецький В. А., Баришев Ю. В.; заявник та патентовласник Вінницький національний технічний університет. – №u200909901; заявл. 28.09.09; опубл. 10.03.10, Бюл. №5.

15. Патент України на корисну модель № 54813 МПК G 09 C 1/00. Спосіб паралельного ключового хешування / Лужецький В. А., Баришев Ю. В.; заявник та патентовласник Вінницький національний технічний університет. – №u201006156; заявл. 21.05.10; опубл. 25.11.10, Бюл. №22.

АНОТАЦІЯ

Баришев Ю. В. Методи та засоби швидкого багатоканального хешування даних в комп'ютерних системах. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – Комп'ютерні системи та компоненти. – Вінницький національний технічний університет, Вінниця, 2012.

Дисертаційна робота присвячена розробці та удосконаленню методів та засобів багатоканального хешування в комп'ютерних системах.

Запропоновано узагальнену модель ітерацій (конструкцію) багатоканального хешування. Аналіз цієї конструкції дозволив визначити параметри хешування, які впливають на стійкість хешування до загальних атак на основі мультиколізій. Запропоновано конструкції багатоканального хешування, які дозволили розробляти методи багатоканального хешування на основі перетворень з керованими параметрами та на основі операції піднесення до степеня за модулем простого числа. Дані методи реалізовані у вигляді програмних та апаратних засобів багатоканального хешування даних в комп'ютерних системах. Тестування програмних засобів багатоканального керованого хешування дозволило підтвердити практичну стійкість запропонованих методів хешування, а також показало збільшення швидкості хешування порівняно з засобами фіналістів конкурсу на новий стандарт хешування SHA-3.

Ключові слова: хешування, багатоканальність, конструкції, піднесення до степеня за модулем, керовані перетворення, автентифікація даних та користувачів.

АННОТАЦИЯ

Барышев Ю. В. Методы и средства быстрого многоканального хеширования данных в компьютерных системах. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 – Компьютерные системы и компоненты. – Винницкий национальный технический университет, Винница, 2012.

Диссертационная работа посвящена разработке и усовершенствованию средств многоканального хеширования в компьютерных системах.

Предложена обобщенная модель итераций (конструкция) многоканального хеширования данных. На основе анализа параметров этой конструкции определено, что на стойкость многоканальных конструкций влияет количество промежуточных хеш-значений, полученных в других каналах, которые участвуют в формирование следующего промежуточного хеш-значения в данном канале. Это свойство многоканального хеширования было учтено при разработке новых конструкций хеширования. В частности, были предложены конструкции, которые обеспечивают связь каналов хеширования посредством использования промежуточных хеш-значений, полученных в других каналах, в функциях сжатия. Предложены конструкции многоканального управляемого хеширования, обеспечивающие связь каналов при помощи векторов управления. Для уменьшения количества аргументов в функциях сжатия и формирования векторов управления, а как следствие увеличения скорости хеширования, предложены конструкции хеширования, обеспечивающие распространение влияния каналов друг на друга с определенной задержкой. Для усложнения предварительной подготовки к атаке в некоторых конструкциях предусматривается наличие псевдослучайного числа и числа уже обработанных данных сообщения.

Разработаны методы многоканального хеширования на основе операции возведения в степень по модулю простого числа, которые позволяют распараллелить процесс хеширования. Для обеспечения связи каналов предложено использовать операции "исключающего или" и умножения.

Для реализации конструкций многоканального управляемого хеширования выбраны базовые операции: "исключающее или", инверсия, логическое умножение, логическое сложения, циклический сдвиг на заданное количество бит вправо. На основе этих операций разработаны функции сжатия, предусматривающие наличие управления количеством разрядов, на которое циклически сдвигаются аргументы функции сжатия. Учитывая особенности этих преобразований, разработаны методы формирования вектора управления, позволяющие адаптироваться к изменению параметров многоканального хеширования. Комбинируя методы формирования вектора управления и функции сжатия, разработаны методы многоканального управляемого хеширования. Особенностью этих методов является отсутствие раундовых повторений преобразований, что обуславливается возможностью

достижения лавинного эффекта при помощи операции циклического сдвига, определяющегося на основе промежуточных хеш-значений, полученных в результате обработки предыдущего блока данных.

Методы многоканального управляемого хеширования реализованы в виде программных средств, что позволило подтвердить их практическую стойкость набором тестов Known Answer Tests, использующихся при исследовании конкурсантов на новый стандарт хеширования SHA-3. Кроме того, сравнение скорости хеширования разработанных программных средств со скоростью средств финалистов этого конкурса, показало, что разработанные при диссертационном исследовании средства быстрее известных.

Для интегрирования в компьютерные системы программных средств на основе предложенных методов хеширования они были реализованы в виде динамических библиотек, использование которых позволило внедрить результаты исследований. Также для возможности интегрирования результатов исследования в компьютерные системы были разработаны структуры специализированных процессоров для многоканального хеширования на основе операции возведения в степень по модулю простого числа и на основе управляемых операций.

Ключевые слова: хеширование, многоканальность, конструкции, возведение в степень по модулю, управляемые преобразования, аутентификация данных и пользователей.

ABSTRACT

Baryshev Y. V. Methods and means for rapid multipipe data hashing within computer systems. – Manuscript.

Thesis for the candidate degree of technical sciences on the speciality 05.13.05 – Computer systems and components. – Vinnytsia National Technical University, Vinnytsia, 2012.

The dissertation is devoted to the development and improvement of methods and means of multipipe hashing within computer systems.

The generalized model of hash iterations (the hash construction) is proposed. The analysis of the construction allows to determine hash parameters, that influence the hash resistance to the generic attacks based on the multicollisions. Multipipe hash constructions, which allow to design methods of multipipe hashing based on the driven operations and ones based on modulo prime number exponentiation are proposed. These methods are implemented as software and hardware means for multipipe hashing within computer systems. Testing of the software means of multipipe driven hashing allows to prove the practical durability of the proposed methods, and it also shows increasing of hashing rate comparatively with means of new hashing standard SHA-3 competition finalists.

Key words: hashing, miltipipeness, constructions, modulo prime number exponentiation, driven operations, data and user authentification.

Підписано до друку 13.02.2012 р. Формат 60x84 1/16.
Тираж 100 прим. Зам. № 2012-018
Віддруковано в інформаційно-видавничому центрі
Вінницького національного технічного університету
21021, Вінниця, вул. Хмельницьке шосе, 95. Тел.: (0432) 59-81-59