Міністерство освіти і науки, молоді та спорту України
Харківський національний університет радіоелектроніки

БОЙКО АРТЕМ ОЛЕКСАНДРОВИЧ

УДК 681.3.06

МЕТОДИ ПОБУДУВАННЯ КОДІВ АВТЕНТИФІКАЦІЇ ПОВІДОМЛЕНЬ З ПІДВИЩЕНОЮ ШВИДКОДІЄЮ

05.13.21 – Системи захисту інформації

Автореферат дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2012

Дисертацією є рукопис.

Робота виконана в Харківському національному університеті радіоелектроніки Міністерства освіти і науки, молоді та спорту України.

Науковий керівник: доктор технічних наук, професор **Горбенко Іван Дмитрович**, завідувач кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, м. Харків

Офіційні опоненти: доктор технічних наук, професор **Максимович Володимир Миколайович,** Інститут комп'ютерних технологій, автоматики та метрології Національного університету "Львівська політехніка, м. Львів, завідуючий кафедрою безпеки інформаційних технологій

кандидат технічних наук, доцент **Єсін Віталиі Іванович** Харківський національний університет імені Каразіна, доцент кафедри безпеки інформаційних систем і технологій

Захист відбудеться «__» _____ 2012 р. о __ годині на засіданні спеціалізованої вченої ради К 64.052.05 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14; т. (057) 702-10-16.

З дисертацією можна ознайомитись у бібліотеці Харківського національного університету радіоелектроніки (просп. Леніна, 14).

Автореферат розісланий «__» _____ 2012 р.

Вчений секретар
спеціалізованої вченої ради І. В. Лисицька

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Функції контролю цілісності та автентичності можуть бути забезпечені або за рахунок використання електронного цифрового підпису або за рахунок кодів автентифікації повідомлень. Вибір на користь одного з двох перелічених методів здійснюється на основі моделі загроз та вимог по швидкодії. Алгоритми електронного цифрового підпису, як правило, повільніші, ніж алгоритми вироблення кодів автентифікації повідомлень, однак дозволяють крім послуг цілісності та автентичності забезпечити ще і послугу неспростовності, реалізуючи таким чином модель взаємної недовіри і взаємного захисту. Коди автентифікації повідомлень, мають більшу швидкодію, але не забезпечують послуги неспростовності, і для їх використання відправник і отримувач повинні довіряти один одному.

В термінах національних критеріїв захищеності інформації в комп’ютерних системах від несанкціонованого доступу використання кодів автентифікації повідомлень дозволяє реалізувати послугу НА-1 “Базова автентифікація відправника”, а використання електронного цифрового підпису — послугу НА-2 “Автентифікація відправника з підтвердженням”, яка є ієрархічно вищою, ніж НА-1, і відрізняється наявністю вимоги, що використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження автентичності об'єкта незалежною третьою стороною .

Однак, оскільки вартість системи захисту інформації не повинна перевищувати втрати від порушення основних властивостей безпеки інформації (принцип економічної доцільності) і має бути мінімізована при проектуванні, то якщо потреби у можливості однозначного підтвердження автентичності об'єкта незалежною третьою стороною немає, то перевагу слід віддати кодам автентифікації повідомлень, оскільки більша швидкодія алгоритмів вироблення кодів автентифікації повідомлень дозволяє зменшити вимоги до обчислювальної потужності пристроїв, які реалізують ці алгоритми.

Випадки відсутності потреби у можливості однозначного підтвердження автентичності об'єкта незалежною третьою стороною виникають, наприклад, при проектуванні розподілених комп'ютерних систем, усі компоненти яких належать одному власнику і обмінюються інформацією через незахищене середовище, а саме в апаратурі утворення віртуальних приватних мереж, апаратурі приймання показів з віддалених датчиків через незахищене середовище, засобах віддаленого керування тощо.

Зв’язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана в рамках НДР "«Аналіз вимог міжнародного

стандарту “ISO/IEC 18032 – Інформаційні технології – Методи захисту – Генерація простих чисел ” та рекомендації щодо його застосування в Україні» (шифр “Гармонія”)", госпдоговірної НДР №11-06 від 01.03.2011р."Розробка методів, комплексів та засобів інфраструктури відкритих ключів (ІВК) для національних та міжнародних інформаційно-телекомунікаційних систем та інформаційних технологій" (ДР № 0111U002634), держбюджетної НДР № 262-1 “Розвиток, стандартизація, уніфікація,удосконалення та впровадження інфраструктури відкритих ключів, включаючи національну систему ЕЦП, на національному та міжнародному рівнях відкритих ключів”, держбюджетної НДР № 237-1 “Розвиток, стандартизація, уніфікація, удосконалення та впровадження інфраструктури відкритих ключів, включаючи національну систему ЕЦП, на національному та міжнародному рівнях відкритих ключів”.у яких здобувач був виконавцем.

Мета та задачі дослідження. *Метою досліджень* є аналіз якості існуючих, удосконалення та розробка нових методів побудування кодів автентифікації повідомлень, які б мали більшу, у порівнянні з існуючими, швидкодію при збереженні заданого рівня стійкості.

Для досягнення поставленої мети в роботі необхідно вирішити наступні задачі:

1. Визначити критерії і показникі оцінки кодів автентифікації повідомлень на основі моделі Сіммонса та результатів, отриманих в ході NIST SHA-3 Competition.

2. Розробити і обґрунтувати методику порівняння кодів автентифікації повідомлень на основі формальних методів підтримки прийняття рішень.

3. Провести порівняльний аналіз відомих підходів до побудування кодів автентифікації повідомлень і визначити фактори, які обмежують швидкодію відомих алгоритмів вироблення кодів автентифікації повідомлень і які впливають на стійкість цих алгоритмів.

3. Удосконалити метод вироблення кодів автентифікації повідомлень на основі обчислення значення від полінома над скінченим полем шляхом використання паралельних обчислень. Провести оптимізацію параметрів удосконаленого методу за показниками ефективності використання паралельних обчислень та ефективності використання кеш-пам'яті процесора.

4. Розробити метод вироблення кодів автентифікації повідомлень на основі обчислення значення від полінома над кільцем цілих чисел за модулем 2^n .

5. Розробити метод вироблення кодів автентифікації повідомлень на основі обчислення значення від полінома над кільцем цілих чисел за модулем 2^n та каскадної конструкції.

6.Оптимізувати параметри для каскадної конструкції за показниками ефективності використання паралельних обчислень та ефективності використання кеш-пам'яті процесора.

7. Розробити математичні та програмні моделі, що реалізують запропоновані методи вироблення кодів автентифікації повідомлень.

8. Оцінити властивості та характеристики розроблених методів, а також зробити порівняльний аналіз розроблених методів по критеріям стійкості та складності (швидкодії).

Об'єктом дослідження є процеси автентифікації даних, які ґрунтуються на використанні універсальних функцій гешування на основі обчислення значення полінома в скінченних полях та кільцях.

Предметом досліджень є методи автентифікації даних з заданим рівнем стійкості на основі обчислення значення полінома в скінченних полях та кільцях, які дозволяють виконати вимоги до кодів автентифікації повідомлень, в тому числі обов'язково колізійна стійкість, складність знаходження прообразу та другого прообразу, висока швидкодія, простота реалізації тощо.

Методи досліджень: методи теорії ігор та теорії інформації – при дослідженні математичної моделі системи з автентифікацією даних та обґрунтування вимог до методів автентифікації даних; методи теорії полів і груп, методи теорії ймовірностей та математична статистика – при визначені ймовірності появи слабких ключів; методи теорії паралельних обчислень – при побудуванні та оцінці властивостей паралельних алгоритмів гешування; методи системного аналізу – при порівнянні існуючих методів автентифікації повідомлень; програмне моделювання – при реалізації процесів універсального гешування.

Наукова новизна одержаних результатів. У роботі одержано такі нові наукові результати.

1. Удосконалено метод універсального гешування на основі обчислення значення полінома над скінченним полем, який відрізняється від прототипу тим, що передбачає гешування повідомлення у n паралельних потоків суперблоками з n блоків з деяким ключем x з наступним гешуванням отриманих проміжних геш-значень з ключем $x^n mod p$, що дозволило збільшити швидкодію у n разів, де n - число потоків.

2. Вперше запропоновано метод універсального гешування, який будується на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l, що дозволяє забезпечити імовірність колізії $\frac{1}{2^{l-1}}$ незалежно від довжини повідомлення, збільшити швидкодію приблизно у 2,5 разів у порівнянні з

функцією гешування на основі обчислення значення полінома над скінченним полем, забезпечити невразливість до атак спостереження за часом виконання.

3. Вперше запропоновано метод універсального гешування, який будується на основі композиційної каскадної схеми і гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l на обох каскадах, що дозволяє забезпечити більшу кількість ключів, які не належать до класів слабких ключів, у порівнянні з методом універсального гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l.

Практичне значення одержаних результатів полягає у наступному:

1. Вперше запропоновано алгоритм паралельного універсального гешування на основі обчислення значення полінома над скінченним полем, який передбачає гешування повідомлення у *n* паралельних потоків суперблоками з *n* блоків з деяким ключем x з наступним гешуванням отриманих проміжних геш-значень з ключем $x^n \bmod p$.

2. Вперше запропоновано алгоритм універсального гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l, який використовує лише перетворення над кільцем цілих чисел модулю 2^l замість перетворень у полях (Акт впровадження).

3. Вперше запропоновано паралельний алгоритм універсального гешування, що реалізує композиційну каскадну схему і гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l на обох каскадах (Акт впровадження).

4. Розроблені комплекси програмного забезпечення (програмні моделі), що реалізують розроблені методи універсального гешування в кільці цілих чисел за модулем 2^l, та проведене програмне моделювання, на основі яких отримані властивості швидкодії алгоритмів (Акт впровадження).

5. Отримано ряд аналітичних співвідношень, які дозволяють зробити оцінки ймовірностей вибору слабких ключів для універсальних функцій гешування на основі обчислення значення полінома над скінченними полями та над кільцем цілих чисел модулю 2^l.

Особистий внесок здобувача. Основні результати отримані здобувачем самостійно [1]. У роботах, що написані у співавторстві, автору належить: [2] – аналіз причин конкурсу NIST SHA-3 Competition; [3] – обгрунтування нових критеріїв порівняння функцій гешування, які враховують можливість використання паралельних обчислень; [5] – аналіз сучасного стану процесів стандартизації функцій гешування в Україні; [6] – аналіз паралельних архітектур функцій гешування з високою швидкодією; [7] – отимізація деревовидної архітектури функцій гешування за показником ефективності паралельних обчислень.

Апробації результатів дисертації. Основні результати досліджень, що проведені в дисертаційній роботі, доповідалися на наступних конференціях та симпозіумах:

– Міжнародний симпозіум «Питання оптимізації обчислень (ПОО-XXXV)», присвячений 40-річчю І Симпозіуму та літньої математичної школи з питань точності й ефективності обчислювальних алгоритмів. (Кацивелі, 2009);

– Науково-практична конференція "Dependable Systems, Services & Technologies 2010" (Кіровоград, 2010);

– Научно-техническая конференция с международным участием «Компьютерное моделирование в наукоемких технологиях»(КМНТ-2010) (Харьков, 2010);

– XIII Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах» (Київ, 18-21 травня 2010 р);

– Вторая Международная научно-техническая конференция «Компьютерные науки и технологии КНиТ-2011» (Белгород, 3-5 октября 2011 г);

– Международная конференция, посвященная 50-летию механико-математического факультета «Современные проблемы математики и ее приложения в естественных науках и информационных технологиях» (Харьков, 17-22 апреля 2011);

– XV Юбилейная Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах» (Київ, 22-25 травня 2012 р).

Публікації. За результатами дисертаційної роботи опубліковано 9 статей в 5 фахових виданнях, що входять до переліків, затверджених ВАК України, 8 матеріалів і тезисів наукових конференцій.

Структура та обсяг дисертації. Дисертація складається із вступу, п’яти розділів і висновків, має загальний обсяг 150 сторінок, з яких 123 сторінки основного тексту, містить 8 рисунків, 18 таблиць, список використаних джерел із 89 найменувань на 10 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми дисертаційної роботи, сформульовано мету та задачі дослідження, розкрито наукову та практичну цінність отриманих результатів, наведені відомості щодо впровадження результатів роботи, публікацій автора та апробацію результатів роботи.

У першому розділі дисертаційної роботи наводяться результати аналізу моделі порушника, впливу властивостей функцій гешування на стійкість системи автентифікації, та визначаються вимоги до функцій гешування.

Проведений аналіз показав, що стійкість системи автентифікації визначається імовірностями реалізації наступних загроз: імперсоналізації (нав'язування хибного повідомлення отримувачу), підміни (побудування хибного повідомлення на основі перехопленого справжнього) та спуфінгу (побудування хибного повідомлення на основі r перехоплених справжніх повідомлень). Мінімальне значення імовірностей загроз досягається виконанням відправником та отримувачем наступних умов:

1) значення кодів автентифікації повідомлень повинні бути розподілені рівноімовірно;

2) вибір правила вироблення коду автентифікації повідомлень (ключа) повинен здійснюватися з дотриманням рівноімовірності і незалежності ключа від повідомлення на вході функції вироблення коду автентифікації повідомлень.

Оскільки функція вироблення коду автентифікації повідомлень є частковим випадком функції гешування, то було проаналізовано вплив характеристик стійкості функцій гешування на стійкість системи автентифікації. Було показано, що складність реалізації загрози імперсоналізації не менше, ніж складність знаходження прообразу, відновлення ключа або розширення повідомлення для функції гешування, складність реалізації загрози підміни не менше, ніж складність знаходження другого прообразу, складність реалізації загрози спуфінгу не менше, ніж складність знаходження колізії.

У результаті проведеного аналізу сформульовано основні вимоги до функцій вироблення коду автентифікації повідомлень.

У другому розділі дисертаційної роботи обґрунтовано критерії і методику порівняння функцій гешування, що використовуються для побудування кодів автентифікації повідомлень.

Критерії оцінки функцій гешування, що використовуються для побудування кодів автентифікації повідомлень, були сформульовані на основі вимог, визначених у першому розділі з урахуванням результатів NIST SHA-3 Competition та наших досліджень.

Аналіз показав, що критерії порівняння доцільно розбити на безумовні (обов'язкові до виконання) і умовні (виконанням яких можна поступитися заради виконання безумовних або інших умовних критеріїв). До безумовних критеріїв належать наступні:

1) імовірність знаходження колізій P_{col} повинна бути не вище $P_{підмін}$;

2) імовірність знаходження другого прообразу $P_{secpreim}$ повинна бути не вище $P_{підмін}$;

3) імовірність знаходження прообразу P_{preim} повинна бути не вище $P_{імперсон}$;

4) імовірність розширення повідомлення P_{ext} повинна бути не вище $P_{імперсон}$.

5) для початку роботи функція гешування не повинна потребувати передачі довжини повідомлення.

До умовних критеріїв віднесені наступні:

1) максимально досяжна швидкодія повинна бути найбільшою;

2) максимальний коефіцієнт прискорення K_{max} повинен бути найбільшим;

3) максимальна ефективність паралельних обчислень $E(N)$ при $K_N = K_{max}$ повинна бути найбільшою;

4) питома витрата пам'яті на одне ядро $RM(N)$ при $K_N = K_{max}$ повинна бути найменшою;

5) кількість інформації щодо змісту повідомлення, яку може отримати порушник по побічним каналам повинна бути найменшою.

Зважаючи на велику кількість критеріїв було запропоновано в якості основи для методики порівняння використати один з методів підтримки прийняття рішень. Перевага була надана методу оцінки вагових коефіцієнтів на основі функції втрат ефективності, тому що він, на відміну від інших методів підтримки прийняття рішень, не потребує участі експертів, а дозволяє побудувати цільову функцію лише на основі об'єктивних показників.

У третьому розділі дисертаційної роботи розглянуті властивості і обґрунтовано використання спеціально розроблених універсальних функцій гешування та сформульовано задачі для досліджень, розв'язання яких дозволить збільшити швидкодію функцій вироблення кодів автентифікації повідомлень на основі спеціально розроблених універсальних функцій гешування.

Визначення 1. Нехай $H-$ клас функцій гешування, що відображають множину A у множину B, причому $|A|>|B|$. Нехай $\delta(x,y)=1$ коли $h(x)=h(y)$ і $x \neq y$, та $\delta(x,y)=0$ у всіх інших випадках. Клас функцій гешування H називається універсальним, якщо для усіх $x,y \in A$ виконується

$$\sum_{h \in H} \delta(x,y) \leq \frac{|H|}{|B|} \qquad (1)$$

Використання універсальних функцій гешування у системах автентифікації без секретності було вперше запропоновано Стінсоном.

Розглянуті підходи до побудування універсальних функцій гешування реалізовані у наступних універсальних функціях гешування:

1) гешування Картера і Вегмана;

2) родина функцій гешування MMH;

3) родина функцій гешування NMH;

4) функція NH;

5) функції гешування на основі обчислення значення полінома над скінченним полем;

6) функції гешування по кривій Ферма.

Підходи, використані для побудування універсальних функцій гешування 1-4 є непрактичними, оскільки вимагають зростання довжини ключа пропорційно довжині повідомлення, яке обробляється.

Проведений аналіз стійкості розглянутих вище універсальних функцій гешування показав, що найвищу стійкість (найменшу імовірність колізії) при однаковій довжині геш-значення забезпечують функції гешування на основі обчислення значення полінома над скінченним полем та функції гешування по кривій Ферма.

В результаті проведеного аналізу і експерементальної перевірки встановлені і зведені в таблицю 1 основні властивості універсальних функцій гешування, які були розлянуті.

Таблиця 1. Основні властивості універсальних функцій гешування

	Функції гешування на основі обчислення значення полінома над скінченним полем	Гешування по кривій Ферма	NH
Швидкодія	низька	низька	висока
Стійкість	середня	висока	низька
Можливість використання паралельних обчислень	немає	немає	SIMD

В результаті аналізу таблиці 1 можна сформулювати два наступних протиріччя.

1. Перше протиріччя – це протиріччя між швидкодією та стійкістю. Універсальна функція гешування NH має дуже високу швидкодію, але низьку стійкість, і навпаки, гешування по функціональним полям кривих Ферма має найвищу стійкість, але найгіршу швидкодію. Функції гешування на основі обчислення значення полінома над скінченним полем за обома показниками знаходиться у проміжному положенні.

2. Друге протиріччя – це протиріччя у способі організації обчислень. Усі три розглянуті функції гешування є однопоточними, тоді як перспективою розвитку електроніки та обчислювальної техніки є широке впровадження паралельних обчислень.

Аналіз результатів вимірювання швидкодії, свідчить про перспективність використання перетворень в кільцях замість перетворень в полях для гешування.

За результатами проведеного аналізу можна сформулювати наступні завдання для розробки:

1) удосконалити існуючу функцію гешування на основі обчислення значення полінома шляхом використання паралельних обчислень;

2) розробити і дослідити функцію гешування на основі обчислення значення полінома, що використовує перетворення в кільцях;

3) розробити і дослідити функцію гешування по функціональним полям кривих Ферма, що використовує перетворення в кільцях.

У четвертому розділі дисертаційної роботи удосконалено метод універсального гешування на основі обчислення значення полінома над скінченним полем шляхом використання паралельних обчислень, розроблено метод гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l, розроблено метод гешування, що використовує композиційну каскадну схему і гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l на обох каскадах.

Для того, щоб побудувати паралельну версію алгоритма був використаний той факт, що обчислення полінома може бути виконане наступним чином:

$$h_x(m) = \sum_{i=0}^{k} x^i m_i \quad modp = \\ = \sum_{j=1}^{\left(\frac{k}{n}\right)} x^{j*n} \left(\sum_{g=0}^{n-1} x^g m_{j*n+g} modp \right) modp + \sum_{g=0}^{kmodn} x^g m_i \tag{2}$$

де k — число блоків повідомлення, n - число процесорних ядер.

Частини, що наведені у формулі (2) у дужках можуть бути обчислені паралельно максимум у $\left(\frac{k}{n}\right)$ потоків. При цьому на значення n не накладається жодних обмежень, що дозволяє гнучко підлаштовувати процес обчислення під властивості конкретної системи. Більш того, оскільки кінцеве геш-значення залишається незмінним згідно із формулою (2), то на різних системах, що взаємодіють, можливо побудувати процес обчислень по-різному, оптимально для кожної з систем, без втрати сумісності, чого не вдавалось досягти із звичайними геш-функціями.

Показано, що така архітектура обчислень є оптимальною з точки зору паралельних обчислень.

Метод гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l передбачає обчислення геш-значення за формулою

$$h_x(m) = \sum_{i=1}^{r} m_i x^i \quad mod 2^l \tag{3}$$

де x – ключ, m_i – блоки повідомлення, а $h_x(m)$ - обчислене геш-значення.

В основі методу гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l лежить той факт, що поліном над замкнутим скіненним кільцем має скінченну кількість коренів, отже існує обмежена множина ключів, які при однаковому вхідному повідомленні дадуть однакове геш-значення, отже імовірність колізії не перевищує певного заданого значення.

Значення ключа необхідно обирати тільки з множини непарних чисел, оскільки тільки непарні числа з визначеною над ними операцією множення за модулем 2^l утворюють циклічну мультиплікативну групу, інакше знаходження колізі буде тривіальною задачею.

Твердження 1. Якщо $r-$ непарне, а для всіх $0 \le m_i < 2^l - 1$ виконується

$$m_i \mod 2 = 0 \tag{4}$$

то поліном виду

$$p_n(x) = x^n(x+r) + \sum_{i=0}^{n-1} m_i \cdot x^i \tag{5}$$

має у множині коренів $p_n(x)$ є один і тільки один непарний корінь.

Доведення. Для доведення скористаємося методом математичної індукції. Спочатку доведемо, що умова твердження виконується для випадку значення параметра $n = 1$.

У випадку значення параметра $n = 1$ поліном (5) прийме вид

$$p_1(x) = k^2 + rk + m_0 \tag{6}$$

Якщо поліном (6) має корені серед цілих чисел, то його можна переписати у вигляді $p_1(x) = (x - a)(x - b)$. Розглянемо наступні випадки:

1) обидва кореня непарні;

2) один з коренів (припустимо a) непарний, а інший – парний;

3) обидва кореня парні.

Розкриємо дужки $(x - a)(x - a) = x^2 - (a + b)x + ab$. Якщо і a, і b непарні, то ab також буде непарним, що суперечить умові 4. Якщо і a, і b парні, то $a + b$ також буде парним, що суперечить умові $r-$ непарне. Отже, єдиним можливим варіантом є варіант, коли один з коренів непарний, а інший – парний. Отже, для значення параметра $n = 1$ твердження виконується.

Припустимо, що умова твердження виконується для полінома $p_n(x)$ з деяким значенням параметра n. Покажемо, що тоді умова виконується і для полінома $p_{n+1}(x)$ із значенням параметра $n + 1$. Для цього необхідно довести, що

результат множення $p_n(x)(x-a)=\left(x^n(x+r)+\sum_{i=0}^{n-1}m_i\cdot x^i\right)(x-a)$, де $a-$ непарне не може бути представлений у вигляді $p_{n+1}(x)=\left(x^{n+1}(x+r)+\sum_{i=0}^{n}m_i\cdot x^i\right)$.

Помножимо поліном $p_n(x)$ виду (5) на $(x-a)$, де $a-$ непарне. Отриманий таким чином добуток повинен мати два непарних кореня.

$$\begin{gathered}\left(k^n(k+r)+\sum_{i=0}^{n-1}m_i\cdot k^i\right)(k-a)=\\ =k\left(k^{n+1}+rk^n+\sum_{i=0}^{n-1}m_i\cdot k^i\right)+a\left(k^{n+1}+rk^n+\sum_{i=0}^{n-1}m_i\cdot k^i\right)=\\ =k^{n+2}+rk^{n+1}+\sum_{i=0}^{n-1}m_i\cdot k^{i+1}+ak^{n+1}+ark^n+\sum_{i=0}^{n-1}m_i\cdot k^i=\\ =k^{n+2}+(a+r)k^{n+1}+ak^n+\sum_{i=0}^{n-1}m_i\cdot k^{i+1}+\sum_{i=0}^{n-1}m_i\cdot k^i\end{gathered} \tag{7}$$

Результат розкриття дужок, отриманий у виразі (7), не може бути представлений як поліном $p_{n+1}(x)$ виду (5) зі значенням параметра $n+1$, оскільки коефіцієнт при члені степеня $n+1$ завжди парний, а за умовою твердження у поліномі виду (5) коефіцієнт при другому за значенням степеня члені завжди непарний. Оскільки при приведенні за модулем 2^l парні числа можуть відображатися тільки в парні, а непарні – в непарні, то $(a+1)mod2^l\neq 1$, якщо a – непарне. Таким чином, якщо умова твердження виконується для полінома з деяким значенням параметра n, то умова виконується і для полінома із значенням параметра $n+1$. А отже, за методом математичної індукції твердження виконується для всіх n.

Кількість коренів полінома визначає імовірність колізії для універсальної функції гешування на основі обчислення значення полінома над скінченним полем. Таким чином, найкращі результати з імовірності колізії забезпечуються при найменшому числі коренів. Найменше число коренів досягається у відповідності до твердження 1 за умови використання непарних ключів і парних блоків повідомлення.

Твердження 2. Метод гешування на основі обчислення значення полінома над кільцями належить до класу $2^{-l+1}-U$ функцій гешування.

Доведення. У відповідності до твердження 1 поліном виду (5) має серед коренів лише один непарний корінь, а значення ключів обираються лише з множини непарних чисел, отже імовірність колізії складає 2^{-l+1} незалежно від довжини повідомлення.

Обчислення геш-значення здійснюється за схемою Горнера. Оскільки значення ключа для розробленого методу завжди непарне, а значення блока

повідомлення завжди парне, то нераціонально зберігати і обробляти молодший біт.

Складання двох парних чисел за модулем 2^l може бути представлене у вигляді

$$(2x_1 + 2x_2) mod 2^l = 2(x_1 + x_2) mod 2^l \quad (8)$$

Використовуючи правило скорочення можна написати

$$2(x_1 + x_2) mod 2^l = 2\left((x_1 + x_2) mod 2^{l-1}\right) \quad (9)$$

Множення непарного числа на парне за модулем 2^l може бути представлене у вигляді

$$\left(2x_1 * (2x_2 + 1)\right) mod 2^l = (4x_1x_2 + 2x_1) mod 2^l \quad (10)$$

Використовуючи правило скорочення можна написати

$$(4x_1x_2 + 2x_1) mod 2^l = 2\left((2x_1x_2 + x_1) mod 2^{l-1}\right) \quad (11)$$

В результаті мовою програмування С основний крок алгоритму виглядатиме наступним чином

```
unsigned int h, k;
unsigned int m*;
...
h = ((h * k) << 1) + h +m[i];
```

Метод гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l має наступну вразливість: якщо ключ утворює циклічну підгрупу невеликого порядка (менше ніж довжина повідомлення), то порушник може обміняти місцями 2 блока повідомлення без зміни геш-значення. Потужність множини ключів складає $2^l / 2 = 2^{l-1}$, отже до класу слабких ключів відносяться ключі, які утворюють циклічну підгрупу розміром менше 2^{l-1}. Розмір найбільшої циклічної підгрупи мультиплікативної групи непарних чисел за модулем 2^l складає 2^{l-2}, отже частка слабких ключів не перевищує $2^{l-2} / 2^{l-1} = 0{,}5$ для повідомлень довжини від 2^{l-2} до 2^{l-1}.

Якщо перевіряти і відкидати слабкі ключі до початку їх використання, то простір ключів зменшиться вдвічі і стане менше простора геш-значень. Тоді порушнику легше буде перебирати ключі, ніж шукати прообраз для геш-значень.

Для захисту від цієї вразливості необхідно використовувати методи, у яких довжина ключа більше довжини геш-значення.

Наші дослідження показали, що метод гешування по проективним кривим над кільцями має низьку стійкість (високу імовірність колізії), тому не може бути застосований.

Метод гешування, що використовує композиційну каскадну схему і гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l на обох каскадах визначається як

$$H = H_2(H_1(M_1)||H_1(M_2)||...||H_1(M_t)) \quad (12)$$

де H_1, H_2 визначають універсальні функцій гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l з різними ключами.

Використання саме композиційної каскадної схеми а не схеми зі зв'язкою геш-значення і тексту обґрунтовано тим, що для схеми зі зв'язкою геш-значення і тексту необхідно до початку обчислення знати довжину повідомлення, що є неприйнятним з точки зору безумовних критеріїв.

Метод гешування, що використовує композиційну каскадну схему і гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l також має клас слабких ключів аналогічно методу гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l, однак кількість сильних ключів значно більша за кількість геш-значень, що робить для порушника більш вигідним атакувати саме перехоплені геш-значення, а не перебирати ключі.

У п'ятому розділі дисертаційної роботи зроблено порівняння швидкості розроблених методів універсального гешування з іншими методами вироблення кодів автентифікації повідомлень, а саме з CBC-MAC за ДСТУ ГОСТ 28147:2009 та HMAC на основі геш-функції Blake. Для цього визначені рівні стійкості, наведені у таблиці 2.

Таблиця 2

Визначення рівнів стійкості

Назва рівня стійкості	імовірність знаходження колізій P_{col}	імовірність знаходження другого прообразу $P_{secpreim}$	імовірність знаходження прообразу P_{preim}	імовірність розширення повідомлення P_{ext}
низький (ДСТУ ГОСТ 28147:2009, 32 біта)	2^{-16}	2^{-32}	2^{-32}	2^{-32}
базовий-1	2^{-112}	2^{-224}	2^{-224}	2^{-224}

(HMAK, 224 біта)				
базовий-2 (HMAK, 256 біта)	2^{-128}	2^{-256}	2^{-256}	2^{-256}
середній (HMAK, 384 біта)	2^{-192}	2^{-384}	2^{-384}	2^{-384}
високий (HMAK, 512 бітів)	2^{-256}	2^{-512}	2^{-512}	2^{-512}

Для кожного рівня стійкості були проведені окремі вимірювання швидкодії. Результати вимірювань зведені у таблицю 3.

Таблиця 3

Результати вимірювань

Рівні стійкості, бітів	32	224	256	384	512
Назва функції гешування	Швидкодія, тактів на байт				
ДСТУ ГОСТ 28147:2009	50,9	-	-	-	-
HMAC-Blake	25,9	25,9	25,9	72,6	72,6
Функції гешування на основі обчислення значення полінома над скінченним полем	9,88	45,8	51,5	71,8	88,8
Функції гешування по полям раціональних функцій проективних кривих	10,5	45,6	53,8	74,0	90,5
Функція гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l	3,45	28,1	31,7	44,2	51,9
Функція гешування, що використовує композиційну каскадну схему і гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l	2,58	25,5	28,0	40,8	48,5

У рядках зазначені функції вироблення кодів автентифікації, а у стовпчиках – швидкодія у тактах на байт.

У кінцевому випадку для всіх рівнів безпеки результат порівняння методів вироблення кодів автентифікації повідомлень за методикою, розробленою у другому розділі, є наступним:

1) Функція гешування, що використовує композиційну каскадну схему і гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l;

2) Функція гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l;

3) Функції гешування по полям раціональних функцій проективних кривих;

4) Функції гешування на основі обчислення значення полінома над скінченним полем;

5) HMAC-Blake;

6) ДСТУ ГОСТ 28147:2009.

Таким чином, розроблені у дисертаційній роботі методи універсального гешування придатні для використання з метою автентифікації повідомлень різних довжин і з різним рівнем стійкості замість існуючих методів, побудованих на основі блокових симетричних шифрів (ДСТУ ГОСТ 28147:2009 в режимі вироблення імітовставки) та на основі криптографічних функцій гешування (HMAC-Blake).

ВИСНОВКИ

В результаті виконаних теоретичних та експериментальних досліджень і розробок в дисертації вирішено низку наукових та практичних задач розвитку теорії та практики кодів автентифікації повідомлень з підвищеною швидкодією.

Достовірність результатів, що отримані здобувачем, підтверджується коректним використанням сучасного математичного апарату, збігом результатів теоретичних та експериментальних досліджень; використанням отриманих з практики даних; ясним тлумаченням результатів, що не суперечать відомим даним.

Висновки, сформульовані в роботі, полягають в наступному.

1. Удосконалено метод універсального гешування на основі обчислення значення полінома над скінченним полем, який відрізняється від прототипу тим, що передбачає гешування повідомлення у n паралельних потоків суперблоками з n блоків з деяким ключем x з наступним гешуванням отриманих проміжних геш-значень з ключем $x^n \bmod p$, що дозволило збільшити швидкодію у n разів, де n – число потоків.

2. Вперше запропоновано метод універсального гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l, який відрізняється від відомих тим, що використовує лише перетворення над кільцем цілих чисел модулю 2^l замість перетворень у полях, що дозволило забезпечити

імовірність колізії $\frac{1}{2^{l-1}}$ незалежно від довжини повідомлення, збільшити швидкодію приблизно у 2,5 разів у порівнянні з функцією гешування на основі обчислення значення полінома над скінченним полем, забезпечити невразливість до атак спостереження за часом виконання. Як і функція гешування на основі обчислення значення полінома над скінченним полем, метод універсального гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l має клас слабких ключів, розмір якого збільшується зі збільшенням довжини повідомлення.

3. Вперше запропоновано метод універсального гешування, що використовує композиційну каскадну схему і універсальне гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l на обох каскадах, який відрізняється від методу гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l тим, що має кількість ключів, які не належать до класів слабких ключів, більшу ніж кількість геш-значень.

4. За результатами порівняння для всіх рівнів безпеки і для всіх довжин повідомлення порядок у рейтингу методів гешування зберігається наступним:

1) Функція гешування, що використовує композиційну каскадну схему і гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l;

2) Функція гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l;

3) Функції гешування по полям раціональних функцій проективних кривих;

4) Функції гешування на основі обчислення значення полінома над скінченним полем;

5) HMAC-Blake;

6) ДСТУ ГОСТ 28147:2009.

5. Розроблені у дисертаційній роботі методи універсального гешування придатні для використання з метою автентифікації повідомлень різних довжин і з різним рівнем стійкості замість існуючих методів, побудованих на основі блокових симетричних шифрів (ДСТУ ГОСТ 28147:2009 в режимі вироблення імітовставки) та на основі криптографічних функцій гешування (HMAC-Blake).

ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Бойко А.О. Універсальні функції гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^n / А.О. Бойко // Тематичний збірник ХУПС “Системи обробки інформації”. – 2012. – № 3. – С. 142–146.

2. Горбенко І.Д. Причини, стан та попередні підсумки проекту SHA-3 / І.Д. Горбенко, А.О.Бойко, А. М. Герцог // Прикладна радіоелектроніка. – 2009. – Т.8, №3. – С. 315–320.

3. Горбенко І.Д. Порівняння перспективних швидкодіючих функцій гешування / І.Д. Горбенко, А.А. Бойко, А.М. Герцог // Прикладная радиоэлектроника. – 2009. – Т.8, №3. – С. 321–326.

4. Корченко А.Г. Многокаскадное универсальное хеширование по рациональным функциям максимальной кривой третьего рода / А.Г. Корченко, Е.В. Котух, А.О. Бойко // Радіотехніка. – 2011. – №166. – С. 44–49.

5. Горбенко І.Д. Стан створення та напрями досліджень і розробок зі створення перспективних стандартів гешування / І.Д. Горбенко, А.О. Бойко, А.М. Герцог // Радіоелектронні і комп'ютерні системи. – 2010. – № 5(46). – С. 67–74.

6. Горбенко І.Д. Методика і результати порівняння алгоритмів геш-функцій, що приймають участь у 3-му раунді конкурсу NIST SHA-3 / І.Д. Горбенко, А.О. Бойко, С.І. Даценко // Прикладная радиоэлектроника. – 2011. – Т.10, № 2. – С. 171–-175.

7. Бойко А.О. Обґрунтування архітектури функції гешування з використанням паралельних обчислень / А.О. Бойко, І.Д. Горбенко // Вісник Харківського національного університету. – 2010. – № 890. – С. 29–36.

8. Горбенко І.Д. Сучасні підходи до побудування геш-функцій з підвищеною стійкістю / І.Д. Горбенко, А.О. Бойко // Праці міжнародного симпозіуму «Питання оптимізації обчислень (ПОО-XXXV)», присвяченого 40-річчю 1-го симпозіуму та літньої математичної школи з питань точності й ефективності обчислювальних алгоритмів (м. Київ, м. Одеса; 1969 рік). – Київ: Інститут кібернетики імені В. М. Глушкова НАН України, – 2009. – Т.1. – С. 159–163.

9. Бойко А.О. Обґрунтування архітектури функції гешування з використанням паралельних обчислень / А.О. Бойко, І.Д. Горбенко // Труды научно-технической конференции с международным участием «Компьютерное моделирование в наукоемких технологиях» (КМНТ-2010) – Харьков: Харьковский национальный университет имени Каразина. – 2010. – Часть 1. – С. 111–113.

10. Бойко А.А Практическая проверка свойств параллельных хеш-функций с различными архитектурами / А.А. Бойко // XIII Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». Тезисы докладов – Киев: Государственная служба специальной связи и защиты информации. – 2010. – С. 55–56.

11. Халимов Г.З. Каскадное универсальное хеширование / Г.З. Халимов, А.А. Бойко, Е.В. Котух // Сборник трудов Второй Международной научно-технической конференции «Компьютерные науки и технологии КНиТ-2011» – Белгород. – 2011. – С. 541–544.

12. Бойко А.О. Порівняльний аналіз сучасних геш-функцій / А.О. Бойко, І.Д. Горбенко // Тезисы докладов международной конференции, посвященной 50-

летию механико-математического факультета «Современные проблемы математики и ее приложения в естественных науках и информационных технологиях» – Харьков: Харьковский национальный университет имени Каразина. – 2011. – С. 172.

13. Бойко А.А. Метод универсального хеширования по алгебраическим кривым над кольцами векторов / А.А. Бойко, Г.З. Халимов // XV Юбилейная Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». Тезисы докладов – Киев: Государственная служба специальной связи и защиты информации Украины. – 2012. – С. 35.

14. Котух Е.В. Метод универсального хеширования по алгебраическим кривым / Е.В. Котух, Г.З.Халимов, А.А. Бойко, А.М. Герцог // XV Юбилейная Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». Тезисы докладов – Киев: Государственная служба специальной связи и защиты информации Украины.– 2012. – С. 36.

АНОТАЦІЯ

Бойко А. О. Методи побудування кодів автентифікації повідомлень з підвищеною швидкодією. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук по спеціальності 05.13.21 – Системи захисту інформації. – Харківський національний університет радіоелектроніки, Харків, 2012.

Дисертаційна робота присвячена розробці та удосконаленню методів вироблення кодів автентифікації повідомлень.

Удосконалено метод універсального гешування на основі обчислення значення полінома над скінченним полем шляхом використання паралельних обчислень. Удосконалений метод дозволяє гешування повідомлення у n паралельних потоків, що дозволило збільшити швидкодію у n разів, де n - число потоків. Вперше запропоновано метод універсального гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l замість перетворень у полях, що дозволило збільшити швидкодію приблизно у 2,5 разів у порівнянні з функцією універсального гешування на основі обчислення значення полінома над скінченним полем, забезпечити невразливість до атак спостереження за часом виконання. Наводяться твердження, що визначають імовірність колізії для розробленого методу. Вперше запропоновано метод універсального гешування, що використовує композиційну каскадну схему і гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l на обох каскадах, що дозволило забезпечити більшу кількість ключів, які не належать до класів слабких ключів. Запропоновано ряд алгоритмічних рішень, які дозволили збільшити швидкодію.

Ключові слова: автентифікація повідомлень, універсальне гешування, перетворення в кільці цілих чисел за модулем 2^l, схема Горнера, паралельне обчислення.

АННОТАЦИЯ

Бойко А. А. Методы построения кодов аутентификации сообщений с повышенным быстродействием. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – Системы защиты информации. – Харьковский национальный университет радиоэлектроники, Харьков, 2012.

Диссертация посвящена разработке и усовершенствованию методов построения кодов аутентификации сообщений с повышенным быстродействием.

Усовершенствован метод универсального хеширования на основе вычисления значения полинома над конечным полем путем использования параллельных вычислений. Усовершенствованный метод позволяет хешировать сообщения в n паралельных потоков, что позволило увеличить быстродействие в n раз, где n-число потоков. Впервые предложен метод универсального хеширования на основе вычисления значения полинома в кольце целых чисел за модулем 2^l вместо преобразований в полях, что позволило увеличить быстродействие приблизительно в 2,5 раза в сравнении с функцией универсального хеширования на основе вычисления значения полинома над конечным полем, обеспечить неуязвимость к атакам наблюдения за временем исполнения. Приводятся утверждения, определяющие вероятность коллизии для разработанного метода. Впервые предложен метод универсального хеширования, использующий композиционную каскадную схему и хеширование на основе вычисления значения полинома в кольце целых чисел за модулем 2^l, что позволило обеспечить большее количество ключей, не относящихся к классу слабых ключей. Предложен ряд алгоритмических решений, позволяющих увеличить быстродействие.

Ключевые слова: аутентификация сообщений, универсальное хеширование, преобразование в кольце целых чисел за модулем 2^l, схема Горнера, паралельное вычисление.

ABSTRACT

Boiko A.O. Message authentication techniques with higher speed. - Manuscript.

Thesis for the degree of candidate of technical sciences on the speciality 05.13.21 - Information Security Systems. - Kharkiv National University of Radio Electronics, Kharkiv, 2012.

The dissertation is devoted to the development and improvement of high-speed message authentication techniques.

Universal hashing technique based on polynomial evaluation over finite fields was improved by using parallel computing. Improved technique allows hashing of message in n parallel threads, which allows increase speed in n times. Universal hashing technique based on polynomial evaluation over ring of integer by modulo 2^l instead of transformations over fields was proposed. The proposed technique is approximately 2.5 times faster then technique based on polynomial evaluation over finite field and is not vulnerable to timing attacks. Some propositions, defining the probability of collisions are placed here. Universal hashing technique based on composition cascading scheme and hashing based on polynomial evaluation over ring of integer by modulo 2^l was proposed. Proposed technique has more keys not belonging to weak keys class. A few algorithmic decisions are proposed increasing speed.

Key words: message authentication, universal hashing, transformation over the ring modulo 2^l, Horner's rule, parallel computing.